|  |  |  |  |
| --- | --- | --- | --- |
| **ODWRÓCONA TABELA ZGODNOŚCI** | | | |
| **projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa** | | | |
| **l.p.** | **jednostka redakcyjna**  **projektu** | **treść przepisu** | **uzasadnienie wprowadzenia przepisu** |
| 1. . | Art. 1 ust. 2 pkt 1-2 | w ust. 2 pkt 1 otrzymuje brzmienie:  „1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów z wyjątkiem art. 66a-66c, art. 67a-67b i art. 73 -74”,  c) w ust. 2 pkt 2 otrzymuje brzmienie:  „2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73) z wyjątkiem art. 67a-67b i art. 73-74;”; | Niniejsza ustawa oprócz implementacji przepisów Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15) (dalej akt o cyberbezpieczeństwie) wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.  Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie. |
|  | Art. 2 pkt. 3a-3d | „3a) 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;  3b) ISAC – centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;  3c) SOC – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie;  3d) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L Nr 218, str. 30), zwanym dalej „rozporządzeniem (WE) nr 765/2008”, | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Nowe definicje związane są z wprowadzeniem nowych elementów mających na celu usprawnienie działania krajowego systemu cyberbezpieczeństwa. |
|  | Art. 2 ust. 1 pkt. 4a | 4a)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;” | Projekt ustawy dostosowuje katalog definicji w ustawie o KSC do zmian jakie zostały wprowadzone w akcie o cyberbezpieczeństwie. W szczególności oznacza to konieczność przyjęcia nowej definicji cyberbezpieczeństwa, która została wprowadzona w ww. akcie prawnym.  Tam gdzie jest to konieczne, zachowano poprzednie znaczenia terminu: „cyberbezpieczeństwo” i wprowadzone zostało pojęcie „bezpieczeństwa systemów informacyjnych” (art. 2 pkt 4a), którego zakres jest identyczny z poprzednią definicją cyberbezpieczeństwa. Nie spowoduje to jednak zmian w zakresie konkretnych obowiązków jakie obecnie nakłada ustawa na podmioty krajowego systemu cyberbezpieczeństwa . W celu zachowania spójności z dyrektywą NIS pojęcie „sieci i systemów informatycznych” zastąpione zostało pojęciem „systemy informacyjne” zgodnie ze sposobem, w jakim to pojęcie zostało implementowane do polskiego porządku prawnego w 2018 roku.  Pojęcie to zastąpiło więc pojęcie „cyberbezpieczeństwa” w przepisach, które były bezpośrednią implementacją przepisów dyrektywy NIS. Dzięki temu treść tych przepisów nie ulega w praktyce zmianie. |
|  | Art. 2 ust. 1 pkt. 5 | 5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”, | Niniejsza zmiana jest wprost wynikiem zmiany definicji cyberbezpieczeństwa i w praktyce sprawie, że treść definicji incydentu nie ulega zmianie. |
|  | Art. 2 ust. 1 pkt. 11 | 11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;”, | Niniejsza zmiana jest wprost wynikiem zmiany definicji cyberbezpieczeństwa i w praktyce sprawie, że treść definicji podatności nie ulega zmianie. |
|  | Art. 2 ust. 1 pkt. 26-31 | 26) deklaracja zgodności – oświadczenie dostawcy sprzętu lub oprogramowania, że wyrób jest zgodny z europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa;  27) krajowy certyfikat cyberbezpieczeństwa - certyfikat cyberbezpieczeństwa wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa;  28) krajowa deklaracja zgodności - deklaracja zgodności wydana w ramach krajowego programu certyfikacji cyberbezpieczeństwa;  29) certyfikat – europejski certyfikat cyberbezpieczeństwa lub krajowy certyfikat cyberbezpieczeństwa;”  30) krajowy poziom uzasadnienia zaufania – potwierdzenie, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi bezpieczeństwa określonego krajowego programu certyfikacji cyberbezpieczeństwa, wskazuje również poziom, na jakim została dokonana ocena danego produktu ICT, usługi ICT lub procesu ICT;  31) ENISA - Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa;; | Wprowadzone w punktach 26-29 definicje związane są z przepisami wprowadzającymi krajowe programy certyfikacji cyberbezpieczeństwa. Wiele kwestii związanych z deklaracjami zgodności i certyfikatami odnoszącymi się do europejskich programów certyfikacyjnych zostało rozwiązanych w bezpośrednio stosowanych przepisach aktu o cyberbezpieczeństwie. Chcieliśmy by przepisy dotyczące krajowe certyfikaty i deklaracje zgodności zawierały analogiczne rozwiązania. Tam więc gdzie istnieje potrzeba by przepis odnosił się tylko do krajowych certyfikatów i deklaracji zgodności stosujemy definicje z pkt. 27-28.  Tam zaś gdzie przepisy odnoszą się do wszystkich certyfikatów i deklaracji zgodności stosowane są definicje z pkt. 26 i 29.  Krajowy poziom uzasadnienia zaufania został wprowadzony gdyż definicja poziomu uzasadnienia zaufania z aktu o cyberbezpieczeństwie odnosi się tylko do europejskich programów certyfikacyjnych.  W związku z tym, chcąc zastosować podobne rozwiązania co w europejskich programach certyfikacyjnych, wprowadzona została definicja krajowego poziomu uzasadnienia zaufania. Treściowo jest ona analogiczna do tej wprowadzonej w akcie o cyberbezpieczeństwie. |
|  | Art. 4 | w art. 4:  a) w pkt 7 wyrazy „w art. 9 pkt 1-6, 8-10, 11 i 12” zastępuje się wyrazami „w art. 9 pkt 1-6, 8 i 9”,  b) po pkt 7 dodaje się pkt 7a-7b w brzmieniu:  „7a) Urząd Komisji Nadzoru Finansowego;  7b) ISAC;”,  c) pkt 8 otrzymuje brzmienie:  „8) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 r. poz. 85, 374, 695, 875 i 1086);”,  d) po pkt 14 dodaje się pkt 14a-14b w brzmieniu:  „14a) Wody Polskie, o których mowa w art. 239 ustawy z dnia 20 lipca 2017 r. Prawo wodne (Dz. U. z 2020 r. poz. 310, 695, 782, 875 i 1378);  14b) Polski Fundusz Rozwoju, o którym mowa w ustawie z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2020 r. poz. 2011);” | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres podmiotowy w celu wzmocnienia cyberbezpieczeństwa wskazanych podmiotów. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. |
|  | Art. 7 ust. 5 | w art. 7 ust. 5 otrzymuje brzmienie:  „5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejsza zmiana ma uporządkować kwestie związane z podpisywaniem wniosków o wpis o do wykazu operatorów usług kluczowych. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. |
|  | Art. 8 pkt 5 lit. b | „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. |
|  | Art. 9 ust. 1 i 2 | 7) w art. 9:  a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”,  b) ust. 2 otrzymuje brzmienie:  „2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego dane osób, o których mowa w ust. 1 pkt 1, zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych - w terminie 14 dni od dnia ich zmiany.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten doprecyzowuje kwestie związane ze zgłaszaniem osób kontaktowych do krajowego systemu cyberbezpieczeństwa. |
|  | Art. 10 | w art. 10  a) w ust. 1-4 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”,  b) w ust. 2 pkt 2 otrzymuje brzmienie:  „2) ochronę dokumentów przed przypadkowym uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”,  c) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazami „bezpieczeństwa systemów informacyjnych”; | Niniejsza zmiana jest związana z wprowadzaniem w akcie o cyberbezpieczeństwie definicji cyberbezpieczeństwa. W związku z tym, iż automatycznie zastąpiła ona dotychczas funkcjonującą krajową definicje cyberbezpieczeństwa. W związku z tym konieczne było dostosowanie przepisów posługujących się tym pojęciem. Tam gdzie konieczne było zachowanie wcześniejszego rozumienia cyberbezpieczeństwa słowo to zostało zastąpione sformułowaniem „bezpieczeństwo systemów informacyjnych”. |
|  | Art. 11 ust. 3 pkt 1-3 | w art. 11 w ust. 3 pkt 1-3 otrzymują brzmienie:  „1) przekazuje jednocześnie właściwemu CSIRT sektorowemu w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4;  2) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;  3) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten doprecyzowuje kwestie związane z działaniem CSIRT-ów sektorowych wobec operatorów usług kluczowych. |
|  | Art. 14 | art. 14 otrzymuje brzmienie:  „Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13 w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach SOC.  2. Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę dotyczącą prowadzenia SOC na jego zlecenie z innym podmiotem. SOC powołany przez operatora usługi kluczowej może realizować zadania, o których mowa w ust. 1, także na rzecz innych podmiotów.  3. SOC, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu:  1) monitorowania i wykrywania incydentów;  2) reagowania na incydenty;  3) zapobiegania incydentom;  4) zarządzania jakością zabezpieczeń systemów, informacji i powierzonych aktywów;  5) aktualizowania ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.  4. Operator usługi kluczowej w przypadku zawarcia umowy dotyczącej prowadzenia SOC informuje organ właściwy do spraw cyberbezpieczeństwa o:  1) zawarciu takiej umowy,  2) danych kontaktowych podmiotu, z którym zawarta została umowa,  3) zakresie świadczonej usługi,  4) terminie obowiązywania umowy,  5) rozwiązaniu umowy  – w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.  5. W przypadkach, kiedy jest to niezbędne dla zapewnienia cyberbezpieczeństwa, podmiot prowadzący SOC zapewnia bezpieczny zdalny dostęp do swoich systemów dla obsługiwanego operatora usługi kluczowej przez co najmniej:  1) ustalenie zasad dostępu do systemu;  2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;  3) minimalizację przechowywanych danych poza bezpiecznym środowiskiem.  6. Przy zawieraniu umowy na świadczenie usług SOC przez podmiot prowadzący SOC dla operatora usługi kluczowej zawiera się zastrzeżenie, że usługi te podlegają prawu polskiemu.  7. Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:  1) nazwa SOC i posiadanych przez SOC kompetencji;  2) zakres obszaru działania, w tym:  a) oferowany rodzaj wsparcia,  b) zasady współpracy i wymiany informacji,  c) politykę komunikacji i uwierzytelniania informacji;  3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów;  4) dane kontaktowe, w tym:  a) adres ze wskazaniem strefy czasowej,  b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC,  c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC,  d) sposoby kontaktu z SOC, w tym sposób zgłaszania incydentów.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: ,,SOC”. Pojęcie to zastąpi struktury odpowiedzialne za cyberbezpieczeństwo u operatorów usług kluczowych. SOC posiadają ugruntowaną na rynku pozycję struktur realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek. Operatorzy usług kluczowych będą dysponowały strukturami SOC wewnątrz organizacji lub zawierali umowę z zewnętrznym podmiotem świadczącym usługi SOC. SOC m.in. będzie prowadził szacowanie ryzyka, wykrywał oraz reagował na incydenty. Minister właściwy do spraw informatyzacji będzie prowadził wykaz operacyjnych centrów bezpieczeństwa. Dotychczasowe wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo oraz podmioty zewnętrze, świadczące usługi cyberbezpieczeństwa dla operatorów usług kluczowych, staną się automatycznie SOC w rozumieniu ustawy o KSC. |
|  | Art.14a | po art. 14 dodaje się art. 14a w brzmieniu:  „14a. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz SOC.  2. Wykaz SOC zawiera:  1) nazwę (firmę) podmiotu prowadzącego SOC;  2) nazwę (firmę) podmiotów, na rzecz których SOC realizuje zadania;  3) siedzibę i adres SOC;  4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;  5) numer we właściwym rejestrze, jeżeli został nadany;  6) datę wpisania do wykazu SOC;  7) datę wykreślenia z wykazu SOC.  3. Wpisanie do wykazu SOC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie po uzyskaniu informacji od operatora usługi kluczowej, o której mowa w art. 14 ust. 2, lecz nie później niż 14 dni po uzyskaniu tej informacji. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1-5.  4. Zmiana danych w wykazie SOC następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa, złożony nie później niż w terminie 6 miesięcy od zmiany tych danych.  5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.  6. Wpisanie do wykazu SOC i wykreślenie z tego wykazu oraz zmiana danych w wykazie SOC jest czynnością materialno-techniczną.  7. Minister właściwy do spraw informatyzacji może, z urzędu, wpisać do wykazu, o którym mowa w ust. 1, SOC inny niż określony w ust. 3, jeżeli SOC:  1) świadczy usługi związane z:  a) monitorowaniem, wykrywaniem reagowaniem i zapobieganiem incydentów,  b) zarządzaniem jakością zabezpieczeń systemów, informacji i powierzonych aktywów,  c) aktualizowaniem ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent;  2) przedstawi dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) oraz,  3) zawrze z ministrem właściwym do spraw informatyzacji porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46.  8. Minister właściwy do spraw informatyzacji wykreśla z wykazu wpisany z urzędu SOC, który przestał spełniać warunki, o których mowa w ust. 7.  9. Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym.  10. Dane z wykazu SOC, w zakresie niezbędnym do realizacji ich ustawowych zadań, minister właściwy do spraw informatyzacji udostępnia, na wniosek, następującym podmiotom:  1) organowi właściwemu do spraw cyberbezpieczeństwa;  2) Policji;  3) Żandarmerii Wojskowej;  4) Straży Granicznej;  5) Centralnemu Biuru Antykorupcyjnemu;  6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;  7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;  8) sądom;  9) prokuraturze;  10) organom Krajowej Administracji Skarbowej;  11) dyrektorowi Rządowego Centrum Bezpieczeństwa;  12) Służbie Ochrony Państwa.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  To kolejny przepis związany z powoływaniem struktur SOC. |
|  | Art. 17 ust. 2 , art. 69 ust. 1 i 2 | użyty w art. 17 w ust. 2, art. 69 w ust. 1, w ust. -2 w pkt 1, 6 i 7, w różnej liczbie i różnym przypadku, wyraz „cyberbezpieczeństwo” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „bezpieczeństwo systemów informacyjnych”; | Niniejsza zmiana jest związana z wprowadzaniem w akcie o cyberbezpieczeństwie definicji cyberbezpieczeństwa. W związku z tym, iż automatycznie zastąpiła ona dotychczas funkcjonującą krajową definicje cyberbezpieczeństwa. W związku z tym konieczne było dostosowanie przepisów posługujących się tym pojęciem. Tam gdzie konieczne było zachowanie wcześniejszego rozumienia cyberbezpieczeństwa słowo to zostało zastąpione sformułowaniem „bezpieczeństwo systemów informacyjnych”. |
|  | art. 8 w pkt 3, pkt 5 lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, 3 w pkt 1, 2, 4, 10, 14 w lit. b i c i w ust. 6 w pkt 2 , w art. 33 w ust. 4a, w art. 35 w ust. 4-5, w art. 37 w ust. 1, w art. 39 w ust. 1, 3 i 4 , w art. 46 w ust. 1 w pkt 5, w art. 51  w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i w ust. 2, w art. 73 w ust. 5 w pkt 1, w art. 83 | ) użyte w art. 8 w pkt 3, pkt 5 lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, 3 w pkt 1, 2, 4, 10, 14 w lit. b i c i w ust. 6 w pkt 2 , w art. 33 w ust. 4a, w art. 35 w ust. 4-5, w art. 37 w ust. 1, w art. 39 w ust. 1, 3 i 4 , w art. 46 w ust. 1 w pkt 5, w art. 51  w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i w ust. 2, w art. 73 w ust. 5 w pkt 1, w art. 83, w różnej liczbie i różnym przypadku, wyrazy „ zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i odpowiednim przypadku wyrazem „ cyberzagrożenie”; | Pojęcie „zagrożenie cyberbezpieczeństwa” zostało zastąpione pojęciem cyberzagrożenia (art. 2 pkt 17). Definicja cyberzagrożenia została wprowadzona w akcie o cyberbezpieczeństwie i jest ona bardzo zbliżona do funkcjonującej w naszym systemie prawnym definicji „zagrożenia cyberbezpieczeństwa”. Nie jest zasadne utrzymywanie w systemie prawnym obu tych pojęć i dlatego pozostawiono jedynie sformułowanie „cyberzagrożenie”. Nowe pojęcie jest zgodne z najnowszą terminologią w dziedzinie cyberbezpieczeństwa stosowaną w państwach członkowskich Unii Europejskiej. |
|  | Art. 21 | w art. 21  a) w ust. 1 wyrazy „osoby odpowiedzialnej” zastępuje się wyrazami „dwóch osób odpowiedzialnych”,  b) w ust. 2 i 3 wyrazy „jedną osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. |
|  | Art. 22 | w art. 22  a)w ust. 1 po pkt 2 dodaje się pkt 2a w brzmieniu:  „2a) będący jednostką samorządu terytorialnego, niezależnie od obowiązku, o którym mowa w pkt 2, zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego wojewody;”;  b) po ust. 1 dodaje się ust. 1a w brzmieniu:  „1a. Podmiot publiczny będący jednostką samorządu terytorialnego przekazuje dane o których mowa w ust. 1 w pkt 5 także do wojewody”. | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. |
|  | Art. 24a | po art. 24 dodaje się art. 24a w brzmieniu:  „Art. 24a. Wojewoda:  1) zapewnia wymianę informacji na temat cyberzagrożeń , podatności oraz incydentów dotyczących jednostek samorządu terytorialnego w województwie;  2) prowadzi listę danych kontaktowych osób z poszczególnych jednostek samorządu terytorialnego w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV;  3) we współpracy z Pełnomocnikiem oraz właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje marszałkowi województwa, starostom, wójtom, burmistrzom, prezydentom miast informacje dotyczące:  a) analiz, standardów, rekomendacji i dobrych praktyk w zakresie cyberbezpieczeństwa,  b) budowania potencjału i zdolności w obszarze cyberbezpieczeństwa,  c) budowania świadomości w obszarze cyberbezpieczeństwa,  d) rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa. | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. |
|  | Art. 25a | „Rozdział 5a  Zadania i obowiązki ISAC w ramach krajowego systemu cyberbezpieczeństwa  Art. 25a. 1. W ramach krajowego systemu cyberbezpieczeństwa może funkcjonować ISAC, do którego zadań należy w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów.  2. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa, zwany dalej wykazem ISAC.  3. Wykaz ISAC zawiera:  1) nazwę (firmę) ISAC;  2) imię i nazwisko osoby reprezentującej ISAC wraz z numerem telefonu oraz adres poczty elektronicznej;  3) siedzibę i adres ISAC, jeżeli posiada;  4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;  5) numer we właściwym rejestrze, jeżeli został nadany;  6) datę wpisania do wykazu ISAC;  7) datę wykreślenia z wykazu ISAC;  8) informację o korzystaniu przez ISAC z systemu teleinformatycznego, o którym mowa w art. 46.  4. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu następuje na wniosek podmiotu prowadzącego ISAC po uzyskaniu pozytywnej opinii wszystkich organów właściwych określonych w art. 41. Wniosek zawiera dane, o których mowa w ust. 3 pkt 1-5.  5. Zmiana danych w wykazie ISAC następuje na wniosek podmiotu prowadzącego ISAC, złożony nie później niż w terminie 6 miesięcy od zmiany tych danych, lub z urzędu.  6. Wnioski, o których mowa w ust. 4 i 5, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.  7. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC jest czynnością materialno-techniczną.  8. Wykaz ISAC jest publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.  9. ISAC współpracują z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów”.  10. ISAC przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.  11. W razie stwierdzenia, że działalność ISAC jest niezgodna z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa, minister właściwy do spraw informatyzacji, w zależności od rodzaju i stopnia stwierdzonych nieprawidłowości, może wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości w określonym terminie lub wykreślić ISAC z wykazu.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa.  ISAC (centrum wymiany i analiz informacji), tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o cyberzagrożeniach i podatnościach oraz wymiana informacji o najlepszych praktykach. |
|  | Art. 26 | w art. 26:  a) ust 2 otrzymuje brzmienie:  „2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek podmiotów krajowego systemu cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.”,  b) w ust. 3 w pkt 16 kropkę zastępuje się średnikiem i dodaje się pkt 17-21 w brzmieniu:  „17) gromadzenie informacji dotyczących cyberzagrożeń podatności i incydentów;  18) przygotowywanie na zlecenie Pełnomocnika i Kolegium analiz w zakresie cyberzagrożeń, podatności i incydentów;  19) przygotowywanie na zlecenie Pełnomocnika analiz skutków incydentów oraz przebiegu obsługi incydentów;  20) przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa;  21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności przez:  a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami,  b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.”,  c) w ust. 4 wyrazy „sektorowymi zespołami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowymi.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa.  Wskazane tu zostały nowe zadania wykonywane przez zespoły reagowania na incydenty komputerowe. |
|  | Art.26 i art. 49 | użyte w art. 26 w ust. 3 w pkt 16 oraz w art. 49 w ust. 3 w pkt 2 w różnej liczbie i różnym przypadku, wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji” zastępuje się wyrazem „ ENISA”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Drobna zmiana redakcyjna związana ze zdefiniowaniem ENISY. |
|  | Art. 32 ust. 4 | art. 32 ust. 4 otrzymuje brzmienie:  „4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotów krajowego systemu cyberbezpieczeństwa mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis stanowi to podstawę do wymiany informacji między CSIRT-ami poziomu krajowego a CSIRT-ami sektorowymi. |
|  | Art. 33 ust. 1a | w art. 33 po ust. 1 dodaje się ust. 1a w brzmieniu:  „1a. Badanie, o którym mowa w ust. 1 przeprowadza się także na wniosek Przewodniczącego Kolegium lub Pełnomocnika, do właściwego zespołu CSIRT, celem weryfikacji informacji będących w dyspozycji Kolegium, dotyczących możliwych podatności.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten rozszerza uprawnienia przewodniczącego Kolegium i Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, dając im większą swobodę działania. |
|  | Art. 34 ust. 1 | art. 34 ust. 1 otrzymuje brzmienie:  „1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy oraz SOC współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Określone w nim zostały zasady współpracy między organami krajowego systemu cyberbezpieczeństwa a organami ścigania. |
|  | Art. 36 | w art. 36:  a) ust. 2 otrzymuje brzmienie:  „2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Pełnomocnika, ministra właściwego do spraw informatyzacji oraz Rządowego Centrum Bezpieczeństwa.”,  b) ust. 6 otrzymuje brzmienie:  „6. Dyrektor Rządowego Centrum Bezpieczeństwa na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1, zawiadamia niezwłocznie członków Zespołu i Pełnomocnika o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten reguluje kwestie związane z udziałem Rządowego Centrum Bezpieczeństwa w sprawach krajowego systemu cyberbezpieczeństwa. |
|  | Art. 39 | w art. 39:  a) użyte w ust. 1-3 i ust. 5-9, w różnej liczbie i różnym przypadku wyrazy ,,sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami ,,CSIRT sektorowy”,  b) w ust. 3 pkt 2 otrzymuje brzmienie:  ,,2) dotyczące telekomunikacyjnych urządzeń końcowych;”, | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsze zmiany związane są z objęciem sektora telekomunikacji ustawą o krajowym systemie cyberbezpieczeństwa. |
|  | Art. 40 | użyte w art. 40 w różnej liczbie i różnym przypadku wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Zmiana wynika z przyjęcia nowego nazewnictwa w tej dziedzinie. |
|  | Art. 42 ust. 8 | w art. 42 w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji” zastępuje się wyrazami „ENISA”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Zmiana wynika z wprowadzenia wcześniej skrótu „Enisa”. |
|  | Art. 44 | w art. 44:  a) ust. 1 otrzymuje brzmienie:  „1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do ustawy, do którego zadań należy:  1) przyjmowanie zgłoszeń o incydentach;  2) reagowanie na incydenty;  3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;  4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;  5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymiana informacji o cyberzagrożeniach;  6) współpraca z CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.”,  b) po ust. 1 dodaje się ust. 1a w brzmieniu:  „1a. CSIRT sektorowy może, w szczególności:  1) zapewniać dynamiczną analizę ryzyka i incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń;  2) koordynować, w ramach sektora lub podesktora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które ich dotyczą;  3) wspierać w uzgodnieniu z operatorem usługi kluczowej wykonywanie przez niego obowiązków określonych w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13  4) zwrócić się do CSIRT NASK, CSIRT GOV, CSIRT MON o wystąpienie z wnioskiem o którym mowa w art 42 ust. 1 pkt 7.”,  c) po ust. 4 dodaje się ust. 5 i 6 w brzmieniu:  „5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadań CSIRT sektorowego jednostkom podległym lub nadzorowanym.  6. W przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5, organ właściwy może, po zasięgnięciu opinii Pełnomocnika, powierzyć realizację zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), oraz określić szczegółowy zakres realizowanych przez niego zadań, biorąc pod uwagę:  1) wymóg posiadania przez ten podmiot przygotowania technicznego i przeszkolonego personelu oraz doświadczenia w zakresie reagowania na incydenty, analizowania incydentów poważnych, wyszukiwania powiązań pomiędzy incydentami oraz opracowywania wniosków z obsługi incydentu;  2) konieczność współpracy tego podmiotu z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV;  3) poziom bezpieczeństwa systemów informacyjnych i liczbę podmiotów w danym sektorze oraz incydenty, które w nim wystąpiły.”;  7. W budżecie państwa tworzy się rezerwę celową na finansowanie utworzenia oraz funkcjonowania CSIRT Sektorowych. Dysponentem rezerwy celowej jest minister właściwy do spraw informatyzacji  8. Organ właściwy do spraw cyberbezpieczeństwa raz w roku przedkłada Pełnomocnikowi sprawozdanie z utworzenia i funkcjonowania CSIRT sektorowego.” | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Zmiany te wynikają z nowej roli CSIRT-ów sektorowych.  Nazwa sektorowego zespołu cyberbezpieczeństwa została zmieniona na CSIRT sektorowy. W przeciwieństwie do dotychczasowego, fakultatywnego trybu ustanawiania zespołu, w projekcie przewidziano obowiązek ustanowienia CSIRT sektorowego dla danego sektora lub podsektora przez organ właściwy.  CSIRT sektorowy będzie odpowiadał za przyjmowanie zgłoszeń o incydentach w sektorze lub podsektorze, dla którego został ustanowiony, a także za reagowanie na zgłoszone incydenty. Zakres obowiązków zostanie więc poszerzony - obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi kluczowej w reagowaniu na incydenty. CSIRT sektorowy będzie również dokonywał dynamicznej analizy ryzyka i incydentów jak również gromadził informacje o cyberzagrożeniach. |
|  | Art. 46 | w art. 46:  a) ust. 2 otrzymuje brzmienie:  „2. Pełnomocnik, CSIRT MON, CSIRT NASK, CSIRT GOV korzystają z systemu teleinformatycznego, o którym mowa w ust. 1.”,  b) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:  „2a. CSIRT sektorowe i Prezes Urzędu Komunikacji Elektronicznej korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości.  2b. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2 i 2a, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  W związku z wprowadzeniem nowego systemu informatycznego usprawniającego działania krajowego systemu cyberbezpieczeństwa konieczne było dodanie przepisów związanych z jego wykorzystaniem. |
|  | Tytuł rozdziału 11 | tytuł rozdziału 11 otrzymuje brzmienie:  „Nadzór i kontrola” | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. |
|  | Art. 53 ust. 1 pkt 1 | w art. 53 w ust. 1 pkt 1 otrzymuje brzmienie:  „1) minister właściwy do spraw informatyzacji w zakresie spełniania przez SOC wymogów, o których mowa w art. 14 ust. 3-6;”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejsza zmiana związana jest z wprowadzeniem SOC-ów do ustawy o krajowym systemie cyberbezpieczeństwa. |
|  | Art. 59B | 1. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:  1) ministra właściwego do spraw informatyzacji;  2) Polskie Centrum Akredytacji;  3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;  4) dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje wyroby procesowi oceny zgodności zgodnie z ustawą.  2. Nadzór nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa w zakresie oceny zgodności sprawuje minister właściwy do spraw informatyzacji. | Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.  W punkcie 4 wskazany jest również wyraźnie dobrowolność poddania swoich wyrobów ocenie zgodności.  Ust. 2 wskazuje wyraźnie organ nadzoru nad systemem certyfikacji cyberbezpieczeństwa tj. ministra właściwego do spraw informatyzacji. Kwestia ta jest następnie uszczegóławiana w kolejnych przepisach. |
|  | Art. 59 e-g | Art. 59e. Rada Ministrów może określić, w drodze rozporządzenia, krajowy program certyfikacji cyberbezpieczeństwa, uwzględniając konieczność opracowania zasad postępowań certyfikacyjnych produktów ICT, usług ICT lub procesów ICT zgodnie z aktualną wiedzą naukowo-techniczną oraz zwiększenie cyberbezpieczeństwa w sektorze przedsiębiorstw.  Art. 59f. 1.Krajowy program certyfikacji cyberbezpieczeństwa o którym mowa w art. 59e, wskazuje jeden lub więcej krajowych poziomów uzasadnienia zaufania produktów ICT, usług ICT lub procesów ICT:  1) podstawowy;  2) istotny;  3) wysoki.  2. Krajowy poziom uzasadnienia zaufania:  1) podstawowy - potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa lub wydana została krajowa deklaracja zgodności, spełniają odpowiadające im wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków;  2) istotny - potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk wystąpienia incydentów i cyberataków przeprowadzanych przez osoby dysponujące niezaawansowanym sprzętem oraz podstawowymi umiejętnościami w zakresie przełamywania zabezpieczeń systemów informacyjnych;  3) wysoki - potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach w zakresie przełamywania zabezpieczeń systemów informacyjnych i dysponujące zawansowanym sprzętem.  Art. 59g. Krajowy program certyfikacji cyberbezpieczeństwa o którym mowa w art. 59e, zawiera w szczególności:  1) przedmiot i zakres programu certyfikacji, w tym rodzaj lub kategorie objętych danym programem produktów ICT, usług ICT lub procesów ICT;  2) opis celu programu i tego, jak wybrane normy, metody oceny i krajowe poziomy uzasadnienia zaufania odpowiadają potrzebom przewidywanych użytkowników programu;  3) wskazanie, czy w ramach systemu dozwolone jest wydanie deklaracji zgodności;  4) szczegółowe lub dodatkowe wymogi, którym podlegają jednostki oceniające zgodność w celu zagwarantowania ich kwalifikacji technicznych odnośnie do oceny wymogów cyberbezpieczeństwa;  5) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte cele w zakresie cyberbezpieczeństwa;  6) niezbędne do celów certyfikacji informacje, które wnioskodawca ma dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność;  7) w przypadku gdy program przewiduje stosowanie znaków lub etykiet – warunki, na jakich takie znaki lub etykiety mogą być stosowane;  8) sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymogami krajowych certyfikatów cyberbezpieczeństwa lub deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;  9) warunki wydawania, utrzymywania, kontynuowania i odnawiania krajowych certyfikatów cyberbezpieczeństwa, a także warunki rozszerzania lub ograniczenia zakresu certyfikacji;  10) skutki dla produktów ICT, usług ICT lub procesów ICT, które uzyskały certyfikację lub w przypadku których wydana została deklaracja zgodności, które nie spełniają wymogów programu;  11) sposób zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo podatności produktów ICT, usług ICT lub procesów ICT oraz sposobu postępowania z nimi;  12) instrukcje dotyczące przechowywania dokumentów przez jednostki oceniające zgodność;  13) treść i wzór graficzny krajowych certyfikatów cyberbezpieczeństwa i krajowych deklaracji zgodności okres dostępności krajowych deklaracji zgodności, dokumentacji technicznej oraz innych istotnych informacji;  14) okres ważności krajowych certyfikatów cyberbezpieczeństwa;  15) sposób udostępniania informacji na temat krajowych certyfikatów cyberbezpieczeństwa, które zostały wydane, zmienione lub cofnięte w ramach programów;  16) sposób dostarczania i aktualizowania dodatkowych informacji na temat cyberbezpieczeństwa przez dostawców sprzętu lub oprogramowania zgodnie z art. 59v. | Akt o cyberbezpieczeństwie pozwala również Państwom Członkowskim na tworzenie krajowych programów certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami.  To narzędzie pozwoli na rozwój rynku certyfikacji oraz umożliwi nam reagowanie na cyberzagrożenia w obszarach, które nie będą zagospodarowane przez Unie Europejską. Przyjęte przepisy są jak najbardziej zbliżone do przepisów aktów o cyberbezpieczeństwie opisujących europejskie programy certyfikacji cyberbezpieczeństwa. Dzięki temu będziemy mogli również stosunkowo łatwo przenieść wykorzystane przez nas rozwiązania na poziom europejski o ile pojawi się taka potrzeba.  Celem krajowych programów certyfikacji cyberbezpieczeństwa jest zapewnienie, by produkty ICT, usługi ICT i procesy ICT certyfikowane zgodnie z takimi programami spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT w niniejszym rozporządzeniu. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo trudne. Zwłaszcza, że mówimy tu o tak różnych przedmiotach jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład poprzez odesłanie do norm lub specyfikacji technicznych, w przypadku gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów zapewni skuteczność tych programów. Trzeba wskazać, że ta różnorodność wpływa na wszelkie aspekty tych programów np. w przypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady poprzez jego aktualizacje podczas gdy wykrycie określonej podatności w przenośnej pamięci usb może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w programie może wymagać zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.  W związku z tym minister właściwy do spraw informatyzacji powinien mieć swobodę opracowywania takiego programu. Następnie przygotowany program będzie przyjmowany w drodze rozporządzenia Rady Ministrów. Zapewni to odpowiednią rangę takiego programu oraz pozwoli wypowiedzieć się o nim wszystkim zainteresowanym podmiotom.  Projektowane art. 59 f-g wyznaczają elementy krajowych programów certyfikacyjnych oraz wskazują poziomy uzasadnienia zaufania do których będą odwoływać się certyfikaty. Przepisy te zostały przygotowane na wzór odpowiednich przepisów aktu o cyberbezpieczeństwie przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania jakie musi spełniać produkt by uzyskać certyfikat określonego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Dzięki temu możliwa będzie promocja krajowych programów certyfikacyjnych w całej Unii Europejskiej i stosunkowo łatwe przenoszenie ich na poziom europejski. Ponadto takie rozwiązanie zapewni porównywalność certyfikatów krajowych z dokumentami z innych państwach członkowskich oraz sprawi, że certyfikaty będą bardziej czytelne dla zagranicznych klientów. |
|  | Art. 59j | Art. 59j. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności.  2. Ocena zgodności jest dobrowolna.  3. Warunki przeprowadzania oceny zgodności określają europejskie lub krajowe programy certyfikacji cyberbezpieczeństwa. | Ten przepis wskazuje możliwość poddawania produktów, usług i procesów ICT ocenie zgodności. Ma on dwojaki cel wskazuje ogólną zasadę dotyczącą poddawania tych wyrobów ocenie zgodności oraz wskazuje, że warunki przeprowadzania tej oceny określają zarówno europejskie jak i krajowe programy certyfikacji cyberbezieczeństwa.  Wyraźne odwołanie do tych programów jest konieczne by nie powstały wątpliwości związane z tym gdzie określone są owe warunki.  Uwzględnienie w ust. 3 krajowych programów wynika z wprowadzenia przepisów, które umożliwią tworzenie takich dokumentów w ramach krajowego porządku prawnego. |
|  | Art. 59k | Art. 59k. 1. Wniosek o certyfikację produktu ICT, usługi ICT lub procesu ICT składa jego dostawca do jednostki oceniającej zgodność.  2. Wniosek o certyfikację zawiera co najmniej:  1) nazwę albo imię i nazwisko wnioskującego oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;  2) informacje potwierdzające spełnianie kryteriów certyfikacji;  3) wskazanie zakresu wnioskowanej certyfikacji.  3. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów certyfikacji.  4. Wniosek składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub osobistym. | Przepis ten reguluje formalności związane z procesem certyfikacji. Określone w nim zostały szczegóły związane z wnioskiem o certyfikację.  Wskazuje on wyraźnie przedsiębiorcy ubiegającemu się o certyfikację jakie dokładnie informacje musi przekazać by pomyślnie zakończyć proces certyfikacji. Eliminuje to ewentualne wątpliwości w tym zakresie.  Wskazane też zostało kto może taki wniosek złożyć.  To doprecyzowanie zapewni sprawny przebieg procesów certyfikacyjnych. |
|  | Art. 59n | Art. 59n. Pozytywny wynik certyfikacji stanowi podstawę do wydania certyfikatu. | Przepis ten wskazuje podstawę do wydania certyfikatu. Jest to kolejny przepis doprecyzowujący kwestie wydawania certyfikatu. Precyzuje on, że pozytywny wynik certyfikacji jest niezbędny do wydania certyfikatu. |
|  | Art. 59v | Art. 59v. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa lub produktów ICT, usług ICT lub procesów IT dla których została wydana krajowa deklaracja zgodności udostępnia publicznie dodatkowe informacje zawierające:  1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT;  2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;  3) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;  4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatnościach związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa.  2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności. | Przepis ten nakłada na przedsiębiorców, którzy uzyskali certyfikację w ramach krajowych programów certyfikacyjnych analogiczne obowiązki jak te spoczywające na tych, którzy podjęli działania w ramach europejskich programów certyfikacyjnych ( art. 55 aktu o cyberbezpieczeństwie).  Chcemy by krajowe i europejskie programy były do siebie jak najbardziej zbliżone oraz gwarantowały analogiczne poziomy cyberbezpieczeństwa. Przekazywanie danych użytkownikom produktów jest bardzo istotnym elementem zapewniającym cyberbezpieczeństwo. Użytkownicy, by prawidłowo korzystać z programów, potrzebują informacji o sposobie korzystania z udostępnionych im wyrobów. Brak tego przepisu prowadziłby do sytuacji w której użytkownicy produktów certyfikowanych w ramach krajowych programów certyfikacyjnych byliby w gorszej sytuacji od tych korzystających z produktów certyfikowanych w ramach programów europejskich. By uniknąć takiej sytuacji oraz by zwiększyć poziom cyberbezpieczeństwo w sektorze przedsiębiorstw wprowadziliśmy niniejszy przepis. |
|  | Art. 59w | Art. 59w. 1. Minister właściwy do spraw informatyzacji pobiera opłatę za zatwierdzenie certyfikatu, o którym mowa w art. 59o ust. 1.  2. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wysokość opłat za zatwierdzanie certyfikatu, biorąc pod uwagę zakres certyfikacji, przewidywany przebieg i długość postępowania w sprawie zatwierdzenia certyfikatu oraz stopień skomplikowania wykonywanych czynności.  3. Maksymalna wysokość opłaty nie może przekroczyć czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o zatwierdzenie certyfikatu, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2020 r. poz. 1222).  4. Opłata stanowi dochód budżetu państwa. | W związku z przyjęciem modelu w którym certyfikaty odwołujące się do poziomu zaufania „wysoki” muszą być dodatkowo zatwierdzane przez ministra właściwego do spraw informatyzacji konieczne jest zapewnienie środków na prowadzenie tego typu działalności.  W związku z tym wprowadzono niniejszy przepis, który zmniejszy obciążenia finansowe spoczywające na administracji publicznej w związku z implementacją przepisów CSA.  Przyjęte w przepisie mechanizm wyznaczający maksymalna opłatę zapewnia, że przepis ten nie spowoduje nadmiernych obciążeń dla przedsiębiorców biorących udział w procesie. |
|  | Art. 59 zd-zf | Rozdział 11b  Operator sieci komunikacji strategicznej  Art. 59zd. 1. W celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji, tworzy się sieć komunikacji strategicznej.  2. Operatorem sieci komunikacji strategicznej jest jednoosobowa spółka Skarbu Państwa, będąca przedsiębiorcą telekomunikacyjnym, posiadająca infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 1, oraz środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej, wyznaczona przez Prezesa Rady Ministrów w drodze zarządzenia.  3. Operator sieci komunikacji strategicznej świadczy usługi telekomunikacyjne w celu realizacji zadań, o których mowa w ust. 1, oraz może świadczyć inne usługi w zakresie realizacji tych zadań, jeżeli podmioty, o których mowa w ust. 4, zgłoszą operatorowi sieci komunikacji strategicznej wniosek o ich realizację, i spełniony jest jeden z następujących warunków:  1) w związku z ich realizacją konieczne jest nadanie związanej z nimi dokumentacji klauzuli, zgodnie z przepisami o ochronie informacji niejawnych, lub  2) wymaga tego istotny interes bezpieczeństwa państwa, ze szczególnym uwzględnieniem cyberbezpieczeństwa państwa, lub  3) wymaga tego ochrona bezpieczeństwa publicznego, lub  4) muszą im towarzyszyć szczególne środki bezpieczeństwa.  4. Operator sieci komunikacji strategicznej może świadczyć usługi, o których mowa w ust. 1, dla:  1) Kancelarii Prezydenta RP;  2) Kancelarii Sejmu;  3) Kancelarii Senatu;  4) Kancelarii Prezesa Rady Ministrów;  5) Biura Bezpieczeństwa Narodowego;  6) urzędów obsługujących organy administracji rządowej, wykonujące zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności Państwa, ochrony granicy Państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sądownictwa i prokuratury;  7) Dowództwa Rodzajów Sił Zbrojnych i ich jednostek organizacyjnych;  8) Żandarmerii Wojskowej;  9) instytucji i przedsiębiorców, wykonujących na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa.  5. Ze względu na ważny interes Państwa, w szczególności na konieczność zapewnienia ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa, operator sieci komunikacji strategicznej może świadczyć usługi telekomunikacyjne także podmiotom innym niż wskazane w ust. 4, za zgodą Prezesa Rady Ministrów.  Art. 59ze. Operator sieci komunikacji strategicznej może świadczyć usługi telekomunikacyjne w oparciu o zasoby częstotliwości, o których mowa w art. 1544 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.  Art. 59zf. 1. Operator telekomunikacyjny jest obowiązany zapewnić odpłatnie dostęp do elementów sieci telekomunikacyjnej na potrzeby komunikacji strategicznej realizowanej przez operatora sieci komunikacji strategicznej.  2. Warunki dostępu do elementów sieci telekomunikacyjnych i związanej z tym współpracy ustala się w umowie o dostępie, zawartej na piśmie pod rygorem nieważności.  3. W przypadku niezawarcia umowy o dostępie do elementów sieci telekomunikacyjnej w terminie 30 dni od dnia złożenia wniosku o taki dostęp przez operatora sieci komunikacji strategicznej Prezes UKE wydaje decyzję w sprawie dostępu do elementów sieci telekomunikacyjnej.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  W ramach dodawanego rozdziału 11b w proponowanym art. 59zd przedstawione zostały przepisy dotyczące utworzenia sieci komunikacji strategicznej oraz przewidujące powierzenie roli operatora tej sieci spółce kapitałowej, w której Skarb Państwa posiada udziały albo akcje reprezentujące co najmniej 51% kapitału zakładowego, będąca przedsiębiorcą telekomunikacyjnym, posiadająca infrastrukturę telekomunikacyjną niezbędną do określony w przepisach realizacji zadań, środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej, wyznaczona przez Prezesa Rady Ministrów w drodze zarządzenia. Głównym zadaniem operatora sieci komunikacji strategicznej będzie zapewnienie bezpiecznej i niezawodnej łączności dla wymienionych w art. 59zd ust. 4 podmiotów i służb.  Właściwy operator telekomunikacyjny będzie zobowiązany zapewnić odpłatnie dostęp do elementów sieci telekomunikacyjnej na potrzeby komunikacji strategicznej realizowanej przez operatora sieci komunikacji strategicznej. Warunki dostępu do sieci telekomunikacyjnej zostaną określone w umowie o dostępie do elementów sieci telekomunikacyjnej. Jeżeli nie zostanie ona zawarta, to na wniosek operatora sieci komunikacji strategicznej Prezes UKE wyda decyzję w sprawie dostępu do elementów sieci telekomunikacyjnej. |
|  | Art. 62 ust. 1 pkt 7 | w art. 62 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:  „7) wydawanie ostrzeżeń.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Niniejszy przepis daje dodatkowe narzędzie Pełnomocnikowi do Spraw Cyberbezpieczeństwa. |
|  | Art. 62a-62b | ,,Art. 62a. 1. W celu zapewnienia możliwości realizacji zadań wymagających specjalistycznej wiedzy z zakresu cyberbezpieczeństwa może być przyznane dodatkowe wynagrodzenie dla 20 osób wykonujących te zadania posiadających doświadczenie zawodowe z zakresu cyberbezpieczeństwa, zatrudnionych lub pełniących służbę w zespołach CSIRT GOV, CSIRT NASK, CSIRT MON lub Agencji Bezpieczeństwa Wewnętrznego realizującej zadania CSIRT GOV, a także w urzędzie obsługującym Pełnomocnika.  2. Zadania, o których mowa w ust. 1, polegają na przygotowywaniu:  1) analiz, na zlecenie Pełnomocnika, w zakresie wpływu cyberzagrożeń, podatności i incydentów na krajowy system cyberbezpieczeństwa, w tym także analiz informacji otrzymywanych w ramach współpracy sojuszniczej i międzynarodowej;  2) analiz, na zlecenie Kolegium, związanych z postępowaniem, o którym mowa w art. 66a;  3) rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa.  3. Dodatkowe wynagrodzenie, o którym mowa w ust. 1, przyznaje:  a) dla osób zatrudnionych w urzędzie obsługującym Pełnomocnika - dyrektor generalny urzędu po uzyskaniu pozytywnej opinii Pełnomocnika;  b) dla osób zatrudnionych lub pełniących służbę w zespole CSIRT GOV, CSIRT NASK, CSIRT MON lub Agencji Bezpieczeństwa Wewnętrznego realizującej zadania CSIRT GOV – dyrektor jednostki organizacyjnej w ramach której powołano zespół CSIRT GOV, CSIRT NASK, CSIRT MON po uzyskaniu pozytywnej opinii Pełnomocnika i organu nadzorującego.  4. Dodatkowe wynagrodzenie nie może przekroczyć piętnastokrotności wynagrodzenia minimalnego o którym mowa w ustawie .z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę Dz.U. z 2020 r. poz. 2207.  5. Rada Ministrów określi, w drodze rozporządzenia wysokość stawki dodatkowego wynagrodzenia osób, o których mowa w ust. 1, biorąc pod uwagę stawki rynkowe oraz konieczność zapewnienia skutecznej realizacji zadań o których mowa w ust. 2.  Art. 62b 1. Pełnomocnik może wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.  2. Rekomendacje Pełnomocnika są publikowane na stronie internetowej obsługującego go urzędu.  3. Ogłoszenie o publikacji rekomendacji Pełnomocnik zamieszcza się w Monitorze Polskim. Ogłoszenie zawiera adres strony internetowej zawierającej treść zalecenia.  4. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.  5. Podmiot krajowego systemu cyberbezpieczeństwa, uwzględnia rekomendacje w zarządzaniu ryzykiem.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Artykuł 62a pozwoli na zatrudnienie w zespołach CSIRT poziomu krajowego i w urzędzie obsługującym Pełnomocnika specjalistów z zakresu cyberbezpieczeństwa na stawkach rynkowych. Pozwoli to na skuteczniejszą reakcję na incydent a także na wykonywanie specjalistycznych analiz na rzecz Pełnomocnika i Kolegium.  Artykuł 62b umożliwi wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Będą one publikowane na stronie internetowej urzędu obsługującego Pełnomocnika a ogłoszenie o publikacji zostanie zawarte w Monitorze Polskim. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej a także inne zbiory dobrych praktyk. Rekomendacje będą niewiążące, lecz podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić je w ramach procesu zarządzania ryzykiem. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Jednakże uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne zabezpieczenia. |
|  | Art. 65 ust. 1 pkt. 7 | 7) decyzji o ocenie ryzyka dostawcy sprzętu lub oprogramowania.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten wyznacza nowe zadanie Kolegium wynikające z przyjęcia Toolboxa 5G. |
|  | Art. 66 ust. 4 | 4. W posiedzeniach Kolegium uczestniczą również:  1) Dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;  2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;  3) Szef Agencji Wywiadu albo jego zastępca;  4) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;  5) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;  6) Szef Służby Wywiadu Wojskowego albo jego zastępca;  7) Dyrektor Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego albo jego zastępca.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Artykuł ten uzupełnia skład Kolegium do Spraw Cyberbezpieczeństwa o szefów służb co przyczyni się do zwiększenia roli Kolegium oraz lepszego przepływu informacji między organami działającymi w sprawach cyberbezpieczeństwa. |
|  | Art. 66a-66d | „Art. 66a. 1. Minister właściwy do spraw informatyzacji może z urzędu lub na wniosek Przewodniczącego Kolegium wszcząć postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dostawcy sprzętu lub oprogramowania, które wykorzystują:  1) podmioty krajowego systemu cyberbezpieczeństwa;  2) przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;  3) właściciele i posiadacze obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2020 r. poz. 1856);  4) przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców  - zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka”.  2. Dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT.  3. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się przepisy Kodeksu postępowania administracyjnego, o ile ustawa nie stanowi inaczej.  4. Wniosek Przewodniczącego Kolegium o wszczęcie postępowania w sprawie uznania za dostawcę wysokiego ryzyka zawiera:  1) dane identyfikujące dostawcę sprzętu lub oprogramowania;  2) wskazanie zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy uwzględnianych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka;  3) opinię Kolegium w zakresie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka dla podmiotów określonych w ust. 1 pkt 1-4.  5. W przypadku wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka z urzędu, minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię.  6. Opinia Kolegium zawiera analizę:  1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego;  2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:  a) stopnia i rodzaju powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,  b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,  c) struktury własnościowej dostawcy sprzętu lub oprogramowania,  d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;  3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.5.2019, str. 1-12 z późn. zm.);  4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;  5) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt. 1-4, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;  6) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.  7. Procedura sporządzenia opinii przebiega w następujący sposób:  1) Przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka. W skład Zespołu wchodzą przedstawiciele członków Kolegium wskazanych przez Przewodniczącego Kolegium;  2) każdy członek Kolegium przygotowuje stanowisko w obszarze swojej właściwości w oparciu o zakres analizy określony w ust. 6, które następnie przekazuje zespołowi, o którym mowa w pkt 1;  3) Zespół przedstawia Przewodniczącemu Kolegium projekt opinii;  4) przyjęcie opinii następuje na posiedzeniu Kolegium;  5) uzgodnioną opinię Przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.  8. Minister właściwy do spraw informatyzacji uznaje w drodze decyzji dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego.  9. Decyzja zawiera:  1) dane identyfikujące dostawcę wysokiego ryzyka;  2) wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.  10. Minister właściwy do spraw informatyzacji może odstąpić od sporządzenia uzasadnienia decyzji, o której mowa w ust. 8, w części dotyczącej uzasadnienia faktycznego, jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego.  11. Minister właściwy do spraw informatyzacji publikuje informacje zawarte w decyzji, o której mowa w ust. 8, w formie ogłoszenia w Dzienniku Urzędowym Monitor Polski, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.  12. Decyzja, o której mowa w ust. 8, podlega natychmiastowej wykonalności.  Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 8, podmioty, o których mowa w art. 66a ust. 1 pkt 1-4:  1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;  2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia opublikowania informacji o decyzji, o której mowa w art. 66a ust. 8 z zastrzeżeniem ust. 2.  2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.  3. Podmioty o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawa – Prawo zamówień publicznych, nie dokonują zamówień sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 8.  Art. 66c. 1. Podmioty krajowego systemu cyberbezpieczeństwa oraz przedsiębiorcy telekomunikacyjnie są zobowiązani przekazać informacje na wniosek uprawnionych organów o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją.  2. Uprawnionymi organami do żądania informacji, o których mowa w ust. 1, są wobec:  1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa;  2) SOC – minister właściwy do spraw informatyzacji;  3) przedsiębiorców telekomunikacyjnych – Prezes UKE;  4) podmiotów publicznych – właściwe organy nadzorcze.  3. Wniosek zawiera:  1) wskazanie podmiotu obowiązanego do przekazania informacji;  2) datę;  3) wskazanie żądanych informacji;  4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;  5) uzasadnienie.  4. Pełnomocnik może zwrócić się do organów, o których mowa w ust. 2, o zwrócenie się o informacje, o których mowa w ust. 1.  Art. 66d. 1. Sąd administracyjny rozpatruje skargę na decyzje, o których mowa w art. 66a ust. 8, na posiedzeniu niejawnym.  2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych.  3. Sąd administracyjny nie może wstrzymać wykonalności decyzji, o której mowa w art. 66a ust. 8, po wniesieniu skargi na tą decyzję.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  W art. 66a została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W rozumieniu tego artykułu dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Postępowanie nie będzie dotyczyło wszystkich produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez:  1) podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych, czy podmioty publiczne (ok. 4000 podmiotów);  2) przedsiębiorców telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (ok. 100 podmiotów);  3) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej w uzasadnieniu zwani operatorami infrastruktury krytycznej (ok. 130 podmiotów);  4) przedsiębiorców o szczególnym znaczeniu gospodarczo obronnym.  Podmioty te są szczególnie ważne dla zapewnienia społeczno-ekonomicznego bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu w trakcie świadczenia usług na rzecz państwa i obywateli.  Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie miał zastosowanie Kodeks postępowania administracyjnego z zastrzeżeniem przepisów wskazanych w tej nowelizacji. Dzięki temu dostawca sprzętu lub oprogramowania będzie miał szanse obrony swoich praw. Decyzja ministra właściwego do spraw informatyzacji będzie miała formę decyzji administracyjnej, co pozwoli dostawcy na składanie środków odwoławczych przewidzianych w kodeksie oraz złożenie skargi na decyzję administracyjną do Wojewódzkiego Sądu Administracyjnego.  Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Przewodniczącego Kolegium. Gdy postępowanie zostanie wszczęte z urzędu to minister właściwy ds. informatyzacji będzie zobowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra.  Wniosek Przewodniczącego Kolegium o wszczęcie postępowania będzie zawierał: dane identyfikujące dostawcę sprzętu lub oprogramowania, a także wskazanie zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy uwzględnianych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. Immanentnym elementem wniosku będzie także opinia Kolegium w zakresie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka dla podmiotów. W takim przypadku Minister nie będzie zasięgał opinii Kolegium, ponieważ otrzyma ją we wniosku.  Art. 66a ust. 6 zawiera wskazanie elementów analizy która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G ). W ramach opinii będzie zawarta analiza dostawcy sprzętu lub oprogramowania na podstawie aspektów technicznych i nietechnicznych. Analizowane będą powiązania dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego oraz powiązania z podmiotami wobec których Unia Europejska zastosowała sankcje za cyberataki. Innym nietechnicznym aspektem będzie analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania.  Do technicznych aspektów opinii należy analiza:  1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;  2) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów o których mowa w ust. 1 pkt. 1-4 oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;  3) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.  Podkreślić należy, że nie jest możliwe ograniczenie się w analizie dostawcy sprzętu lub oprogramowania wyłącznie do aspektów technicznych oferowanych przez niego produktów ICT, usług ICT czy procesów ICT. Postęp technologiczny umożliwił nie tylko poprawę jakości komunikacji ale także umożliwił nowe formy ingerencji państw trzecich w bezpieczeństwo narodowe. Coraz więcej urządzeń jest stale podłączonych do globalnej sieci, co powoduje że w każdej chwili jest przesyłana ogromna ilość danych. Dla służb wywiadowczych obcych państw są to potencjalnie potężne zasoby informacyjne, które mogą zostać wykorzystane przeciwko Polsce. Ponadto dostęp do urządzeń stale podłączonych do sieci poprzez ukryte (lub celowo zaprojektowane) podatności mógłby skutkować przejęciem kontroli nad znaczną liczbą urządzeń używanych przez podmioty krajowego systemu cyberbezpieczeństwa, czy operatorów infrastruktury krytycznej. W konsekwencji niezbędne jest aby istniała prawna formuła zidentyfikowania dostawcy wysokiego ryzyka i ograniczenia używania oferowanego przez niego sprzętu lub oprogramowania. |
|  | Art.. 67a-67b | Art. 67a. 1. Pełnomocnik w przypadku uzyskania informacji wskazującej na możliwość wystąpienia incydentu krytycznego, może wydać ostrzeżenie w celu poinformowania o cyberzagrożeniu:  1) podmiotów, o których mowa w art. 4 pkt 1–16;  2) przedsiębiorców telekomunikacyjnych;  3) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;  4) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców;  5) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2020 r. poz. 794);  6) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.).  2. Pełnomocnik, przed wydaniem ostrzeżenia, przeprowadza we współpracy z Zespołem analizę uzasadniającą jego wydanie obejmującą:  1) istotność cyberzagrożenia;  2) prawdopodobieństwo wystąpienia incydentu krytycznego;  3) rodzaje ryzyk;  4) skuteczność alternatywnych metod zapewnienia cyberbezpieczeństwa.  3. Ostrzeżenie zawiera:  1) wskazanie rodzajów ryzyk;  2) wskazanie rodzajów podmiotów, których dotyczy;  3) zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu;  4) datę wejścia w życie;  5) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 2.  4. Pełnomocnik przeprowadza nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. W ramach przeglądu ostrzeżeń Pełnomocnik może przeprowadzić analizę, o której mowa w ust. 1. Pełnomocnik po uzyskaniu informacji o ustaniu zagrożenia wystąpienia incydentu krytycznego odwołuje ostrzeżenie.  5. Pełnomocnik publikuje:  1) informację o wydanym ostrzeżeniu, a także o odwołaniu ostrzeżenia,  2) listę wydanych i odwołanych ostrzeżeń  - na stronie podmiotowej w Biuletynie Informacji Publicznej urzędu obsługującego Pełnomocnika, a także na stronie internetowej urzędu obsługującego Pełnomocnika.  6. Jeżeli przemawia za tym interes publiczny, informacja o wydaniu ostrzeżenia może być udostępniona za pomocą środków masowego przekazu.  7. Informacja o wydaniu ostrzeżenia może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46.  8. Przez zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu krytycznego, rozumie się zalecenie:  1) przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;  2) dokonania przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością;  3) wdrożenia określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;  4) dokonania określonej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;  5) prowadzenia wzmożonego monitorowania zachowania systemu;  6) odstąpienia od korzystania z określonego sprzętu lub oprogramowania;  7) wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.  9. Operator usługi kluczowej uwzględnia wydane ostrzeżenia podczas procesu szacowania ryzyka.  Art. 67b. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może wydać polecenie zabezpieczające w stosunku do:  1) podmiotów, o których mowa w art. 4 pkt 1–16;  2) przedsiębiorców telekomunikacyjnych;  3) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;  4) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców;  5) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2020 r. poz. 794);  6) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.).  2. Polecenie zabezpieczające wydaje się w drodze decyzji administracyjnej na czas koordynacji obsługi incydentu krytycznego, nie dłużej niż na dwa lata.  3. Polecenie zabezpieczające podlega natychmiastowej wykonalności.  4. Do postępowania w sprawie o wydanie polecenia zabezpieczającego stosuje się przepisy Kodeksu postępowania administracyjnego z zastrzeżeniem przepisów niniejszej ustawy.  5. Minister właściwy do spraw informatyzacji, przed wydaniem polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, analizę uzasadniającą jego wydanie, obejmującą:  1) istotność cyberzagrożenia;  2) przewidywane skutki incydentu krytycznego;  3) rodzaje ryzyk;  4) skutki finansowe, społeczne i prawne wydania polecenia zabezpieczającego.  Analizę włącza się do akt sprawy.  6. Minister właściwy do spraw informatyzacji może odstąpić od sporządzenia uzasadnienia polecenia zabezpieczającego w części dotyczącej uzasadnienia faktycznego, jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego.  7. Minister właściwy do spraw informatyzacji publikuje informację o wydaniu i treści polecenia zabezpieczającego w Dzienniku Urzędowym ministra właściwego do spraw informatyzacji, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.  8. Polecenie zabezpieczające zawiera:  1) wskazanie rodzajów podmiotów, których dotyczy;  2) wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się;  3) datę wejścia w życie;  4) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 5.  9. Przez wskazanie określonego zachowania, które zmniejszy skutki incydentu krytycznego lub zapobiegnie jego rozprzestrzenieniu, rozumie się:  1) nakaz przeprowadzenie szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;  2) przegląd planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością;  3) polecenie zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;  4) nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;  5) polecenie wzmożonego monitorowania zachowania systemu;  6) zakaz korzystania z określonego sprzętu lub oprogramowania;  7) nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL;  8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;  9) zabezpieczenie określonych informacji, w tym dzienników systemowych;  10) wytworzenie obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepisy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zawierają dodanie dwóch specjalnych środków – ostrzeżenia oraz polecenia zabezpieczającego. Ich stosowanie będzie ograniczone do niektórych grup podmiotów gospodarki i społeczeństwa. Będą mogły być stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) lub po zaistnieniu incydentu krytycznego, w celu skoordynowania efektywnej reakcji (polecenie zabezpieczające). Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie - po przeprowadzeniu należytej oceny - może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.  Pełnomocnik będzie mógł wydać ostrzeżenie, które będzie miękkim, niewiążącym środkiem wskazującym na ryzyko związane z możliwością wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko wystąpienia tego incydentu. Instrument ten jest wzorowany na ostrzeżeniach wydawanych przez czeską Narodową Agencję Bezpieczeństwa Cybernetycznego i Informacji.  Z kolei minister właściwy do spraw informatyzacji będzie mógł wydać w formie decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Polecenie zabezpieczające będzie wydawane w sytuacji zapewnienia koordynacji reakcji na incydent krytyczny oraz konieczności ograniczenia skutków tego incydentu.  Przed wydaniem ostrzeżenia lub polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.  Zarówno ostrzeżenie jak i polecenie będą musiały zawierać:  1) wskazanie rodzajów ryzyk;  2) wskazanie rodzajów podmiotów, których dotyczy;  4) datę wejścia w życie;  5) uzasadnienie zawierające wyniki analizy.  Ostrzeżenie jako miękki środek będzie zawierało zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu. Katalog możliwych zaleceń został wskazany w art. 67a ust. 8. Z kolei polecenie zabezpieczające jako mocniejszy środek, będzie zawierało wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Katalog zachowań został wskazany w art. 67b ust. 9.  Decyzja o zastosowaniu się do ostrzeżenia przez operatorów usług kluczowych będzie należeć do nich samych, przepis jedynie zobowiązuje ich do uwzględnienia ostrzeżenia podczas procesu szacowania ryzyka. |
|  | Art. 73 ust. 2a-2c | „2a. Karze pieniężnej podlega podmiot określony w art. 66a ust. 1 pkt 1-4, który nie dostosował się do obowiązków określonych w art. 66b.  2b. Karze pieniężnej podlega podmiot, określony w art. 67b ust. 2 który nie dostosował się do polecenia zabezpieczającego.  2c. Karze pieniężnej podlega podmiot publiczny, który nie wyznaczył osób, o których mowa w art. 21.”,  d) w ust. 3:  - w pkt 9 po wyrazie „wynosi” dodaje się wyraz „do”,  - dodaje się pkt 14-16 w brzmieniu:  „14) ust. 2a wynosi:  a) w przypadku podmiotów określonych w art. 66a ust. 1 pkt 1-4, z wyjątkiem podmiotów publicznych, w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,  b) w przypadku podmiotów publicznych do 100 000 zł;  15) ust. 2b wynosi:  a) w przypadku podmiotów określonych w art. 67b ust. 2 z wyjątkiem podmiotów publicznych, w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,  b) w przypadku podmiotów publicznych do 100 000 zł;  16) ust. 2c wynosi do 10 000 zł.”; | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Wprowadzone w tych ustępach przepisy karne odnoszą się do obowiązków niezwiązanych z aktem o cyberbezpieczeństwie. |
|  | Art. 74 ust. 1 | „1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.” | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten wskazuje organ właściwy do wydawania kar. |
|  | Art. 74 ust. 1b | 1b. Karę pieniężną określoną w art. 73 ust. 2a i 2b nakłada w drodze decyzji minister właściwy do spraw informatyzacji. | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Przepis ten wskazuje organ właściwy do wydawania kar. |
|  | Załącznik 3 | Kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług  1. Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.  2. Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.  3. Zarządzanie łącznością ze urządzeniami użytkowników i przydzielanie zasobów radiowych.  4. Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.  5. Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.  6. Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.  7. Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.  8. Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.  9. Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.  10. Zabezpieczenia połączeń z innymi sieciami. | Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.  Wskazane tu zostały najważniejsze funkcji, których będą dotyczyły wcześniej wskazane rozwiązania. |