Projekt z dnia 20 stycznia 2021 r.

U S T A W A

z dnia …… 2021 r.

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369) wprowadza się następujące zmiany:

1) w art. 1:
   a) w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu:
      „1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu 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), zwanego dalej, „rozporządzeniem 2019/881”,
   b) 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;”;
2) w art. 2:
   a) po pkt 3 dodaje się pkt 3a-3d w brzmieniu:

„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”,

b) pkt 4 otrzymuje brzmienie:

„4) cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;”,

c) po pkt 4 dodaje się pkt 4a w brzmieniu:

„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;”,

d) pkt 5 otrzymuje brzmienie:

„5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”,

e) pkt 11 otrzymuje brzmienie:

„11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;”,

f) pkt 17 otrzymuje brzmienie:

„17) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku systemów informacyjnych, użytkowników takich systemów oraz innych osób;”,

g) po pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20-31:

„20) produkt ICT – element lub grupę elementów systemów informacyjnych;

21) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;

22) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;

23) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008;

24) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008;

25) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;

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;

3) użyte w art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 11 w ust. 3, w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 15 w ust. 2 w pkt 3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5, w art. 44, w art. 48 w pkt 1, w art. 49 w ust. 3, w art. 64, w art. 65 w ust. 1 w pkt 2 i 4, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa", zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy";

4) w art. 4:

a) w pkt 7 wyrazy „w art. 9 pkt 1-6, 8, 9, 11 i 12" zastępuje się wyrazami „w art. 9 pkt 1-6, 8-10",

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);",

e) pkt 16 otrzymuje brzmienie:

„16) SOC;";

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.";

6) w art. 8 w pkt 5 lit. b otrzymuje brzmienie:

„b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,";

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.”;

8) 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”;

9) 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.”;

10) 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.”;

11) 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.”;

12) 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”;

13) 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”;

14) 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”;

15) 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”;

16) 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.

17) po art. 25 dodaje się rozdział 5a w brzmieniu:

„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.";

18) 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 12 wyrazy „30 maja” zastępuje się wyrazami „31 stycznia”;
- 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.”;

19) 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 (ENISA)” zastępuje się wyrazem „ENISA”;

20) 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.”;

21) 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.”;

22) 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.”;

23) 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.”;

24) 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;”,

25) użyte w art. 40 w różnej liczbie i różnym przypadku wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”;

26) w art. 42 w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazami „ENISA”;

27) 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.”

28) 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.”;

29) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola”

30) 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;”;

31) po rozdziale 11 dodaje się rozdziały 11a i 11b w brzmieniu:

„Rozdział 11a

Krajowy system certyfikacji cyberbezpieczeństwa

Art. 59a. Krajowy system certyfikacji cyberbezpieczeństwa ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT.

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.

Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z oceną zgodności wyrobów;
2) monitorowanie wdrażania i stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;
3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59b ust. 1 pkt 3-4;
4) przeprowadzanie wzajemnego przeglądu o którym mowa art. 59 rozporządzenia 2019/881;
5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;
6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”;

7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania „wysoki”;
8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;
9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonych europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa;
10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność;
11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;
12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b-d oraz ust. 8 rozporządzenia 2019/881;
13) uczestnictwo w pracach ECCG;
14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;
15) nadzorowanie i egzekwowanie zawartych w europejskich i krajowych programach certyfikacji bezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;
16) przygotowywanie propozycji krajowego programu certyfikacji cyberbezpieczeństwa.

Art. 59d. Polskie Centrum Akredytacji sprawuje nadzór nad jednostkami oceniającymi zgodność, w zakresie spełniania przez nie wymagań, o których mowa w art. 24 ust. 3 ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544 oraz z 2020 r. poz. 1086) oraz w załączniku nr 1 do rozporządzenia 2019/881.

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.

Art. 59h. 1. Jednostka oceniająca zgodność podlega akredytacji na podstawie ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.

2. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.

3. Informacja o udzielonej akredytacji, o której mowa w ust. 1, zawiera:

1) oznaczenie podmiotu, któremu udzielono akredytacji;

2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.

4. Akredytacji udziela się na okres nie dłuższy niż 5 lat.

5. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o cofnięciu akredytacji, o której mowa w ust. 1.

6. Informacja o cofnięciu akredytacji, o której mowa w ust. 1, zawiera:

1) oznaczenie podmiotu, któremu cofnięto akredytację;

2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;

3) wskazanie daty cofnięcia akredytacji.

Art. 59i. 1. W przypadku, gdy:

1) europejski program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881,

2) krajowy program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi o których mowa w art. 59g pkt 4

- minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie zadań w ramach takich programów wyłącznie jednostkom oceniającym zgodność spełniającym te wymogi.

2. Minister właściwy do spraw informatyzacji może cofnąć, ograniczyć lub zawiesić zezwolenie, o którym mowa w ust. 1, jeśli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego albo krajowego programu certyfikacji

cyberbezpieczeństwa. Cofnięcie, ograniczenie lub zawieszenie zezwolenia, o którym mowa w ust. 1, następuje w drodze decyzji.

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.

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.

Art. 59l. Jednostka oceniająca zgodność przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jej cofnięcia.

Art. 59m. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem:

1) deklaracji zgodności - badaniom przez wytwórcę lub dostawcę, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy;
2) certyfikatu - certyfikacji przez jednostkę oceniającą zgodność, w zakresie właściwym do danego programu certyfikacji cyberbezpieczeństwa.

Art. 59n. Pozytywny wynik certyfikacji stanowi podstawę do wydania certyfikatu.

Art. 59o. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji przesyła do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:

1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania „wysoki”;
2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania „wysoki”.

2. Minister właściwy do spraw informatyzacji:

1) zatwierdza certyfikat, o którym mowa w ust. 1;
2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą lub programami, o których mowa w ust. 1;

3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego lub krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.

4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg procesu oceny zgodności.

5. Jeżeli wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, zawiera braki formalne, organ administracji publicznej wzywa organ wnioskujący do ich uzupełnienia w terminie czternastu dni od dnia doręczenia wezwania.

6. Jeżeli organ wnioskujący nie uzupełni w terminie braków formalnych wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, nie podlega rozpatrzeniu i jest zwracany organowi wnioskującemu.

7. Minister właściwy do spraw informatyzacji cofa certyfikat, jeśli jest on niezgodny z rozporządzeniem 2019/881, europejskim lub krajowym programem certyfikacji cyberbezpieczeństwa lub z ustawą.

8. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

Art. 59p 1. Dostawca, który poddał produkt ICT, usługę ICT lub proces ICT ocenie zgodności z zasadniczymi wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa i potwierdził ich zgodność, wydaje krajową deklarację zgodności.

2. Krajowa deklaracja zgodności, odwołuje się do określonych w krajowym programie certyfikacji cyberbezpieczeństwa specyfikacji technicznych, norm i procedur, w tym kontroli technicznych mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

3. Krajowa deklaracja zgodności wydawana jest wyłącznie dla produktów ICT, usług ICT lub procesów ICT odpowiadających wymaganiom dla krajowego poziomu uzasadnienia zaufania „podstawowy”.

Art. 59q. Po wydaniu deklaracji zgodności dostawca przesyłała jej kopię do ministra właściwego do spraw informatyzacji

Art. 59r. Domniemywa się, że wyrób, dla którego wydano deklarację zgodności jest zgodny z wymaganiami określonymi w obowiązujących krajowych lub europejskich programach certyfikacyjnych.

Art. 59s. W przypadku stwierdzenia, że podmiot ubiegający się o certyfikację nie spełnia kryteriów certyfikacji, jednostka oceniająca zgodność odmawia jej dokonania, wskazując brak spełnienia kryteriów certyfikacji.

Art. 59t. 1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) oznaczenie produktu ICT, usługi ICT lub procesu ICT podlegającego certyfikacji;
4) numer lub oznaczenie certyfikatu;
5) zakres certyfikacji;
6) okres, na jaki została dokonana certyfikacja;
7) wskazanie poziomu uzasadnienia zaufania określonego europejskim programie certyfikacji cyberbezpieczeństwa lub krajowego poziomu uzasadnienia zaufania określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
8) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

3. Certyfikat, wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa, odwołuje się do związanych z nim specyfikacji technicznych, norm i procedur, w tym kontroli technicznych mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

Art. 59u. 1. W okresie, na jaki został wydany certyfikat, podmiot któremu go wydano, jest obowiązany spełniać kryteria obowiązujące na dzień jego wydania.

2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji.

3. Jednostka oceniająca zgodność informuje ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu.

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.

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.

Art. 59x. Podmiot, o którym mowa w art. 59b ust. 1 pkt 3-4, na wniosek ministra właściwego do spraw informatyzacji, przedstawia informacje dotyczące:

1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;

2) funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa;

3) liczby wydanych certyfikatów w tym programów w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;

4) liczby wydanych deklaracji zgodności w tym programów w ramach których zostały wydane;

5) liczby i sposobu rozpatrzenia skarg o których mowa w art. 59za.

Art. 59y. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59b ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.

2. Do kontroli, o której mowa w ust. 1, realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców;

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Art. 59z. Przepisy art. 55-59 stosuje się odpowiednio do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa.

Art. 59za. 1. Jednostki oceniające zgodność publikują na swojej stronie internetowej informacje o procedurze postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881. Procedura postępowania ze skargami określa termin załatwienia sprawy oraz przebieg procesu rozpatrywania skargi.

2. Skargę składa się w terminie 14 dni od dnia doręczenia rozstrzygnięcia. Jednostki oceniające zgodność mogą określić dłuższy termin na złożenie skargi.

3. Skargę rozpatrują osoby, które nie brały udziału w podejmowaniu rozstrzygnięcia, którego dotyczy skarga.

4. Jednostka oceniająca zgodność na każdym etapie informuje skarżącego o stanie postępowania oraz o przysługującym mu prawie skierowania sprawy do sądu.

5. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na jednostkę oceniającą zgodność.

Art. 59zb. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na podmiot, który wydał unijną lub krajową deklarację zgodności, jeśli produkt ICT, usługa ICT lub proces ICT którego dana deklaracja dotyczy nie spełnia wymogów określonych w programie certyfikacji cyberbezpieczeństwa.

Art. 59zc. Do skarg, o których mowa w art. 59 za ust. 5 oraz art. 59zb, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.

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. 115^4 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.”;

32) w art. 62 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:
„7) wydawanie ostrzeżeń.”;

33) po art. 62 dodaje się art. 62a-62b w brzmieniu:

,,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.”;

34) w art. 65 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) decyzji o ocenie ryzyka dostawcy sprzętu lub oprogramowania.”;

35) w art. 66 ust. 4 otrzymuje brzmienie:

„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.”;

36) po art. 66 dodaje się art. 66a-66d w brzmieniu:

„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.”;

36) po art. 67 dodaje się art. 67a-67b w brzmieniu:

„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.”;

38) w art. 73:

a) w ust. 1 w pkt 4 wyraz „osoby” zastępuje się wyrazem „osób”,

b) po ust. 1 dodaje się ust. 1a-1c w brzmieniu:

1a. Jednostka oceniająca zgodność, która:

1) nie przekazuje informacji, o których mowa w art. 59l i art. 59u ust. 3 lub przekazuje je nieprawdziwe lub niekompletne,

2) nie wykonuje obowiązku określonego w art. 59za ust. 1

- podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie przepisów o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”.

1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotnego przeciętnego wynagrodzenia.

1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:

1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, podlega karze pieniężnej w wysokości do dwudziestokrotnego przeciętnego wynagrodzenia,

2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, podlega karze pieniężnej w wysokości do piętnastokrotnego przeciętnego wynagrodzenia,

3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,

4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji

- podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego przeciętnego wynagrodzenia.

c) po ust. 2 dodaje się ust. 2a-2c w brzmieniu:

„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.”;

39) w art. 74

a) ust. 1 otrzymuje brzmienie:

„1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.”,

b) dodaje się ust. 1a i 1b w brzmieniu:

„1a. Karę pieniężną, o której mowa w art. 73 ust. 1a-1c, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

1b. Karę pieniężną określoną w art. 73 ust. 2a i 2b nakłada w drodze decyzji minister właściwy do spraw informatyzacji.”;

40) w art. 93 uchyla się ust. 8 i ust. 23;

41) po załączniku nr 2 do ustawy dodaje się załącznik nr 3 do ustawy w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. 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) po art. 115^3 dodaje się art. 115^4 w brzmieniu:

„Art. 115^4. 1. Prezes UKE może zapewnić odpowiednie częstotliwości w celu oferowania przez przedsiębiorcę telekomunikacyjnego na zasadach niedyskryminacyjnych usług na warunkach hurtowych w celu ich dalszej sprzedaży przez innego przedsiębiorcę telekomunikacyjnego.

2. Zapewnienie częstotliwości, o którym mowa w ust. 1, poprzedza analiza Prezesa UKE, która uwzględnia:

1) stopień realizacji celów wynikających z dokumentów programowych Unii Europejskiej na terytorium Rzeczypospolitej, w tym w szczególności w zakresie pokrycia terytorium kraju infrastrukturą zapewniającą dostęp do sieci bardzo szybkich przepustowości;
2) możliwości efektywnego wykorzystania częstotliwości;
3) stan rynku telekomunikacyjnego;
4) plany inwestycyjne przedsiębiorców telekomunikacyjnych;
5) długoterminowe spodziewane korzyści społeczno-gospodarcze;
6) promowanie innowacyjnych usług cyfrowych.

3. Wyniki analizy, o której mowa w ust. 3, Prezes UKE przedstawia Prezesowi Rady Ministrów w terminie 30 dni od dnia jej sporządzenia.

4. Prezes Rady Ministrów, w oparciu o analizę, o której mowa w ust. 3, w celu zapewnienia realizacji celów wynikających z dokumentów programowych Unii Europejskiej, w szczególności w zakresie pokrycia terytorium kraju infrastrukturą zapewniającą dostęp do sieci bardzo szybkich przepustowości, może wyznaczyć podmiot, który świadczył będzie usługi, o których mowa w ust. 1.

5. Podmiot, o którym mowa w ust. 4, wykorzystuje częstotliwości do wykonywania zadań, o których mowa w ust. 1, na podstawie decyzji o rezerwacji częstotliwości wydanej przez Prezesa UKE po uzgodnieniu z ministrem właściwym do spraw informatyzacji.”.

Art. 3. 1. Z dniem wejścia w życie ustawy:

1) wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej przed wejściem w życie niniejszej ustawy stają się SOC powołanymi w ramach operatora usługi kluczowej;
2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;
3) sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym staje się CSIRT sektorowym.

2. Podmioty publiczne wyznaczają osoby, o których mowa w art. 21 ustawy zmienianej w art. 1 w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

3. Organ właściwy ustanawia CSIRT sektorowy zgodnie z art. 44 ust. 5 w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

4. Organ właściwy do spraw cyberbezpieczeństwa publikuje komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w Dzienniku Urzędowym Monitor Polski.

5. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika,

2) zespołów CSIRT GOV, CSIRT MON, CSIRT NASK,

- a także jest przekazywana za pomocą systemu informacyjnego, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa.

6. Operator usługi kluczowej zgłasza incydenty, do właściwego CSIRT sektorowego od momentu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

Art. 4. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 - informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2021 r. – 16,41 mln zł;
2) w 2022 r. – 67,95 mln zł;
3) w 2023 r. – 59,06 mln zł;
4) w 2024 r. – 57,38 mln zł;

5) w 2025 r. – 58,4 mln zł;
6) w 2026 r. – 64,29 mln zł;
7) w 2027 r. – 70,10 mln zł;
8) w 2028 r. - 81,86 mln zł;
9) w 2029 r. – 84,07 mln zł;
10) w 2030 r. – 78,31 mln zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2021 r. – 2,54 mln zł;
2) w 2022 r. – 2,68 mln zł;
3) w 2023 r. – 2,84 mln zł;
4) w 2024 r. – 3,00 mln zł;
5) w 2025 r. – 3,09 mln zł;
6) w 2026 r. – 3,19 mln zł;
7) w 2027 r. – 3,29 mln zł;
8) w 2028 r. – 3,39 mln zł;
9) w 2029 r. – 3,50 mln zł;
10) w 2030 r. – 3,61 mln zł.

3. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętych na dany rok budżetowy maksymalnych limitów wydatków, o których mowa w ust. 1, zostaną zastosowane mechanizmy korygujące polegające na:

1) ograniczeniu finansowania działalności wyznaczonego CSIRT sektorowego wskazanego przez ministra właściwego do spraw informatyzacji;
2) ograniczeniu finansowania wynagrodzeń dla osób, o których mowa w art. 62a i są zatrudnione w CSIRT NASK lub urzędzie obsługującym Pełnomocnika;
3) ograniczeniu finansowania wynagrodzeń dla osób, o których mowa w art. 62a i są zatrudnione lub pełnią służbę w Agencji Bezpieczeństwa Wewnętrznego.

4. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 3 pkt 1 i 2, dokonuje minister właściwy do spraw informatyzacji.

5. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 3 pkt 3, dokonuje Szef Agencji Bezpieczeństwa Wewnętrznego.

Art. 5. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
REDAKCYJNYM I LEGISLACYJNYM
Aleksandra Wrochna
Zastępca Dyrektora Departamentu Prawnego
w Kancelarii Prezesa Rady Ministrów
/- podpisano elektronicznie/

Załącznik do ustawy z dnia …

Załącznik nr 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.

UZASADNIENIE

Ustawa o krajowym systemie cyberbezpieczeństwa, zwana dalej „ustawą o KSC”, przyjęta w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. W tym zakresie jest to także implementacja dyrektywy NIS.

Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów bezpieczeństwa. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym”), który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej ,,CSIRT”). Do zadań zespołów CSIRT poziomu krajowego należy także klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej - Państwowym Instytucie Badawczym, zwanym dalej „NASK”) oraz CSIRT MON (działającego w Ministerstwie Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach zespołu do spraw incydentów krytycznych.

Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół - CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego.

Obecnie w krajowym systemie cyberbezpieczeństwa nie znajdują się przedsiębiorcy telekomunikacyjni ani dostawcy usług zaufania.

Pełnomocnik

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany dalej ,,Pełnomocnikiem", jest odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań w obszarze cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu lub podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy również analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników, opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium

Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej ,,Kolegium", jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje również wymagania cyberbezpieczeństwa dotyczące decyzji Prezesa UKE w sprawie rezerwacji częstotliwości. Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów może wydać wiążące wytyczne w celu koordynacji działań w zakresie cyberbezpieczeństwa.

Potrzeba i cele projektu ustawy

Ustawa umożliwiła podjęcie prac nad dalszym rozwojem krajowego systemu cyberbezpieczeństwa, a doświadczenia zebrane przez dwa lata funkcjonowania systemu w Polsce, wskazały potrzebę dokonania zmian na poziomie ustawowym.

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Do tej pory powołano tylko jeden taki zespół - CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego, w sektorze najbardziej dojrzałym. Zespół powstał w oparciu o wewnętrzne środki i zasoby kadrowe UKNF. Dla podniesienia skuteczności reagowania na incydenty zachodzi konieczność ustanowienia CSIRT sektorowych dla każdego z kluczowych sektorów polskich gospodarki. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami, gdyż otrzymają bezpośrednie wsparcie w reagowaniu na incydenty.

Zauważono potrzebę zwiększenia uprawnień Pełnomocnika w celu skuteczniejszej koordynacji współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa i efektywniejszej odpowiedzi na nowe cyberzagrożenia.

Jednym z najczęściej występujących problemów jest brak właściwych struktur u operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo lub zakres posiadanych kwalifikacji (w tym kadr) oraz dostępności do informacji o cyberzagrożeniach utrudnia skuteczne reagowanie na incydenty.

Należy również wskazać na konieczność uregulowania zasad współpracy pomiędzy podmiotami publicznymi funkcjonującymi na poziomie województwa. Z informacji zawartej w wystąpieniu pokontrolnym Najwyższej Izby Kontroli z 2019 r. wynika, że negatywnie oceniono aż 70% kontrolowanych jednostek samorządu terytorialnego w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji. Z analiz przeprowadzonych na zlecenie Ministra Cyfryzacji duże zastrzeżenia budzi poziom zabezpieczeń e-usług oferowanych przez samorządy.

Kluczowa jest kwestia dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń. Do tej pory powstało w Polsce tylko jedno centrum wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa - ISAC (Information Sharing and Analysis Center). Pierwsze ISAC powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku. ISAC gromadzi informacje o podatnościach i cyberzagrożeniach, a następnie

przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w tym systemie. Taka formuła znacząco wpływa na poprawę cyberbezpieczeństwa i jest praktykowana w państwach Unii Europejskiej. Wskazane jest, aby więcej takich organizacji powstało w Polsce.

Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym. Centra ISAC stanowią platformę takiej współpracy poprzez wymianę informacji na temat przyczyn, incydentów, cyberzagrożeń jak również dzielenie się doświadczeniem wiedzą i analizami.

Akt o cyberbezpieczeństwie zachęca do tworzenia ISAC. Co więcej, jednym z obowiązków nałożonych na ENISA jest konieczność wspierania działań mających na celu wymianę informacji w ramach sektorów.

Przykładem sektorowego ISAC na poziomie europejskim jest European Energy Information Sharing & Analysis Centre (EE ISAC). Został zorganizowany z inicjatywy przemysłu energetycznego. W ramach EE ISAC wymieniają informacje dostawcy usług, przedsiębiorstwa użyteczności publicznej, instytucje naukowe, organizacje rządowe i pozarządowe (m.in. członkiem EE ISAC jest Polskie Sieci Elektroenergetyczne Spółka Akcyjna).

W Europie działa również amerykański Financial Services Information Sharing and Analysis Center zrzeszający około 7 000 instytucji finansowych z całego świata.

Coraz większe znaczenia dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe będą uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Polska brała udział w opracowaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (zwanego dalej “5G Toolbox”), w którym zawarto środki na poziomie strategicznym i technicznym oraz wskazano działania wspierające. Efektywne wdrożenie tych środków znacząco ograniczeni ryzyka cyberbezpieczeństwa w europejskich sieciach 5G.

Państwa członkowskie UE zobowiązały się w 5G Toolbox w szczególności do:

1) zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych,

2) oceniania profili ryzyka dostawców,

3) stosowania odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe,

4) wdrożenia strategii mających na celu zapewnienie dywersyfikacji dostawców, w celu unikania uzależnienia od dostawców stwarzających wysokie ryzyko.

5) Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox.

Krajowy system certyfikacji cyberbezpieczeństwa

W związku z rosnącą liczbą zagrożeń w cyberprzestrzeni jak i coraz istotniejszą rolą pełnioną przesz systemy informacyjne konieczne jest zapewnienie sprawdzonych i bezpiecznych rozwiązań technologicznych zarówno dla sektora publicznego, jak i prywatnego. W ostatnim czasie dało się także zauważyć wzrost liczby cyberprzestępstw zwłaszcza związanych z wykorzystaniem złośliwego oprogramowania takiego jak ransomware. Dlatego też konieczne jest zapewnienie każdemu zainteresowanemu dostępu do technologii umożliwiających bezpieczne przetwarzanie danych. Ze względu na wielką różnorodność wykorzystywanych technologii istotne jest stosowanie jednolitych standardów w zakresie bezpieczeństwa na terenie całej Unii Europejskiej.

Przygotowane rozwiązania zapewnią prawno-organizacyjne warunki do utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa, który zapewni wszystkim zainteresowanym podmiotom dostęp do możliwości testowania, badania produktów ICT, usług ICT i procesów ICT oraz otrzymywania certyfikatów cyberbezpieczeństwa opartych na europejskich programach, a także powszechnie uznawanych na obszarze Unii Europejskiej

Konieczność stworzenia takiego systemu wynika również z bezwzględnie obowiązujących przepisów prawa europejskiego, zawartych w rozporządzeniu 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), zwanym dalej „aktem o cyberbezpieczeństwie”.

Ten akt prawny został uchwalony w 2018 roku i ustanowił europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu

certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów.

Akt o cyberbezpieczeństwie nakłada na wszystkie państwa członkowskie obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa, który będzie nadzorował rynek i kontrolował prawidłowość działań w zakresie certyfikacji. Konieczne jest również wprowadzenie przepisów związanych z akredytacją podmiotów uprawnionych do wydawania certyfikatów oraz procedury związane z działaniem tego systemu jak np. kwestie zatwierdzania certyfikatów o poziomie zaufania „wysoki".

Przyjęte rozwiązania sprawią, że polskie firmy będą mogły swobodnie konkurować na europejskim rynku. Trzeba tu wskazać, że w wielu państwach Europy Środkowej rynek ten jest mniej rozwinięty niż w Polsce. W związku z tym, przyjęcie procedowanych przepisów może umożliwić polskim przedsiębiorcom przyciągnięcie klientów z regionu.

Przyjęte rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja w dziedzinie cyberbezpieczeństwa będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku.

Certyfikaty

Akt 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. Certyfikaty odwołujące się do najwyższego poziomu zaufania tj. poziomu „wysoki", w celu zagwarantowania, że proces ich wydawania przebiegał prawidłowo, będą musiały zostać zatwierdzone przez ministra właściwego do spraw cyfryzacji. Procedura ta zapewnia wysoką jakość usług przy równoczesnym zachowaniu reguł konkurencji rynkowej. Dzięki temu certyfikaty najwyższego poziomu będą mogły być wydawane przez każdy podmiot działający na rynku. Gwarantuje to najwyższy możliwy poziom dostępu do usług certyfikacyjnych przy równoczesnym wykonaniu przepisów aktu o cyberbezpieczeństwie.

Certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym. Ustawa tworzy ramy w jakich będzie wykonywana równocześnie nie nakładając żadnych obowiązków na podmioty działające na rynku. Każdy chętny będzie więc mógł rozpocząć działalność w tym zakresie jak i uzyskać certyfikację swojego produktu, usługi czy procesu ICT, równocześnie nie będąc do tego zobowiązanym.

Przyjęte rozwiązania służą również realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, zwanej dalej „Strategią". Ustanowienie krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa stanowią działania służące realizacji drugiego celu szczegółowego strategii - podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. W zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy o systemie oceny zgodności i nadzoru rynku. Polskie Centrum Akredytacji będzie zajmowało się akredytacją jednostek oceniających zgodność. Wymagania dotyczące jednostek oceniających zgodność zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. Ponadto dodatkowe wymagania dla nich mogą być też określane w konkretnych programach certyfikacji cyberbezpieczeństwa. Również konkretne kryteria jakie będą musiały spełniać produkty certyfikowane będą określone w krajowych i europejskich programach certyfikacji cyberbezpieczeństwa. Stosowane przepisy proceduralne będą więc dobrze znane i sprawdzone, a nowe będą jedynie stosowane przepisy materialne.

Prócz stworzenia ram dla funkcjonowania europejskich programów cyberbezpieczeństwa, ustawa tworzy też podstawę tworzenia krajowych programów certyfikacji cyberbezpieczeństwa. Umożliwi to podjęcie decyzji o certyfikowaniu produktów, które nie zostały objęte unijnymi programami certyfikacji. Zapewni to również możliwość reagowania na pojawiające się cyberzagrożenia bez konieczności czekania na powstanie programu certyfikacyjnego na poziomie europejskim.

Podjęcie prac związanych z utworzeniem krajowego systemu certyfikacji cyberbezpieczeństwa wynika zarówno z potrzeby stworzenia impulsu do rozwoju rynku w zakresie certyfikacji i zapewnienie bezpiecznych technologii dla zainteresowanych, a z drugiej strony z konieczności wdrożenia do polskiego porządku prawnego aktu o cyberbezpieczeństwie

Zgodność projektu ustawy z celami strategicznymi Rady Ministrów

Projekt ustawy służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024) jakim jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Realizuje on także cel szczegółowy w postaci rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawnych dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii szczególnie w odniesieniu do zapewnienie bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

Zmiany wprowadzane do krajowego systemu cyberbezpieczeństwa

CSIRT sektorowy

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.

ISAC

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.

SOC

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.

Koordynacja zadań na poziomie województwa

Jednostki samorządu terytorialnego są coraz częściej narażone na cyberataki, jednocześnie mają ograniczone zasoby w zakresie reagowania na incydenty. W celu skuteczniejszej koordynacji reagowania na incydenty na poziomie wojewódzkim, samorządy będą wspierane przez struktury podległe wojewodzie, w szczególności w procesie zapewnienia wymiany informacji pomiędzy zespołami CSIRT poziomu krajowego i Pełnomocnikiem a podmiotami publicznymi w województwie. Ułatwi to wymianę informacji o cyberzagrożeniach cyberbezpieczeństwa, incydentach czy podatnościach. Dzięki temu zwiększone zostaną możliwości przeciwdziałania incydentom w jednostkach samorządu terytorialnego oraz w innych podmiotach publicznych w województwie takich jak terenowa administracja rządowa czy też sądy.

Procedura uznania dostawcy za dostawcę wysokiego ryzyka

Odporność na cyberzagrożenia zależy w dużym stopniu od bezpieczeństwa sprzętu, oprogramowania i usług. Dotyczy to zarówno systemów teleinformatycznych, sieci telekomunikacyjnych oraz przemysłowych systemów sterowania. Dlatego nowelizacja przewiduje wprowadzenie postępowania w sprawie uznania dostawcę sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa za dostawcę wysokiego ryzyka. Postępowanie w tej kwestii będzie prowadził minister właściwy do spraw informatyzacji. Postępowanie będzie oparte o transparentne procedury określone w Kodeksie postępowania administracyjnego. Minister właściwy ds. informatyzacji każdorazowo będzie zasięgał opinii Kolegium. Rolą Kolegium będzie sporządzenie opinii na temat dostawcy sprzętu lub oprogramowania i dostarczanych przez niego produktów ICT, usług ICT, procesów ICT. W ramach opinii brane pod uwagę zarówno aspekty techniczne, jak i pozatechniczne, mające wpływ na bezpieczeństwo narodowe. Postępowanie będzie kończyło się decyzją administracyjną w sprawie uznania dostawcy za dostawcę wysokiego ryzyka. Będzie ona podlegać zaskarżeniu do sądu administracyjnego.

Podkreślić należy, że ocena profili ryzyka dostawców jest jednym z narzędzi strategicznych (Strategic Measure - SM04) uzgodnionych przez państwa członkowskie Unii Europejskiej, Komisję Europejską i ENISA w 5G Toolbox

Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych, czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorcami) w zależności od decyzji ministra właściwego do spraw informatyzacji w zakresie uznania danego dostawcę za dostawcę wysokiego ryzyka, będą musiały z użycia wycofać wskazany sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka w terminie 7 lat od wydania decyzji administracyjnej. Natomiast duzi przedsiębiorcy telekomunikacyjni będą musieli wycofać produkty, usługi i procesy ICT w ciągu 5 lat, jeżeli znajdują się one w zakresie funkcji krytycznych określonych w załączniku nr 3 do ustawy. Podkreślenia wymaga fakt, że obowiązkowi wycofania będą podlegały produkty, usługi i procesy ICT wskazane w decyzji ministra właściwego do spraw informatyzacji – a więc nie wszystkie produkty, usługi i procesy ICT oferowane przez dostawcę wysokiego ryzyka.

Zapobieganie incydentom krytycznym i zwiększenie skuteczności reagowania na incydenty krytyczne

W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne będą mogły być wydawane:

1) ostrzeżenia (wydawane przez Pełnomocnika) - w przypadku uzyskania informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,

2) polecenia zabezpieczające (wydawane przez ministra właściwego do spraw informatyzacji) - w zapewnienia koordynacji i odpowiedniej reakcji w sytuacji wystąpienia incydentu krytycznego.

Krajowe programy certyfikacji cyberbezpieczeństwa

Projekt ustawy przewiduje też tworzenie krajowych programów certyfikacji cyberbezpieczeństwa, na podstawie których przeprowadzana będzie certyfikacja. W dokumentach tych zawarte zostaną techniczne standardy, które produkty, usługi i procesy ICT będą musiały spełniać. Ponadto, będą określały szczegóły związane z procesem certyfikacji czy procedury sanacyjne w przypadku, gdy po samej certyfikacji ujawnią się wady produktów. Wszystkie te elementy muszą być bardzo ściśle dostosowane do konkretnego produktu, usługi

czy procesu ICT. Krajowy program cyberbezpieczeństwa będzie określany przez Radę Ministrów w drodze rozporządzenia (art. 59e).

Elementy programu zostały sformułowane na wzór przepisów aktu o cyberbezpieczeństwie dotyczących europejskich programów certyfikacji cyberbezpieczeństwa. Dzięki temu wymagania i standardy wobec krajowych i europejskich programów certyfikacji będą bardzo do siebie zbliżone co sprawi, że nie będzie konieczne tworzenie osobnej terminologii dla krajowych programów certyfikacji. Umożliwi to więc wykorzystanie w jak największym stopniu praktyk wypracowanych w ramach europejskich programów certyfikacji. Ponadto certyfikaty cyberbezpieczeństwa wydane na podstawie krajowych programów certyfikacyjnych mogą, w skutek przyjętych rozwiązań, łatwo zostać uznane w innych krajach UE. Ponadto możliwe będzie rozszerzenie rynku certyfikacji przez objęcie programami produktów, usług i procesów ICT nieujętych w europejskich programach certyfikacyjnych. Bliskość z programami europejskimi umożliwi też stosunkowo łatwe przenoszenie programów krajowych na poziom europejski. Będzie to bardzo ważnym narzędziem do kreowania polskiej polityki w zakresie certyfikacji cyberbezpieczeństwa na poziomie europejskim (art. 59 f-g).

Jednostki oceniające zgodność

Proces certyfikacji będzie prowadzony przez jednostki oceniające zgodność akredytowane przez Polskie Centrum Akredytacji na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i systemach nadzoru rynku (Dz. U. z 2019 r. poz. 544, z późn. zm.). Wykorzystanie już obowiązujących przepisów zapewni możliwie najsprawniejsze wprowadzenie w życie systemu certyfikacji cyberbezpieczeństwa. Polskie Centrum Akredytacji będzie sprawowało nadzór nad akredytacją jednostek oceniających zgodność. Będzie też na bieżąco wymieniać się informacjami z ministrem właściwym do spraw informatyzacji co zapewni skuteczną kontrolę nad całym systemem. (art. 59 h)

W przypadku certyfikatów odwołujących się do najniższego z poziomów uzasadnienia zaufania sami dostawcy sprzętu lub oprogramowania będą mogli wydawać deklaracje zgodności by wskazać, że ich produkt spełnia dane wymagania (art. 59 p-r). Zapewni to im możliwość skorzystania z programów certyfikacyjnych ograniczając równocześnie koszty uczestnictwa w nich.

Przewidywane skutki społeczne, gospodarcze, prawne i finansowe wprowadzanych zmian

Skutki społeczne

Dodanie CSIRT sektorowych, SOC i ISAC pozwoli na zwiększenie skuteczności funkcjonowania krajowego systemu cyberbezpieczeństwa.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, które stworzą nie tylko skuteczny system reagowania na incydenty, ale też zapewni bazę wiedzy o cyberzagrożeniach i podatnościach danego sektora. Dzięki temu incydenty w sektorze będą obsługiwane szybciej, z uwzględnieniem szczególnych uwarunkowań danego sektora. Natomiast centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa.

Przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw. Większe wykorzystanie rozwiązań odpornych na cyberataki zwiększy też ogólne bezpieczeństwo danych obywateli.

Skutki gospodarcze

Celem krajowego systemu cyberbezpieczeństwa jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Poprzez nałożenie dodatkowych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą. Zobowiązuje bowiem tych przedsiębiorców do dbania o cyberbezpieczeństwo. Po stronie przedsiębiorców powoduje to koszty związane z koniecznością dostosowania się do wymogów ustawy. Należy jednak zauważyć, że wielu z nich już obecnie posiada operacyjne centra bezpieczeństwa, ponieważ podobny wymóg istnieje w obowiązującej wersji ustawy. Poza tym, podmiot inwestujący we własne cyberbezpieczeństwo zyskuje zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom skuteczniej dbać o cyberbezpieczeństwo w swojej działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

Przyjęte rozwiązania będą również promowały rozwiązania, które zapewniają wysokie standardy w zakresie cyberbezpieczeństwa. Prywatni przedsiębiorcy będą mieli ułatwiony wybór bezpiecznych rozwiązań technologicznych. Ponadto nowe regulacje będą zapewniały, że firmy, które zakupią certyfikowane produkty, usługi czy procesy ICT będą miały pewność, że ich certyfikaty będą honorowane na terenie całej Unii Europejskiej. Projektowana ustawa

zawiera szereg rozwiązań zapewniających właściwe standardy postępowania przy ocenie zgodności co daje dodatkowe gwarancje jakości.

Krajowy system certyfikacji cyberbezpieczeństwa będzie też stanowił cenne uzupełnienie krajowego systemu cyberbezpieczeństwa. Stworzy wyraźny system oceny produktów ICT dzięki czemu jasno wskazane będą produkty spełniające najlepsze standardy w dziedzinie bezpieczeństwie.

Przyjęte przepisy nie nałożą żadnych dodatkowych obowiązków na podmioty niezainteresowane uczestnictwem w tym systemie. Przyjęty model nie tworzy też barier dostępu do rynku.

Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa m.in. sektorowych CSIRT, będzie wymagało dodatkowych nakładów finansowych. Należy jednak podkreślić, że jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częste i bardziej zaawansowane. Drastycznie wzrosła liczba incydentów cyberbezpieczeństwa oraz samych cyberataków, których ofiarami padają urzędy, szpitale ale także coraz więcej ataków obserwujemy w sektorze prywatnym oraz w stosunku do obywateli. Od początku 2020 roku do końcu listopada tylko zespół CSIRT NASK odnotował 30300 zgłoszeń. W samym listopadzie 2020 r. były to 3833 zgłoszenia. Z tej liczby CSIRT NASK zarejestrował od początku roku 2020 do końca listopada aż 9604 incydenty cyberbezpieczeństwa (w listopadzie zarejestrowano 1381). Jest to znaczący wzrost w stosunku do 2019 r., w którym CSIRT NASK odnotował 6484 incydenty.

Istnieje także stałe zagrożenie działaniami wywiadowczymi w cyberprzestrzeni. Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne, a mają one również wymiar finansowy. Inwestycja w rozbudowę krajowego systemu cyberbezpieczeństwa pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne efekty. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Przyjęcie przepisów o krajowym systemie certyfikacji cyberbezpieczeństwa będzie miało korzystne skutki dla całego sektora przedsiębiorstw. Obecnie firmy ponoszą coraz większe straty w wyniku działalności cyberprzestępców. Wprowadzenie certyfikacji w tej dziedzinie

sprawi, że firmom łatwiej będzie wybierać rozwiązania gwarantujące najwyższy poziom bezpieczeństwa. Ponadto samo stworzenie systemu przyczyni się do wzrostu świadomości cyberbezpieczeństwa. W efekcie straty ponoszone przez sektor przedsiębiorstw powinny zostać zmniejszone.

Skutki prawne

Powstaną nowe rejestry pomagające właściwym instytucjom wykonywać swoje ustawowe zadania – wykaz SOC oraz wykaz ISAC.

Wojewoda stanie się aktywnym uczestnikiem wymiany informacji między Pełnomocnikiem, zespołami CSIRT poziomu krajowego a jednostkami samorządu terytorialnego w województwie. Poprawi to jakość współpracy miedzy nimi a w konsekwencji zwiększy świadomość cyberbezpieczeństwa w samorządzie terytorialnym.

Minister właściwy do spraw informatyzacji będzie mógł przeprowadzić postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

Pełnomocnik i minister do spraw informatyzacji uzyskają nowe narzędzia w celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne

Umocowany krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował uprawnieniami do nadzoru nad systemem certyfikacji cyberbezpieczeństwa oraz będzie dysponował narzędziami do usuwania z obiegu prawnego certyfikatów wydanych wbrew przepisom ustawy oraz do kontrolowania podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Ponadto przepisy ustanawiają podstawę prawną i procedury dla przyjmowania krajowych programów certyfikacji cyberbezpieczeństwa.

Źródła finansowania projektowanych zmian

Wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki z budżetu państwa.

Wyniki przeprowadzonych konsultacji

W dniach 30.06-8.07 2020 przeprowadzone zostały pre-konsultacje robocze w ramach zespołu doraźnego przy Kolegium.

Zostały przeprowadzone konsultacje wewnątrz resortu Ministerstwa Cyfryzacji obsługującego w czasie ich trwania ministra właściwego do spraw informatyzacji .

Projekt zostanie ponadto wysłany do organizacji branżowych, organów właściwych ds. cyberbezpieczeństwa, operatorów usług kluczowych i partnerów społecznych. Ze względu na poruszaną kwestię współpracy z samorządami, zostanie skierowany do opiniowania przez stowarzyszenia zrzeszające samorządy.

Ponadto, projekt zostanie przekazany do zaopiniowania związkom zawodowym i organizacjom pracodawców.

Uzasadnienie poszczególnych przepisów materialnych

W art. 1 został dodany w ust. 1 pkt 1a w związku z rozszerzeniem zakresu przedmiotowego ustawy o krajowy system certyfikacji cyberbezpieczeństwa. Zmodyfikowane zostały również wyłączenia przedmiotowe ustawy w ust. 2 pkt 1 – 2. Do przedsiębiorców telekomunikacyjnych będą się stosować:

1) przepisy o wycofaniu produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka

2) przepisy o ostrzeżeniu i poleceniu zabezpieczającym

3) przepisy o karach pieniężnych

Z kolei do dostawców usług zaufania będą stosować się:

1) przepisy o ostrzeżeniu i poleceniu zabezpieczającym;

2) przepisy o karach pieniężnych.

Artykuł 2 obecnie obowiązującej ustawy zawiera słowniczek pojęć używanych w ustawie, stąd niezbędne było dodanie do niego w projektowanych punktach 3a-3d definicji CSIRT sektorowego, ISAC i SOC, a także dostawcy. Z kolei dodanie punktów 20-32 wynikało z konieczności wprowadzenia do ustawy pojęć związanych z certyfikacją cyberbezpieczeństwa. W związku ze zmianą nazwy proponuje się w nowelizacji zamianę frazy „sektorowy zespół cyberbezpieczeństwa” na CSIRT sektorowy.

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. Nowe definicje są więc całkowicie zgodne z przepisami zawartymi w akcie o cyberbezpieczeństwie. Takie rozwiązanie zapewnia zgodność z polskim porządkiem prawnym.

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.

Wprowadzone zostały pojęcia produktu ICT, usługi ICT oraz procesu ICT. Te trzy pojęcia służą objęciu systemem certyfikacji jak największego zakresu dostępnych na rynku świadczeń. Produkt oznacza „element lub grupę elementów systemów informacyjnych". Będzie więc obejmował praktycznie wszystkie przypadki oprogramowania oraz urządzeń podlegających certyfikacji. Usługi będą dotyczyły wszelkich działań związanych z przetwarzaniem informacji w systemach informacyjnych. Obejmują więc sytuację gdy żadne operacje nie są wykonywane w ramach systemów klienta, który jedynie otrzymuje ich końcowy efekt. Proces ICT oznacza „zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT". Są to więc wszelkiego rodzaju działania związane z tworzeniem systemów informacyjnych i ich bieżącym utrzymaniem.

Ponadto projektowana ustawa posługuje się pojęciami certyfikat oraz krajowy certyfikat cyberbezpieczeństwa. Certyfikat odnosi się do wszystkich certyfikatów w dziedzinie cyberbezpieczeństwa tj. zarówno tych wydanych w ramach krajowych jak i europejskich

programów certyfikacji. Z kolei krajowy certyfikat cyberbezpieczeństwa dotyczy tylko dokumentów wydanych na podstawie krajowych programów certyfikacyjnych. To rozróżnienie jest potrzebny dla wyodrębnienia przepisów, które dotyczą tylko krajowych certyfikatów. Certyfikaty te będą traktowane jednakowo. Wiele kwestii związanych z europejskimi certyfikatami jest już określona w unijnym rozporządzeniu. Dlatego dla certyfikatów krajowych przyjęto odpowiadające im w niniejszej nowelizacji.

Analogiczna sytuacja występuje w przypadku deklaracji zgodności i krajowych deklaracji zgodności.

Konsekwencją tych zmian była konieczność dostosowania pozostałych przepisów ustawy do ww. zmian.

Wprowadzono pojęcie dostawcy – jest to producent, upoważniony przedstawiciel, importer lub dystrybutor w rozumieniu rozporządzenia unijnego o wymaganiach w zakresie akredytacji i nadzorze rynku[1)]. Definicja ta jest potrzebna przy przepisach dotyczących krajowego systemu certyfikacji cyberbezpieczeństwa oraz na potrzeby postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Wprowadzono również skrót nazwy Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA). Skrót jest powszechnie rozpoznawalny wśród osób zajmujących się cyberbezpieczeństwem – jego stosowanie w ustawie poprawi redakcję przepisów.

W nowelizacji artykułu 4, który wymienia podmioty KSC proponuje się dodać w punktach 7a, 7b, 14a i 14b nowe podmioty: Urząd Komisji Nadzoru Finansowego (w związku ze zmianą ustawy o nadzorze nad rynkiem finansowym zmienił formę prawną działania[2)]), wyszczególniono uczelnie wyższe odwołując się do Prawa o szkolnictwie wyższym i nauce. Dodano także ISAC Zgodnie ze zmianą nazewnictwa podmioty świadczące usługi cyberbezpieczeństwa zmieniono na SOC. Do tej pory nie były objęte ustawą inne dwa istotne dla funkcjonowania państwa podmioty – Wody Polskie oraz Polski Fundusz Rozwoju S.A. Wody Polskie jako podmiot zajmujący się gospodarką wodną realizuje ważne zadania

---

[1)] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93

[2)] Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz. U. poz. 2243).

publiczne – zapobieganie suszom i powodziom, zapewnianie dobrej jakości wody dla mieszkańców Polski. Z kolei Polski Fundusz Rozwoju S.A. odpowiada za wsparcie polskich przedsiębiorców, w tym realizuje program Tarczy Antykryzysowej. Do krajowego systemu cyberbezpieczeństwa zostaną dodane także samodzielne publiczne zakłady opieki zdrowotnej, które podczas pandemii COVID-19 pełnią szczególną rolę. Dlatego konieczne jest objęcie tych podmiotów obowiązkami z art. 21-23 ustawy o krajowym systemie cyberbezpieczeństwa a także zapewnienie im wsparcia właściwego zespołu CSIRT poziomu krajowego w przypadku incydentu.

W propozycji nowelizacji artykułu 7 ust. 5 dodaje się możliwość podpisania wniosku o wpisanie operatora usługi kluczowej do wykazu operatorów także podpisem osobistym. Podpis osobisty został uregulowany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2020 r. poz. 332, 695, 875, 1517 i 2320). Jest to zaawansowany podpis elektroniczny umieszczony w warstwie elektronicznej dowodu osobistego. Podpisanie danych podpisem osobistym ma taki sam skutek, co podpis własnoręczny wobec podmiotu publicznego.

Proponuje się zmianę brzmienia art. 8 pkt 5 lit. b. Zostanie doprecyzowany obowiązek aktualizacji oprogramowania przez operatorów usług kluczowych.

W artykule 9 wprowadzono zmianę, na mocy której operatorzy usług kluczowych będą musieli wyznaczyć 2 osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa.

W nowelizowanym art. 10 ust. 2 pkt 2 rozszerzono obowiązki nadzoru nad dokumentacją o ochronę dokumentów przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem.

Proponowana zmiana art. 11 ust. 3 pkt 1-3 polega na dostosowaniu przepisu do CSIRT sektorowych. W związku z obowiązkiem utworzenia CSIRT sektorowych przez organy właściwe do spraw cyberbezpieczeństwa, operatorzy usług kluczowych będą musieli uwzględnić w swoich procedurach obowiązek zgłoszenia incydentu do CSIRT sektorowego, współdziałać z CSIRT sektorowym podczas obsługi incydentu a także zapewnić CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach. Warto zauważyć, że dla operatorów usług kluczowych nie są to obowiązki uciążliwe. Mają one na celu umożliwienie CSIRT sektorowemu udzielanie skutecznej pomocy podczas incydentu poważnego lub krytycznego.

Art. 14 zostanie całkowicie zmieniony w nowelizacji. Wskazano, że zadania operatorów usług kluczowych w zakresie cyberbezpieczeństwa realizowane są za pomocą funkcji SOC. SOC może być powołany wewnątrz organizacji danego operatora usługi kluczowej lub stanowić odrębny podmiot. W tym drugim przypadku operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o zawarciu umowy z zewnętrznym podmiotem realizującym zadania funkcji SOC, jego danych kontaktowych i zakresie świadczonej usługi na rzecz tego operatora.

Art. 14 ust. 3 nowelizacji nakazuje SOC wprowadzić zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Jeżeli operator usługi kluczowej zawiera z podmiotem trzecim umowę o realizację funkcji SOC to o umowie i jej szczegółach informuje niezwłocznie organ właściwy ds. cyberbezpieczeństwa.

W niezbędnych sytuacjach SOC ma zapewnić bezpieczny zdalny dostęp do swoich systemów dla obsługiwanego operatora usługi kluczowej. Istotne jest, aby opracować procedury i stosować środki, które zminimalizują zagrożenie wycieku danych z SOC.

Nawiązując do praktyki obecnej na rynku (publikowanie informacji na podstawie wzoru RFC 2350) podmioty trzecie świadczące funkcje SOC udostępniają na stronie internetowej podstawowej informacje o swojej działalności.

Aby odpowiednie urzędy i służby miały dostęp do danych SOC w zakresie swoich ustawowych kompetencji, minister właściwy do spraw informatyzacji będzie prowadził wykaz SOC. W wykazie znajdą się zarówno podmioty prowadzące SOC oraz podmioty, na rzecz których SOC realizują zadania. Do wykazu mogą być wpisane SOC, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk. Muszą one posiadać zdolność do ochrony informacji niejawnych. Dodatkowym wymogiem jest również podpisanie porozumienia z ministrem właściwym do spraw informatyzacji w sprawie korzystania z systemu teleinformatycznego opisanego w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Co istotne, wprowadzony zostanie obowiązek aby przy zawieraniu umowy na świadczenie usług SOC przez podmiot prowadzący SOC dla operatora usługi kluczowej umowa ta zawierała zastrzeżenie, że usługi te podlegają prawu polskiemu.

W celu umożliwienia wykonywania swoich zadań dane z wykazu SOC są udostępniane CSIRT MON, CSIRT NASK, CSIRT GOV i właściwemu ze względu na sektor CSIRT sektorowemu, jak również operatorowi usługi kluczowej w dotyczącym go zakresie. Na wniosek dane z wykazu SOC mogą być udzielane organom właściwym, służbom, sądom, prokuraturze.

Zmiana artykułu 21 polega na wprowadzeniu obowiązku wyznaczenia przez podmioty publiczne nie jednej a dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dzięki temu zwiększy się możliwość kontaktu z podmiotem publicznym podczas trwania incydentu w podmiocie publicznym.

W art. 22 ust. 1 zostanie dodany pkt 2a. Zgodnie z nim podmioty publiczne będące jednostkami samorządu terytorialnego będą zgłaszały incydent w podmiocie publicznym także do wojewody. Zadanie to służy zapewnieniu obowiązku informacyjnego wobec wojewody.

W nowym art. 24a dodano nowe zadania wojewody, który będzie uczestniczył w wymianie informacji między zarządem województwa, powiatu, wójtami, burmistrzami, prezydentami miast, a Pełnomocnikiem i zespołami CSIRT poziomu krajowego. Będzie również prowadził listę osób kontaktowych z jednostek samorządu terytorialnego.

Po rozdziale 5 zostanie dodany rozdział 5a dotyczący ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Nic nie stało do tej pory na przeszkodzie, aby były tworzone podmioty na wzór ISAC, na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji. Nowelizacja tego nie zmienia, daje jedynie możliwość funkcjonowania ISAC w ramach krajowego systemu cyberbezpieczeństwa.

W projektowanym artykule 25a wskazano (w otwartym katalogu) zadania ISAC. Będą to: wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów. Dodano przepisy odnośnie prowadzenia wykazu ISAC, wpisu do niego oraz wykreślenia. Wpis do wykazu będzie odbywał się po uzyskaniu opinii organów właściwych do spraw cyberbezpieczeństwa. ISAC ma współpracować z zespołami CSIRT poziomu krajowego. Będą musiały również złożyć sprawozdanie ze swojej działalności ministrowi właściwemu ds. informatyzacji. Jeżeli ISAC prowadzi działalność niezgodną z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa to minister właściwy ds. informatyzacji może zwrócić się do ISAC o usunięcie nieprawidłowości w określonym terminie albo wykreślić ten podmiot z wykazu.

W nowelizacji art. 26 ust. 3 pkt 2 zmiany polegają na uproszczeniu nazewnictwa. W ust. 3 dodane zostały nowe zadania zespołów CSIRT poziomu krajowego: gromadzenie informacji dotyczących cyberzagrożeń, podatności i incydentów, przygotowywanie dla Pełnomocnika analiz, przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa. Zespoły CSIRT otrzymają także możliwość prowadzenia działań na rzecz podniesienia poziomu cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa takich jak testy bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami. Będą mogły też identyfikować podatności systemów dostępnych w otwartych sieciach teleinformatycznych oraz informować właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

W związku z pismem Komisji Europejskiej Ref. Ares(2019)2130481 z dnia 26 marca 2019 r. w zakresie zmiany terminu przekazania przez państwa członkowskie sprawozdania rocznego dotyczącego informacji o zgłoszonych przez operatorów usług kluczowych incydentach poważnych i zgłoszonych przez dostawców usług cyfrowych incydentach istotnych, informacje o zgłoszonych incydentach od roku 2020 dane za rok poprzedni muszą być przekazywane do dnia 15 lutego. Dlatego też zmieniono termin przekazania tych danych przez zespoły CSIRT poziomu krajowego do Pojedynczego Punktu Kontaktowego z 30 maja na 31 stycznia.

W art. 36 ust. 2 rozszerza się zakres podmiotowy Zespołu do spraw Incydentów Krytycznych, dalej zwany jako „Zespół”. W skład Zespołu wejdą także przedstawiciele Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Związane jest to z nowymi zadaniami Pełnomocnika – wydawanie ostrzeżeń oraz ministra właściwego do spraw informatyzacji – wydawanie poleceń zabezpieczających.

Proponowana w nowelizacji nowa treść art. 44 wprowadza obowiązek powołania przez organ właściwy CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał operatorów usług kluczowych tego sektora w obszarze reagowania na incydenty. Projektowane zadania CSIRT sektorowego będą szersze niż obecnych sektorowych zespołów. Zespoły te m.in. będą przyjmować zgłoszenia o wszystkich incydentach i reagować na nie. Będą mogły również gromadzić informacje o podatnościach i cyberzagrożeniach. Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze a także będą mogły, w uzgodnieniu z

operatorem usługi kluczowej, wspierać go w wykonywaniu jego obowiązków określonych w rozdziale 3 ustawy KSC.

Organ właściwy może powierzyć realizację tych zadań podległym lub nadzorowanym jednostkom. Gdyby organ nie wywiązał się z tego obowiązku to organ będzie mógł, po zasięgnięciu opinii Pełnomocnika, powierzyć wykonywanie zadań CSIRT jednostkom sektora finansów publicznych, innym państwowym jednostkom organizacyjnym nieposiadającym osobowości prawnej, a także osobom prawnym, nad którymi kontrolę sprawują jednostki sektora finansów publicznych lub inne państwowe jednostki organizacyjne.

Budowa i utrzymanie CSIRT sektorowych będzie finansowana z rezerwy celowej, której dysponentem będzie minister właściwy do spraw informatyzacji. Zapewni to skuteczne finansowanie CSIRT sektorowych. Dodatkowo organy właściwe do spraw cyberbezpieczeństwa przedkładać sprawozdania z funkcjonowania CSIRT sektorowych do Pełnomocnika.

Proponowana w nowelizacji zmiana art. 46 określa dostęp podmiotów krajowego systemu cyberbezpieczeństwa do tworzonego na podstawie tego samego artykułu systemu teleinformatycznego. Pełnomocnik oraz zespoły CSIRT poziomu krajowego będą miały stały i nieograniczony dostęp do tego systemu. Prezes UKE oraz zespoły CSIRT sektorowe będą miały dostęp do systemu tylko w obszarze swojej właściwości. Pozostałe podmioty krajowego systemu cyberbezpieczeństwa będą mogły uzyskać dostęp do systemu po podpisaniu porozumienia z ministrem właściwym do spraw informatyzacji. Dostęp do systemu otrzyma także Pełnomocnik.

Po rozdziale 11 zostaje dodany rozdział 11a zawierający przepisy 59a-59zc regulujące krajowy system certyfikacji cyberbezpieczeństwa.

W projektowanym art. 59a ustanowiono krajowy system certyfikacji cyberbezpieczeństwa. Wskazany został również cel, jakiemu nowy system ma służyć. System ten ma przyczynić się do większej harmonizacji rozwiązań z zakresu cyberbezpieczeństwa w całej Unii Europejskiej oraz do zwiększenia poziomu bezpieczeństwa w sektorze przedsiębiorstw.

Projektowany art. 59b wyznacza zakres podmiotowy nowego systemu oraz wskazuje organ nadzoru nad jego działaniem. Do systemu będą należały Polskie Centrum Akredytacji, minister właściwy do spraw informatyzacji oraz zainteresowane jednostki oceniające zgodność

i przedsiębiorcy certyfikujące swoje produkty. Należy tu podkreślić, że podmioty prywatne nie będą w żaden sposób zmuszone do dołączenia do tego systemu. Obowiązki z niego wynikające będą więc dotyczyć tylko tych, którzy dobrowolnie się im poddadzą. Tyczy się to zarówno jednostek oceniających zgodność jak i wytwórców.

Art. 59c wyznacza zadania dla ministra właściwego do spraw informatyzacji. Zadania te wynikają wprost z przepisów aktu o cyberbezpieczeństwie i dotyczą nadzoru i kontroli nad podmiotami tego systemu jak również współpracy międzynarodowej w tym zakresie.

Minister właściwy do spraw informatyzacji będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli pod kątem przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w ustawie o krajowym systemie cyberbezpieczeństwa. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania nowej ustawy.

W ramach obowiązków krajowego organu minister właściwy do spraw informatyzacji będzie prowadzić szereg postępowań administracyjnych dotyczących m.in.:

- zatwierdzania certyfikatów odwołujących się do poziomu zaufania wysoki (art. 59o),

- wydawania zezwoleń na prowadzenie oceny zgodności w przypadku gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność (art. 59i ust. 1),

- cofania i ograniczania, zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność (art. 59i ust. 2),

- cofnięcia certyfikatu wydanego wbrew przepisom ustawy lub wbrew postanowieniom programu certyfikacyjnego (art. 59o ust. 7),

- nakładania kar pieniężnych (art. 73 ust. 1a).

Wszystkie rozstrzygnięcia w tym zakresie będą wydawane zgodnie z przepisami Kodeksu postępowania administracyjnego.

Do obowiązków krajowego organu będą również należeć kwestie współpracy z analogicznymi organami w innych państwach Unii Europejskiej, jak również będzie przeprowadzał wzajemne przeglądy z tymi organami (art. 59c ust. 1 pkt 4). W ramach tych

działań organy będą nawzajem oceniać swoje działania. Konieczność wdrożenia tej procedury wynika wprost z przepisów aktu o cyberbezpieczeństwie.

Projektowany art. 59d wyznacza rolę Polskiego Centrum Akredytacji, które będzie nadzorowało jednostki oceniające zgodność pod kątem spełnienia przez nie wymogów akredytacji. PCA będzie tu pełniło taką samą rolę jaką pełni w ogólnym systemie oceny zgodności. Zapewni to szybkie wdrożenie nowych przepisów w praktyce.

Zgodnie z projektowanym art. 59e krajowe programy certyfikacyjne będą określane w drodze rozporządzeń Rady Ministrów. Przy ich tworzeniu będzie brany pod uwagę obecny stan wiedzy w dziedzinie techniki oraz kwestia potrzeb rynku w zakresie cyberbezpieczeństwa. Dzięki temu programy certyfikacyjne będą brały pod uwagę konkretne potrzeby przedsiębiorców oraz promować w tym zakresie najlepsze rozwiązania z tej dziedziny.

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 na poziomie ustawy szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT. 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 przez 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 przez 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.

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.

Projektowany art. 59h wyznacza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji. Aby prowadzić badania produktów, usług i procesów ICT podmioty będą musiały uzyskać akredytację Polskiego Centrum Akredytacji. Wymagania dla zainteresowanych zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. PCA będzie procedować na podstawie przepisów ustawy o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544). Są to przepisy na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania z ich strony.

Sprawna wymiana informacji między PCA sprawującym nadzór nad akredytacją oraz ministrem właściwym do spraw informatyzacji jest niezbędna do sprawnego działania nowego systemu. W związku z tym PCA będzie informować ministra o dokonanych akredytacjach oraz o odmowie ich dokonania. Proponowane rozwiązania gwarantują, że minister właściwy do spraw informatyzacji będzie poinformowany o wszystkich podmiotach wydających certyfikaty oraz będzie posiadał informacje niezbędne do prowadzenia nadzoru nad tym rynkiem.

Art. 59i reguluje sytuację gdy program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku, oprócz akredytacji, te jednostki będą musiały uzyskać zezwolenia ministra właściwego do spraw informatyzacji. Zezwolenia określone w projektowanym art. 59i wynikają wprost z obowiązku wdrożenia aktu o cyberbezpieczeństwie. Jeśli bowiem europejskie lub krajowe programy certyfikacyjne będą zawierały postanowienia o szczególnych wymaganiach w zakresie jednostek oceniających zdolność musi istnieć organ sprawdzający te wymagania oraz zezwalający na ich działanie w ramach określonego programu certyfikacji. Taka regulacja wynika wprost z obowiązku wdrożenia Akt o cyberbezpieczeństwie.

Nowe art. 59 j-k wyznaczają ogólne zasady związane z oceną zgodności i zasadami wydawania certyfikatów. Są one utworzone w sposób analogiczny do przepisów dotyczących systemu oceny zgodności. Wskazują one wyraźnie, że poddanie produktów, usług i procesów ICT ocenie zgodności jest całkowicie dobrowolne. Warunki przeprowadzania oceny zgodności będą określane w europejskich i krajowych programach certyfikacji. Taka konstrukcja jest konieczna ze względu na bardzo szeroki zakres produktów jakie będą podlegały certyfikacji. Dlatego też nie jest możliwe określenie jednolitych warunków dla wszystkich tych towarów.

Art. 59k reguluje zagadnienia związane z wnioskiem o certyfikację, jaki zainteresowane podmioty będą składać do jednostek oceniających zgodność. Taki dokument musi wskazywać od kogo pochodzi, jakich produktów dotyczy oraz wskazywać spełnienie niezbędnych wymagań. Aby przyśpieszyć proces do wniosku muszą być dołączone dokumenty potwierdzające spełnienie wymagań. Wniosek o spełnienie wymagań może być złożony zarówno w tradycyjnej papierowej formie jak i w formach elektronicznych. To rozwiązanie stanowi istotne ułatwienie dla przedsiębiorców, którzy mogą wybrać formę procedowania jaka będzie dla nich najwygodniejsza. Wniosek zawiera też jedynie niezbędne minimum elementem jakie potrzebne są do wydania certyfikatu. Projektowane art. 59 m-n wskazują, kiedy otrzymuje się certyfikat oraz kiedy możliwe jest wydanie deklaracji zgodności. W przypadku najniższego poziomu zaufania producent może sam przeprowadzić badanie produktu, a następnie wskazać w deklaracji zgodności, że produkt spełnia wymagania. Takie rozwiązanie stanowi ważne ułatwienie dla przedsiębiorców chcących uzyskać certyfikację przy możliwie najmniejszych kosztach. Będą mogli bowiem sami przeprowadzić niezbędne badania i wystawić deklarację zgodności. Równocześnie należy tu wspomnieć, że dalsze przepisy penalizują wprowadzanie

w błąd w zakresie spełniania wymagań certyfikacyjnych. W związku z tym istnieje zabezpieczenie przed nadużywaniem tego przepisu.

Otrzymanie certyfikatu wymaga przeprowadzenia badań produktu, usługi lub procesu przez niezależny podmiot. Jest to niezbędna gwarancja dla prawidłowego przebiegu procesu certyfikacji. Należy nadmienić, że możliwość wystawienia deklaracji zgodności dotyczy jedynie najniższego poziomu uzasadnienia zaufania.

Projektowany art. 59o daje dodatkową gwarancję dla certyfikatów najwyższego poziomu. Taki certyfikat musi być zatwierdzony przez ministra właściwego do spraw informatyzacji. Dotyczy to zarówno certyfikatów wydanych na podstawie europejskich jak i krajowych programów certyfikacji cyberbezpieczeństwa. Odmowa zatwierdzenia jest możliwa w przypadku gdy certyfikat został wydany wbrew przepisom lub postanowieniom programu certyfikacyjnego w ramach, którego prowadzona była ta procedura. Do tego postępowania będą stosowane przepisy kodeksu postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające proces prawidłowego. Wymóg ten służy do przyśpieszenia postępowania przez przekazanie do organu potrzebnych mu dokumentów. Bez tego przepisu organ musiałby wystąpić o te dokumenty co przedłużyłoby cały proces. Przepis ten reguluje również kwestie cofania certyfikatów wydanych niezgodnie z ustawą lub przepisom programu certyfikacyjnego. Obowiązek wprowadzenia takiej procedury wynika z aktu o cyberbezpieczeństwie.

Projektowane art. 59 p-r określają kwestie związane z deklaracjami zgodności. Możliwość ich wydawania dotyczy tylko najniższego poziomu uzasadnienie zaufania i daje szansę skorzystania z programów certyfikacyjnych przy minimalnych kosztach. Producenci będą mogli sami wskazać, że ich produkty spełniają wymagania bez potrzeby przechodzenia przez proces certyfikacji co pozwoli im znacząco ograniczyć posiadane koszty.

Projektowany art. 59s reguluje, kiedy jednostka oceniająca zgodność odmawia dokonania certyfikacji. Może to nastąpić jedynie w przypadku gdy dany projekt nie spełnia wymagań określonych w procesie certyfikacji. Ponadto przy odmowie certyfikacji jednostka oceniająca zgodność musi wyraźnie wskazać, które wymagania nie są spełnione przez dany produkt. Zapewnia to, że każda decyzja odmowna będzie jasno wskazywała jej przyczyny umożliwiając klientowi odwołanie się od niej.

Projektowany art. 59t reguluje jakie informacje musi zawierać certyfikat. Każdy z certyfikatów wskazuje komu został wydany, jakiego produktu dotyczy oraz kto go wydał. Ponadto każdy z nim będzie posiadał indywidualny numer, wskazywał w ramach jakiego programu został wydany, jakiego poziomu uzasadnienia zaufania dotyczy oraz okres na jaki certyfikat został wydany. Przepis ten gwarantuje, że wydany dokument będzie zawierał wszystkie informacje niezbędne do jego skutecznego wykorzystania w obrocie gospodarczym.

Projektowany art. 59u reguluje sytuację gdy produkt, usługa lub proces ICT przestają spełniać wymagania już po otrzymaniu certyfikatu. Programy certyfikacyjne będą przewidywać zasady monitorowania produktów, usług i procesów, które uzyskały certyfikaty. W ramach tego monitoringu właściciele certyfikowanych produktów będą musieli wykazać, że ich towar wciąż spełnia wymagania określone w programie. W przypadku gdy przestanie je spełniać jednostka oceniająca zgodność obowiązana jest do cofnięcia certyfikatu. Musi również o tym poinformować ministra właściwego do spraw informatyzacji. Otrzymywanie takich informacji jest niezbędny by minister mógł wykonywać swoje obowiązki związane z nadzorem nad rynkiem certyfikacji.

Zgodnie z projektowanym art. 59v podmiot, którego produkt, usługa czy proces ICT zostały certyfikowany jest obowiązany zapewnić by spełniał on wymogi określone w programie certyfikacji przez cały cykl życia danego produktu. Musi on również udostępniać użytkownikom wszelkie informacje niezbędne do bezpiecznego z nich korzystania. Postanowienia te są niezbędne do właściwego funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa. Produkty wymagają bowiem odpowiednio wyszkolonego personelu wsparcia by pełnić swą funkcję. Ponadto w przypadku wielu produktów, usług i procesów ICT ciągłe aktualizacje są niezbędnym elementem zapewnienia bezpieczeństwa. Wiele z najbardziej skutecznych cyberprzestępstw dotykało urządzeń, które nie przeszły niezbędnych aktualizacji oprogramowania jak np. w czasie rozprzestrzeniania się wirusa WannaCry. Dlatego zagwarantowanie bezpieczeństwa systemów informacyjnych wymaga nałożenia takich obowiązków na ich dostawców.

Projektowany art. 59w określa kwestię opłat za zatwierdzanie certyfikatów najwyższego poziomu zaufania. Zatwierdzanie będzie odbywało się w drodze postępowania administracyjnego, co gwarantuje zachowanie wszystkich praw stron postępowania. Opłata ta powinna pokrywać tylko niezbędne administracyjne koszty postępowania zatwierdzającego. Jej wysokość będzie zależała od stopnia skomplikowania postępowania i zakresu certyfikacji i

będzie określana w drodze rozporządzenie przez ministra właściwego do spraw informatyzacji. Równocześnie jako gwarancję, że opłaty nie będą nadmiernie obciążające wprowadzono ust. 3 który określił górną granicę opłaty na czterokrotność przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o zatwierdzenie certyfikatu.

Art.59x dodaje kolejną metodę sprawowania nadzoru przez ministra właściwego do spraw informatyzacji. Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa będę musiały przekazywać ministrowi wyjaśnienia w kwestiach związanych z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa. Daje to ministrowi możliwość sprawdzania otrzymywanych informacji bez konieczności stosowania długotrwałej i uciążliwej dla przedsiębiorcy procedury kontrolnej. Umożliwi to również ministrowi zbieranie informacji o zjawiskach zachodzących na rynku certyfikacji.

Projektowane art. 59 y-z dają podstawę prawną dla prowadzenia kontroli u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji. Do kontroli będą stosowane dotychczasowe przepisy ustawy o krajowym systemie cyberbezpieczeństwa. Dzięki temu organ będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli. Pozwoli to na najszybsze wdrożenie się organu do nowych obowiązków. W przypadku kontroli u podmiotów administracyjnych będzie stosowana ustawa o kontroli w administracji rządowej, a w przypadku przedsiębiorców stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców. W związku z tym wszelkie gwarancje dla przedsiębiorców będą zachowane w tej procedurze.

Ponadto będą tu stosowane przepisy art. 55-59 ustawy. W art. 55 w punktach od 1 do 6 wskazano zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zauważyć, że w celu uniknięcia sytuacji, w której podmiot kontrolowany zwleka z wydaniem przepustki osobie przeprowadzającej kontrolę, wskazano, że osoba prowadząca czynności kontrolne, legitymująca się odpowiednimi dokumentami upoważniającymi do kontroli, ma prawo do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki. Warto zaznaczyć, że uprawnienia wynikające z art. 55 dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych

przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że te uprawnienia nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli.

Art. 57 wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58). W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, iż protokół podpisują osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany, osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole.

W art. 59 wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie, poinformować organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń. Wskazana powyżej regulacja jest istotna z punktu widzenia regulacji zawartych w rozdziale 14 dotyczących nakładania administracyjnych kar pieniężnych. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej. Zgodnie z obowiązującymi regulacjami w podobnych dziedzinach, od zaleceń pokontrolnych nie przysługują środki odwoławcze – warto za to przypomnieć, że wymierzanie kar pieniężnych będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych (z możliwością odwołania i drogi sądowej).

Ważnym elementem zagwarantowania jakości i przejrzystości procesów oceny zgodności są przepisy dotyczące skarg. Zainteresowanym udostępniono tu dwa tryby składania skarg na jednostki oceniające zgodność. Po pierwsze jednostki te muszą udostępniać swoim klientom

procedury składania skarg do ich wewnętrznych organów, zgodnie z art. 63 ust. 1 Aktu o Cyberbezpieczeństwie (art. 59za). Dzięki temu każdy zainteresowany będzie mógł wskazać nieprawidłowości samej jednostce z którą zawarł umowę. Przepisy wskazują też na minimalne wymagania jakie muszą spełniać wewnętrzne procedury rozpatrywania skarg tak by zapewnić prawidłowy przebieg tego procesu np. obowiązek rozpatrywania skargi przez osoby, które nie prowadziły wcześniej oceny zgodności.

Równocześnie osoby zainteresowane mogą też złożyć skargę na daną jednostkę oceniającą zgodność do ministra właściwego do spraw informatyzacji (art. 59za ust. 5). Ta skarga może być podstawą do podjęcia działań nadzorczych wobec danej jednostki oraz przeprowadzenia audytu czy kontroli w tej jednostce.

Obie procedury dotyczące skarg są od siebie niezależne i mogą być prowadzone równolegle. Daje to zainteresowanym swobodę wyboru postępowania w przypadku niezadowolenia z postępowania jednostki oceniającej zgodność. Nie ograniczają też w żaden sposób uprawnień poszczególnych podmiotów do dochodzenia swoich praw na drodze sądowej.

Projektowany art. 59zb wskazuje, że minister właściwy do spraw informatyzacji jest też organem właściwym do rozpatrywania skarg na unijne i krajowe deklaracje zgodności dotyczące cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt dla którego wydano deklarację zgodności nie spełnia wymagań określonych w programie certyfikacji. To uprawnienie dla ministra wynika wprost z przepisów aktu o cyberbezpieczeństwie.

Projektowany art. 59zc wskazuje, że skargi składane do ministra właściwego do spraw informatyzacji rozpatrywane będą zgodnie z przepisami kodeksu postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra wskazano, że przepisy te będą stosowane odpowiednio.

Projektowana ustawa w zakresie, w jakim przewiduje utworzenie operatora sieci komunikacji strategicznej (rozdział 11b) zapewni funkcjonowanie operatora telekomunikacyjnego, który świadczyć będzie usługi telekomunikacyjne dla najważniejszych osób w państwie oraz jednostkom i służbom podległym oraz nadzorowanym przez Ministra Obrony Narodowej, administracji rządowej a także dla 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. Założeniem jest, że sieć komunikacji strategicznej będzie siecią zapewniającą właściwy dla realizowanych zadań poziom bezpieczeństwa przekazywanych informacji. W obecnym stanie prawnym brak jest podobnych rozwiązań.

Operatorem sieci komunikacji strategicznej będzie jednoosobowa spółka Skarbu Państwa, będąca przedsiębiorcą telekomunikacyjnym, posiadająca niezbędną infrastrukturę telekomunikacyjną oraz środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej, wyznaczona przez Prezesa Rady Ministrów w drodze zarządzenia

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.

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.

W art. 66 ust. 4 dokonuje się rozszerzenie składu Kolegium, poprzez dodanie Szefa Służby Kontrwywiadu Wojskowego albo jego zastępcy, Szefa Służby Wywiadu Wojskowego

albo jego zastępcy oraz Szefa Centralnego Biura Antykorupcyjnego albo jego zastępcy. Ponadto, umożliwiono, aby pozostali szefowie służb (wymienieni w ust. 5) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka

Zawarty w rozdziale I Konstytucji art. 20 stanowi o ustroju gospodarczym Rzeczpospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości podejmowania się działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym[3)]. Państwo może, więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[4)]. Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłoby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego a także prawno-międzynarodowym zobowiązaniom państwa jak również zdrowiu obywateli[5)]. Tutaj warto dodać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest również zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji).

W ślad za powyższym projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy

---

[3)] Wyrok Trybunału Konstytucyjnego z dnia 08 kwietnia 1998 r., sygn. K 10/97.
[4)] Ibidem.
[5)] Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01.

ICT pochodzące od dostawcy, który zostanie uznany jako dostawca wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Wymóg ten ukierunkowany jest na zapewnienie bezpieczeństwa narodowego - obecnie nie ma żadnych środków prawnych umożliwiających wycofywanie z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce. Nowe rozwiązania pozwolą na wycofanie produktów, usług i procesów ICT, które m.in. w wyniku wykorzystania znanych oraz nie wykrytych jeszcze podatności przez obce służby wywiadowcze są z powodów technicznych na tyle niebezpieczne, że ich masowe użycie w kluczowej infrastrukturze państwa mogłoby poważnie zagrozić bezpieczeństwu narodowemu. Warto tutaj dodać, że podczas pandemii COVID-19 to właśnie dzięki powszechnemu wykorzystywaniu nowoczesnych technologii zapewnianych przez produkty ICT, usługi i procesy ICT administracja rządowa, gospodarka a przede wszystkim wszyscy obywatele są w stanie bezpiecznie funkcjonować, pracować, czy uczyć się. Gdyby wskutek wykorzystania ukrytych podatności kontrolę nad tymi produktami, usługami, procesami przejęły obce podmioty mogłoby to poważnie zaszkodzić funkcjonowaniu państwa w obecnym czasie. Prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka oceny ryzyka jest zatem uzasadnione.

Proponowane przepisy będą ograniczały swobodę podejmowania decyzji gospodarczych przez podmioty zobowiązane do wycofania wskazanych w decyzji administracyjnej typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT. Wpłyną również na możliwość konkurowania na rynku typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT przez dostawcę wysokiego ryzyka. Należy przy tym zauważyć, że proponowany mechanizm zakłada przeprowadzenie transparentnego postępowania administracyjnego, które będzie mogło być skontrolowane przez sąd administracyjny. Wobec tego zostanie zapewniona możliwość obrony swoich praw przez dostawcę sprzętu lub oprogramowania. Przeprowadzając test proporcjonalności należy stwierdzić, że proponowane rozwiązania są w stanie doprowadzić do zwiększenia bezpieczeństwa narodowego oraz w świetle przedstawionego wyżej orzecznictwa Trybunału są niezbędne, aby wzmocnić bezpieczeństwo narodowe. Niewątpliwie dochodzi tutaj do kolizji dwóch wartości konstytucyjnych – swobody prowadzenia działalności gospodarczej (przez dostawcę sprzętu lub oprogramowania oraz podmioty zobowiązane do wycofania sprzętu) oraz bezpieczeństwa narodowego. Ważąc te dwie zasady wyraźnie należy stwierdzić, że przeważa ochrona bezpieczeństwa narodowego nad swobodą prowadzenia działalności gospodarczej. Prawidłowe funkcjonowanie obrotu gospodarczego nie jest możliwe w sytuacji, gdyby państwo, w ramach zapewniania swobody gospodarczej, dopuszczało do

korzystania przez podmioty gospodarcze o kluczowym dla niego znaczeniu ze sprzętu niebezpiecznego, z ukrytymi podatnościami, lub pochodzącego od dostawcy, na którego wpływ mają podmioty nastawione wrogo wobec państwa. Stałoby w jaskrawej sprzeczności z zapewnieniem swobody działalności gospodarczej, ponieważ jej wykonywanie ograniczałby wpływ podmiotów zewnętrznych. Ponadto zagrażałoby to ochronie bezpieczeństwa narodowego jako elementowi dobra wspólnego jakim jest Rzeczpospolita Polska. W sposób oczywisty stałoby to w sprzeczności z wartościami konstytucyjnymi. Dlatego należy uznać, że proponowane rozwiązania są zasadne i są w stanie skutecznie ochronić państwo i rynek nowych technologii przed produktami niebezpiecznymi.

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 będą miały zastosowanie przepisy Kodeksu 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[6)]. 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.

[6)] Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

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 nie tylko zapewnił 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.

Procedura sporządzania opinii Kolegium została określona w art. 66a ust. 7

Warto zaznaczyć, że do postępowania w sprawie uznania za dostawcę wysokiego ryzyka będą miały ogólne zasady dotyczące postępowania dowodowego z rozdziału 4 Kodeksu postępowania administracyjnego. Minister właściwy ds. informatyzacji wyda więc decyzję na podstawie nie tylko opinii Kolegium, ale również, innych dowodów przedstawionych przez stronę postępowania, jak i pozyskanych w trakcie prowadzonego postępowania dowodowego.

Po przeprowadzeniu postępowania minister właściwy ds. informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z

przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego. W doktrynie bezpieczeństwo narodowe jest rozumiane jako kategoria obejmująca bezpieczeństwo państwa, bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne, bezpieczeństwo zewnętrzne, oraz porządek publiczny[7)]. Decyzja będzie zawierać dane identyfikujące dostawcę wysokiego ryzyka oraz wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – zagrożenie dla bezpieczeństwa narodowego – decyzja ta będzie podlegała natychmiastowej wykonalności.

W celu ochrony informacji niejawnych minister właściwy ds. informatyzacji będzie mógł odstąpić od sporządzenia uzasadnienia decyzji w części dotyczącej uzasadnienia faktycznego, jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Jest to przepis szczególny w rozumieniu art. 107 § 5 Kodeksu postępowania administracyjnego.

Aby podmioty mogły zastosować się do obowiązków wynikających z decyzji administracyjnej, informacje w niej zawarte zostaną opublikowane w formie ogłoszenia w Dzienniku Urzędowym Monitor Polski, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia, a także przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów, usług i procesów, jak i używanych.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji.

[7)] Czuryk, M., Dunaj, K., Karpiuk, M., Prokop, K. Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne, Olsztyn 2016, str. 21.

Natomiast przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa Państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3.

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Podobne kompetencje będzie miał w stosunku do przedsiębiorców telekomunikacyjnych Prezes UKE.

W artykule 66d wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze lex specialis do ustawy - Prawo o postępowaniu przed sądami administracyjnymi. Jest on wzorowany na art. 38 ustawy o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[8)]. Przepis stanowi odstąpienie od zasady ustności i jawności, jednakże strona i tak będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym. Sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

[8)] Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14.

Ze względu na szczególny interes bezpieczeństwa państwa, zgodnie z art. 61 § 3 prawa o postępowaniu przed sądami administracyjnymi, dodano ust. 3 który wyłącza wstrzymanie wykonania zaskarżonej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka przez sąd administracyjny.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia.

Ostrzeżenie i polecenie zabezpieczające

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.

Zmiany w zakresie art. 73 obejmują kary dla podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. W szczególności przewidziane zostały kary dla posługiwania się certyfikatem lub deklaracją zgodności w przypadku niespełniania przez dany produkt warunków określonych w programie certyfikacji. Zapewnia to, że próby nadużycia systemu będą spotykały się ze zdecydowaną reakcją. Wysokość kar administracyjnych została odpowiednio zróżnicowana tak by były one adekwatne do dotyczących ich czynów (art. 73 ust.1a-1c).

Wprowadzono kary dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka a także dla podmiotów, do których zostało skierowane polecenie zabezpieczające. Kara będzie wynosić do 3% całkowitego rocznego światowego obrotu danego podmiotu z poprzedniego roku obrotowego. W przypadku podmiotów publicznych kara będzie wynosić do 100 000 zł. Kary będzie nakładał minister właściwy do spraw informatyzacji. Jest to spowodowane koniecznością zapewnienia jednolitej praktyki orzeczniczej.

Podkreślić należy, że potencjalna kara za niewycofanie sprzętu lub za niedostosowanie się do polecenia zabezpieczającego nie ma na celu naruszenia konstytucyjnej niezależności organów wymienionych w konstytucji. Nie dotyczy bowiem ich działalności unormowanej w Konstytucji i ustawach. Celem jest jedynie zapewnienia bezpieczeństwa wykonywanych zadań publicznych przez jednostki organizacyjne obsługujące np. Sejm, Senat, Prezydenta, Rzecznika Praw Obywatelskich, Narodowy Bank Polski.

Wprowadzono także karę dla podmiotów publicznych za nie wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Będzie ona wynosić 10 000 zł. Pomimo upływu ponad dwóch lat od uchwalenia ustawy o krajowym systemie cyberbezpieczeństwa wiele podmiotów publicznych nie wyznaczyło tych osób. Wprowadzenie sankcji za niewykonanie tego obowiązku zmotywuje podmioty publiczne do wyznaczenia tych osób.

Zmiany w obowiązujących przepisach

Zmiana zaproponowana w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne ma na celu zapewnienie odpowiednich mechanizmów Prezesowi UKE, które mogą w przyszłości doprowadzić do zintensyfikowania działań mających na celu realizację przez Rzeczpospolitą Polską celów w zakresie zapewnienia dostępu do usług szerokopasmowych każdemu obywatelowi Unii Europejskiej. Ambitne cele wynikające z unijnych dokumentów programowych, takich jak wyznaczająca cele do 2020 r. Europejska Agenda Cyfrowa, oraz Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego wskazują na konieczność realizacji celów w zakresie dostępu do sieci o bardzo dużej przepustowości, w tym dotyczące pokrycia tymi sieciami m.in. głównych szlaków komunikacyjnych do roku 2025. Projektowane zmiany przewidują możliwość przeznaczenia przez Prezesa UKE zasobów

częstotliwości, które będą mogły być przeznaczone dla przedsiębiorcy telekomunikacyjnego, który świadczyć będzie – na zasadach niedyskryminacyjnych – usługi na warunkach hurtowych w celu ich sprzedaży przez innych przedsiębiorców telekomunikacyjnych. Prezes UKE poprzedza przeznaczenie zasobów częstotliwości przeprowadzeniem analizy, która uwzględniać powinna:

1) stopień realizacji celów wynikających z dokumentów programowych Unii Europejskiej na terytorium Rzeczypospolitej;

2) możliwości efektywnego wykorzystania częstotliwości;

2) stan rynku telekomunikacyjnego;

3) plany inwestycyjne przedsiębiorców telekomunikacyjnych;

4) długoterminowe spodziewane korzyści społeczno-gospodarcze;

5) promowanie innowacyjnych usług cyfrowych.

Wynik analizy przedstawiany będzie Prezesowi Rady Ministrów, który w oparciu o wynik analiz może podjąć decyzję o wyznaczeniu przedsiębiorcy telekomunikacyjnego do oferowania usług hurtowych na zasobie częstotliwości. Kluczowe jednak w tym procesie będą wyniki analiz wykonanych przez Prezesa UKE. W przypadku gdyby wynik analizy wskazywał na to, że najbardziej efektywna realizacja przez Rzeczpospolitą Polską celów wskazanych przez europejskie dokumenty strategiczne (pokrycie szlaków komunikacyjnych i dotarcie do trudnych i oddalonych miejsc) będzie zapewniona poprzez 1 podmiot, PRM będzie uprawniony do jego wskazania. Następnie temu podmiotowi przydzielona zostanie decyzja rezerwacyjna, zgodnie z przepisami ustawy – Prawo telekomunikacyjne.

Przepisy przejściowe i przepis końcowy

Art. 3 ust. 1 zawiera przepisy dostosowujące. Według niego:

1) dotychczas powołane w ramach operatora usługi kluczowej wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo stają się SOC powołanymi w ramach operatora usługi kluczowej;

2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;

3) dotychczas powołany sektorowy zespół cyberbezpieczeństwa (CSIRT KNF) staje się CSIRT sektorowym.

Podmioty publiczne wyznaczają osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Przewidziano termin 18 miesięcy od dnia wejścia w życie ustawy na powołanie przez organy właściwe do spraw cyberbezpieczeństwa CSIRT sektorowych.

Powyższy przepis przejściowy jest niezbędny na przeprowadzenie organizacji tych zespołów, w tym na zapewnienie środków w nowej ustawie budżetowej, jak również przygotowanie niezbędnych składników materialnych i pozyskanie wysoko kwalifikowanej kadry ekspertów.

Termin vacatio legis wynosi 30 dni od dnia ogłoszenia.

Pozostałe informacje

Wpływ projektu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 4 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt został zamieszczony w wykazie prac legislacyjnych.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa oraz § 138 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Projektowana regulacja będzie poddana notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.).

Nazwa projektu
Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne

Ministerstwo wiodące i ministerstwa współpracujące
Kancelaria Prezesa Rady Ministrów
Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu
Marek Zagórski, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów

Kontakt do opiekuna merytorycznego projektu
Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl
Tomasz Wlaź, naczelnik wydziału, e-mail: tomasz.wlaz@mc.gov.pl; tel. 22 556 84 48

Data sporządzenia
20 stycznia 2020 r.

Źródło:
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
Rozporządzenie 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)

Nr w wykazie prac legislacyjnych i programowych Rady Ministrów
UD68

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa o krajowym systemie cyberbezpieczeństwa (zwana dalej „ustawą o KSC"), przyjęta w 2018 r., stanowi implementację dyrektywy NIS i tworzy podstawy prawno-organizacyjne systemu cyberbezpieczeństwa na poziomie krajowym. Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa systemów informacyjnych, utrzymania niezakłóconego świadczenia usług, a także zgłaszania i obsługi incydentów bezpieczeństwa. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów, które zostały wskazane w załączniku nr 1 do ustawy. Ustawa określa 6 kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa sektorów gospodarki tj.: energii, transportu, zdrowia, bankowości i infrastruktury rynków finansowych, zaopatrzenia w wodę oraz infrastruktury cyfrowej. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym"), który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Obecnie w krajowym systemie cyberbezpieczeństwa nie znajdują się przedsiębiorcy telekomunikacyjni, ani dostawcy usług zaufania.

Zespoły CSIRT
Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „CSIRT") poziomu krajowego. Do zadań zespołów CSIRT poziomu krajowego należy także klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej - Państwowym Instytucie Badawczym, zwanym dalej „NASK") oraz CSIRT MON (działającego w Ministerstwie Obrony Narodowej). Ustawa klarownie określa zakres kompetencyjny oraz podmiotowy wskazany dla danego zespołu CSIRT poziomu krajowego. CSIRT GOV koordynuje obsługę incydentów zgłoszonych m.in. od podmiotów administracji rządowej oraz operatorów infrastruktury krytycznej. CSIRT MON, jest właściwy do podmiotów podległych resortowi obrony narodowej. Natomiast CSIRT NASK posiada najszerszy zakres podmiotowy od operatorów usług kluczowych m.in. w sektorze bankowości po jednostki samorządu terytorialnego. Zespoły

CSIRT współpracują ze sobą na bieżąco w oparciu o procedury operacyjne. Ponadto, w przypadku wystąpienia incydentu krytycznego, zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw Incydentów Krytycznych.

Sektorowe zespoły cyberbezpieczeństwa
Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół - CSIRT KNF dla sektora bankowości i infrastruktury rynków finansowych, w Urzędzie Komisji Nadzoru Finansowego.

Pełnomocnik
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany dalej ,,Pełnomocnikiem", jest odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań dotyczących cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu lub podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy również analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników, opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium
Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej ,,Kolegium", jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje również kwestie cyberbezpieczeństwa dotyczące decyzji Prezesa UKE w sprawie rezerwacji częstotliwości. Na czele Kolegium stoi Prezes Rady Ministrów, a w jego skład – jako stali członkowie - wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów może wydać wiążące wytyczne w celu koordynacji działań w zakresie cyberbezpieczeństwa.

Doświadczenia z funkcjonowania krajowego systemu cyberbezpieczeństwa
Dwa lata doświadczeń na poziomie krajowym (od 2018 r. – wejście w życie ustawy o KSC) pozwoliły ocenić skuteczność wdrożonych rozwiązań prawno-organizacyjnych oraz zidentyfikować obszary wymagające zmian ustawowych, które usprawniają funkcjonowanie systemu cyberbezpieczeństwa m.in. konieczność ujednolicenia na poziomie krajowym procedur zgłaszania incydentów, przyspieszenie tworzenia sektorowych zespołów cyberbezpieczeństwa, czy umożliwienia tworzenia centrów analizy i wymiany informacji (ISAC).

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Dotychczas powstał tylko jeden sektorowy CSIRT w sektorze finansowym – CSIRT-KNF. Wzrasta liczba incydentów cyberbezpieczeństwa i cyberzagrożeń, co sprawia, że zachodzi konieczność ustanowienia takich zespołów dla każdego z sektorów lub podsektorów kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa i obywateli. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z cyberzagrożeniami oraz otrzymają bezpośrednie wsparcie w skutecznej reakcji na incydenty.
Ponadto, wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo (a także podmioty świadczące usługi z zakresu cyberbezpieczeństwa) nie współpracują ze sobą, co skutkuje brakiem przepływu istotnych informacji między podmiotami systemu. Operatorzy usług kluczowych mają trudności ze spełnieniem wyśrubowanych wymogów technicznych dla wewnętrznych struktur cyberbezpieczeństwa.
Należy również wskazać na konieczność uregulowania zasad współpracy pomiędzy podmiotami publicznymi funkcjonującymi na poziomie województwa. W informacji o wynikach kontroli Najwyższej Izby Kontroli z 2019 r.

negatywnie ocenione aż 70% kontrolowanych jednostek samorządu terytorialnego (JST) w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji. Co więcej, szereg incydentów bezpieczeństwa, które miały miejsce w JST w ostatnim czasie m.in. w Kościerzynie oraz Lututowie, pokazują, że zapewnienie odpowiedniej reakcji (w tym koordynacji działań) na poziomie województwa jest krytyczne.
Do tej pory powstało w Polsce tylko 1 centrum wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa – ISAC-Kolej, które rozpoczęło działalność w październiku 2020 r. ISAC (Information Sharing and Analysis Center, centrum wymiany informacji i analiz) gromadzi informacje o podatnościach i cyberzagrożeniach. Taka formuła znacząco wpływa na poprawę cyberbezpieczeństwa. Wskazane jest, aby więcej takich organizacji powstało w Polsce.

W celu wykonywania specjalistycznych analiz z zakresu cyberbezpieczeństwa oraz przygotowywania rekomendacji, zaleceń bezpieczeństwa, niezbędne jest posiadanie wysoko wykwalifikowanej kadry eksperckiej o unikalnych kompetencjach m.in. z zakresu Cyber Threat Intelligence, czy analizy złośliwego oprogramowania. Obecne środki budżetowe nie pozwalają na zatrudnienie takich osób na stawkach rynkowych w instytucjach publicznych, co powoduje że zespoły CSIRT poziomu krajowego mają ograniczoną możliwość pozyskiwania specjalistycznej kadry.

Zauważono również, że uprawnienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa są niewystarczające dla zadań, które musi wypełniać. Brakuje mu skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa, w tym przede wszystkim wydawania ostrzeżeń w sytuacji prawdopodobieństwa wystąpienia incydentu krytycznego. Chodzi o podobny instrument jaki jest m.in. w Czechach, czyli ostrzeżenie szefa agencji NUKIB.

Brakuje również środka prawnego, który umożliwiałby wydawanie rekomendacji o charakterze technicznym (w tym zakresie Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa RP na lata 2019-2024) i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa w trakcie procesu zarządzania ryzykiem.

Zmiany na poziomie UE
Ponadto, w tym samym okresie doszło do istotnych zmian w prawie europejskim. Jednym z priorytetów Komisji Europejskiej stało się zapewnienie cyberbezpieczeństwa sieciom telekomunikacyjnym. Weszła w życie nowa regulacja – dyrektywa Europejski Kodeks Łączności Elektronicznej (EKŁE), który umożliwia (w odróżnieniu od poprzedniej regulacji tzw. dyrektywy ramowej) uspójnienie procedury zgłaszania i reagowania na incydenty na poziomie krajowym. O tej możliwości, czyli zharmonizowaniu procedury zgłaszania incydentów w rozumieniu ustawy o KSC, z incydentami raportowanymi przez przedsiębiorców telekomunikacyjnych wskazuje się także w niedawno opublikowanym eksperckim opracowaniu „Synergies in Cybersecurity Incident Reporting". Jest to dokument przygotowany przez Grupę Współpracy NIS we współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, zwanej dalej „ENISA" oraz Komisję Europejską. Opracowanie wprost wskazuje, że państwa mogą dokonać harmonizacji procedur z dyrektywy NIS, EKŁE oraz rozporządzenia eIDAS, dzięki m.in. posiadaniu podobnej taksonomii w klasyfikacji incydentów, konieczności określenia progów incydentów. Co więcej podkreślono fakt, że usługi objęte tymi trzema reżimami prawnymi mają krytyczne znaczenie dla naszych społeczeństwa.
EKŁE nie jest jedynym symbolem zmian w postrzeganiu przez Komisję Europejską bezpieczeństwa w sektorze telekomunikacyjnym. Komisja wielokrotnie m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanego jako 5G Toolbox. Zestaw obejmuje zarówno narzędzia o charakterze strategicznym i technicznym, jak również te o charakterze wspierającym. Cele są dwa: po pierwsze, bezpieczeństwo sieci 5g, a po drugie: uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox zawiera też m.in. definicje zestawu środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą kręgosłupem Jednolitego Rynku Cyfrowego UE. Są środki o charakterze:

- Strategicznym - m.in. większe uprawnienia dla organów właściwych, w tym ocena bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,

- Technicznym –m.in. badanie bezpieczeństwa oprogramowania i urządzeń – uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT GOV, CSIRT MON, CSIRT NASK – wynikające z art. 33 ustawy o KSC,
- Wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa

Pakiet cyberbezpieczeństwa UE

16 grudnia 2020 r. Komisja Europejska opublikowała cały pakiet dokumentów, które ukształtują europejski ekosystem cyberbezpieczeństwa w kolejnej dekadzie. Jednym z elementów wchodzących w skład tego pakietu jest nowa Strategia Cyberbezpieczeństwa Unii Europejskiej - The EU's Cybersecurity Strategy for the Digital Decade.

Proponowane obszary interwencji i działań wzmacniających europejski system cyberbezpieczeństwa dotyczą m.in.:

- Stworzenia sieci operacyjnych centrów bezpieczeństwa (SOC) w UE. Sieci, która będzie wspierana przez innowacyjne technologie oparte m.in. o sztuczną inteligencję,
- Położony zostanie nacisk na wsparcie małych i średnich przedsiębiorstw, w tym działania dot. podniesienia świadomości, wiedzy i kompetencji pracowników.
- Rozbudowa zdolności operacyjnych na poziomie UE poprzez utworzenie Joint Cyber Unit (Wspólnego zespołu operacyjnego) odpowiedzialnego m.in. za przeciwdziałanie, odstraszaniu i reagowaniu na cyberataki.
- Wzmocniony zostanie mechanizm unijnych sankcji wobec podmiotów, w tym państwowych, przeprowadzających cyberataki.
- Zwrócono szczególna uwagę na sprawne wdrożenie zaleceń z 5G Toolbox we wszystkich państwach członkowskich.

Krajowy System Certyfikacji Cyberbezpieczeństwa
Projektowana ustawa pozwala dostosować polski porządek prawny do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia 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, zwanego dalej Aktem o Cyberbezpieczeństwie. Stanowi również realizację celu 2. Strategii Cyberbezpieczeństwa rzeczypospolitej Polskiej na lata 2019-2024 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Szczególnie istotną kwestią jest tu dostosowanie definicji zawartych w ustawie o KSC do zmian jakie zaszły w tej dziedzinie na poziomie europejskim. Prawo europejskie wprowadziło cały szereg nowych pojęć oraz dokonało aktualizacji już istniejących. Dostosowanie do tych zmian jest więc konieczne zarówno ze względu na konieczność zachowania spójności porządku prawnego jak również ze względu na korzyści wynikające z posiadania jednolitej terminologii z partnerami z Unii Europejskiej.

Rola sieci i systemów teleinformatycznych wzrosła niepomiernie w ostatnich latach sprawiając, że stały się one niezbędnym elementem współczesnej gospodarki. W związku z pandemią koronawirusa proces ten zapewne będzie postępował coraz szybciej. Jako, że społeczeństwa coraz bardziej będą polegały na produktach i usługach funkcjonujących w cyberprzestrzeni, tym istotniejsze staje się zapewnienie bezpieczeństwa działań podejmowanych w tej płaszczyźnie. Wprowadzenie jednolitych zasad przyznawania certyfikatów cyberbezpieczeństwa i ich wzajemne uznanie w państwach Unii Europejskiej zapewnią, że przedsiębiorstwa będą w stanie lepiej zabezpieczyć swoje interesy w cyberprzestrzeni. Ponadto wzajemne uznawanie certyfikatów zapewni im lepszą pozycję do konkurencji na rynku europejskim. Działania te przyczynią się do ogólnego wzrostu bezpieczeństwa w cyberprzestrzeni. Posłużą też uporządkowaniu rynku w tym zakresie oraz objęciu procesów certyfikacji nadzorem. Wyraźne wsparcie państwa w zakresie certyfikacji powinno również przyczynić się do zwiększenia świadomości społecznej w kwestii cyberbezpieczeństwa.

Szybkie przyjęcie proponowanych przepisów może dać polskim przedsiębiorcom dużą szansę do pozyskania klientów z sąsiednich krajów zainteresowanych certyfikacją ich produktów. Będzie to więc szansą dla znacznego poszerzenia bazy potencjalnych klientów.

Sama certyfikacja w zakresie cyberbezpieczeństwa jest procesem czasochłonnym i kosztownym co ogranicza dostępność do certyfikatów. Wprowadzenie krajowego systemu certyfikacji powinno przyczynić się do zmiany tego stanu rzeczy.

Przyjęte w ustawie rozwiązania umożliwiają również tworzenie krajowych programów certyfikacyjnych. Dzięki temu możliwe będzie zwiększenie cyberbezpieczeństwa w obszarach uznanych za kluczowe.
Dzięki przepisom umożliwiającym tworzenie krajowych programów certyfikacji cyberbezpieczeństwa administracja publiczna uzyska skuteczne narzędzie pozwalające reagować na cyberzagrożenia dotyczące konkretnych produktów, usług czy procesów. Możliwe będzie opracowanie programu certyfikacji, które weźmie te zagrożenia pod uwagę bez konieczności oczekiwania na działania na forum Unii Europejskiej.

Projektowana ustawa w zakresie, w jakim przewiduje utworzenie operatora sieci komunikacji strategicznej zapewni funkcjonowanie operatora telekomunikacyjnego, który świadczyć będzie usługi telekomunikacyjne dla najważniejszych osób w państwie oraz jednostkom i służbom podległym oraz nadzorowanym przez Ministra Obrony Narodowej, administracji rządowej a także dla 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. Założeniem jest, że sieć komunikacji strategicznej będzie siecią zapewniającą właściwy dla realizowanych zadań poziom bezpieczeństwa przekazywanych informacji. W obecnym stanie prawnym brak jest podobnych rozwiązań.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Oczekiwany efekt wprowadzenia ww. narzędzi interwencji:

- Przebudowany zostanie model współpracy w ramach krajowego systemu cyberbezpieczeństwa. Sektorowe zespoły cyberbezpieczeństwa i podmioty świadczące usługi z zakresu cyberbezpieczeństwa zostaną zastąpione odpowiednio przez CSIRT sektorowe i SOC (operacyjne centra bezpieczeństwa) z tylko nieco zmienionymi zadaniami.
- Zostanie dodany nowy rodzaj podmiotu – ISAC – który umożliwi nawet niewielkim a wyspecjalizowanym podmiotom na dołączenie się do krajowego systemu cyberbezpieczeństwa.
- Zostanie wzmocniona pozycja Pełnomocnika poprzez udostępnienie mu konkretnych uprawnień w zakresie wydawania ostrzeżeń o incydentach krytycznych wraz z zaleceniem określonych zachowań. Pełnomocnik będzie mógł również wydawać rekomendacje mające na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Z kolei te podmioty będą zobowiązane uwzględnić te rekomendacje podczas procesu zarządzania ryzykiem. Decyzja o zastosowaniu się do tych rekomendacji należeć będzie do tych podmiotów.
- Wojewoda będzie przekazywał informacje o cyberzagrożeniach, czy incydentach dla podmiotów publicznych – przede wszystkim JST – w regionie. Ponadto, będzie mógł koordynować wsparcie dla JST, które staną się obiektem cyberataku – koordynacja w ramach zarządzania kryzysowego.
- Minister właściwy do spraw informatyzacji dzięki nowemu uprawnieniu do wydawania poleceń zabezpieczających (w ramach transparentnej procedury administracyjnej) będzie miał skuteczne narzędzie do ograniczenia skutków incydentu krytycznego w podmiotach krajowego systemu cyberbezpieczeństwa.
- Dostawcy sprzętu i oprogramowania będą mogli zostać poddani procedurze sprawdzającej pod kątem zagrożenia jakie może wywołać wykorzystywanie oferowanego przez nich konkretnego sprzętu lub oprogramowanie w podmiotach krajowego systemu cyberbezpieczeństwa. . W przypadku, w którym zostaną zidentyfikowani jako źródło zagrożenia, zostaną m.in. wyłączeni z systemu zamówień publicznych w Polsce. Ponadto, podmioty krajowego systemu cyberbezpieczeństwa, których będzie obejmował zakres przedmiotowy oceny, będą musiały wycofać z użytkowania dany sprzęt lub oprogramowanie w ciągu 7 lat od wydania decyzji administracyjnej przez ministra właściwego ds. informatyzacji o ocenie ryzyka poziomu wysokiego.
- Powstanie Krajowy System Certyfikacji Cyberbezpieczeństwa w ramach, którego wydawane będą certyfikaty w zakresie cyberbezpieczeństwa
- Minister właściwy do spraw informatyzacji będzie przygotowywać programy na podstawie, których będzie można przeprowadzać certyfikacje. Programy te będą ostatecznie przyjmowane w drodze rozporządzenia Rady Ministrów.

- Organ nadzorczy będzie przeprowadzał kontrolę w podmiotach należących do krajowego systemu certyfikacji cyberbezpieczeństwa. W zakresie certyfikatów odwołujących się do poziomu zaufania „wysoki" będzie również zatwierdzał każdy wydany certyfikat. Rozwiązanie to jest gwarantem, że ocena zgodności na najwyższy poziom bezpieczeństwa będzie przeprowadzana zgodnie z najlepszymi standardami w tej dziedzinie.
- Określone zostały procedury akredytacji jednostek oceniających zgodność oraz procedury wydawania certyfikatów
- Określone zostały obowiązki spoczywające na podmiotach krajowego systemu certyfikacji cyberbezpieczeństwa
- Projekt zakłada stworzenie sieci komunikacji strategicznej, czyli bezpiecznej i niezawodnej sieci telekomunikacyjnej dla najważniejszych osób w państwie, najważniejszych urzędów państwowych, administracji rządowej, zarządzanej przez wskazany przez Prezesa Rady Ministrów podmiot – przedsiębiorcę telekomunikacyjnego -jednoosobową spółkę Skarbu Państwa, będąca przedsiębiorcą telekomunikacyjnym, posiadająca infrastrukturę telekomunikacyjną niezbędną do świadczenia.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

KPRM przy projektowaniu przepisów prawa dotyczących uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka – czyli wdrożenia zaleceń z tzw. 5G Toolbox, dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów:

- Francja:

Przepisy prawa już zostały zaimplementowane. Premier Francji jest organem właściwym do wydawania zezwoleń na użytek sprzętu i oprogramowania komunikacji elektronicznej, w tym także w sprawie wykluczenia określonych dostawców oprogramowania i urządzeń. Prowadzi on również wykaz urządzeń podlegających obowiązkowi wydania dedykowanego zezwolenia, który podlega zaopiniowaniu przez Urząd Regulacji Komunikacji Elektronicznej i Poczty.
Wydanie zezwolenia na wykorzystywanie urządzeń i oprogramowania podlega ocenie pod kątem ochrony interesów bezpieczeństwa narodowego i obrony państwa. Dotyczy to urządzeń, które z uwagi na swoje funkcje mogą stwarzać zagrożenie dla trwałości, integralności, bezpieczeństwa, dostępności sieci oraz poufności przesyłu danych. Przepisy odnoszą się do operatorów komunikacji elektronicznej, którzy wykorzystują urządzenia bezpośrednio lub za pośrednictwem zewnętrznych dostawców.
Przy ocenie ryzyka brany jest pod uwagę poziom zabezpieczeń urządzeń, plany operatora rozmieszczenia i sposobu wykorzystania infrastruktury oraz fakt znajdowania się danego operatora lub jego usługodawców pod wpływem państwa trzeciego niebędącego państwem członkowskim Unii Europejskiej. Odmowa udzielenia podlega obowiązkowi uzasadnienia, chyba że wiązałoby się to z ujawnieniem informacji niejawnych. Francja nie przewiduje żadnej formy rekompensaty dla przedsiębiorców, którzy będą musieli wycofać wskazany sprzęt lub oprogramowanie z eksploatacji.
Wydawane przez Premiera zezwolenia są ważne na okres od 3 do 8 lat – w zależności od rodzaju sprzętu lub oprogramowania. Za łamanie przepisów i warunków udzielonego zezwolenia przewidziane są sankcje karne w postaci 5 lat pozbawienia wolności lub grzywny w wysokości 300 000 euro.

- Wielka Brytania

Procedowany obecnie w Parlamencie Zjednoczonego Królestwa Telecommunications (Security) Act 2020 nowelizuje The Communications Act 2003. Właściwy sekretarz stanu może wydać "designated vendor directions" jeśli uważa, że są one niezbędne ze względu na interes bezpieczeństwa narodowego i jeśli nałożone przez ten środek wymagania są proporcjonalne. Do tych aktów muszą stosować się przedsiębiorcy telekomunikacyjni.
Designated vendor direction zawierają zakazy lub ograniczenia dotyczące używania produktów, usług dostarczanych przez dostawcę.
Designated vendor directions mają być przeglądane, co jakiś czas. Sekretarz stanu może wymagać od dostawców usług telekom przygotowania i przedstawienia planu wdrożenia wymagań określonych w designated vendor directions.
Dostawca zostaje określony w designation notice. Przy wydawaniu tego aktu sekretarz stanu bierze pod uwagę czynniki techniczne (jakość, niezawodność, bezpieczeństwo produktów) jak i nietechniczne (związki między dostawcą a krajem pochodzenia, tożsamość osób uczestniczących w rozwoju lub produkcji produktów).

- Finlandia

7 grudnia 2020 r. fiński parlament przyjął w nowelizacji ustawy o usługach łączności elektronicznej przepisy prawa regulujące kwestię oceny ryzyka dostawców. Organem odpowiedzialnym za ocenę sprzętu telekomunikacyjnego pod kątem zagrożenia dla bezpieczeństwa narodowego i obrony narodowej będzie Fińska Agencja Transportu i Komunikacji (The Finnish Transport

and Communications Agency, FTCA). Ponadto, projekt przewiduje całkowity, że zakaz używania sprzętu lub oprogramowania od dostawcy wysokiego ryzyka w krytycznych częściach publicznej sieci komunikacyjnej oraz w odniesieniu do krytycznych podmiotów dla bezpieczeństwa państwa, w tym m.in. elektrowni jądrowych, portów, lotnisk oraz odpowiadających im kluczowych aktywności w sieci prywatnej podłączonej do publicznej sieci komunikacyjnej (stałe ograniczenie geograficzne)
Przed podjęciem decyzji FTCA może konsultować się z właścicielem lub operatorem sieci telekomunikacyjnej w celu umożliwienia mu usunięcia zidentyfikowanych problemów bezpieczeństwa. Jednakże, jeśli sytuacja tego wymaga (pilność sprawy), a usunięcie podatności i konsultacje z operatorem nie mogą być zrealizowane, Agencja wydaje decyzje bez konsultacji z danym podmiotem.
Organem wspierającym działalność FTCA będzie nowoutworzony organ o nazwie Rada ds. Bezpieczeństwa Sieci (Network Security Advisory Board). Rada powoływana jest przez rząd i posiada kompetencje opiniodawczo-doradcze. Wydaje zalecenia m.in. w zakresie uwzględnienia kwestii bezpieczeństwa narodowego i ochrony sieci telekomunikacyjnych, w szczególności w ich krytycznych elementach. W skład Rady wchodzą m.in. przedstawiciele ministerstw oraz przedsiębiorcy telekomunikacyjni.. FTCA ma obowiązek uwzględnić opinię wydana przez Radę ds. Bezpieczeństwa Sieci.
Prawo przewiduje możliwość uzyskania pełnego odszkodowania za straty poniesione w związku z nakazem wycofania określonego sprzętu z użytku pod warunkiem, że sprzęt wprowadzono do użytku przed wejściem w życie znowelizowanej ustawy. Wysokość odszkodowania jest uzależniona od wyceny kosztów oraz poniesionych strat finansowych.

- Szwecja

Rozwiązania szwedzkie reguluje Ustawa o łączności elektronicznej. Organem uprawnionym do udzielania zezwoleń na użytek danego sprzętu i oprogramowania jest Krajowy Urząd Poczty i Telekomunikacji (The National Post and Telecom Authority, PTS), który ma obowiązek wystąpić o wiążącą opinię Służb Specjalnych (The Swedish Security Service) oraz Sił Zbrojnych Szwecji. Dostawcy sprzętu i oprogramowania oceniani są pod kątem zagrożenia dla bezpieczeństwa narodowego.
Podmioty ubiegające się o uzyskanie zezwolenia na użytek sprzętu i oprogramowania składając wniosek są zobowiązani odnieść się do kwestii dotyczących wpływu właścicieli przedsiębiorstwa na działalność wnioskodawcy. Ponadto oceniany jest poziom powiązań operatora z rządem lub władzami państw trzecich niebędących państwami członkowskimi Unii Europejskiej. Ocenie podlega także prawodawstwo państwa pochodzenia wnioskodawcy, szczególnie pod kątem poszanowania zasad praworządności i ochrony danych, powiązań operatora z państwami i organizacjami prowadzącymi ofensywne działania w cyberprzestrzeni wymierzone przeciwko Szwecji.
Wnioskodawca ma prawo odwołania się do Sądu Administracyjnego od wyroku którego przysługuje zaskarżenie do Sądu Apelacyjnego, który jest ostatnią instancją rozpatrującą sprawy z zakresu telekomunikacji.
Udzielone zezwolenie może być w każdym momencie wycofane, jeżeli zaistnieją przesłanki wskazujące na powstanie zagrożenia dla bezpieczeństwa państwa.

- Estonia

W 2020 roku Parlament Estonii (Riigikogu) przyjął nowelizację ustawy o komunikacji elektronicznej. Nowe przepisy upoważniają rząd do wprowadzenia obowiązku przedstawienia przez przedsiębiorstwo telekomunikacyjne szczegółowych informacji o sprzęcie i oprogramowaniu wykorzystywanych w sieciach komunikacji elektronicznej w celu zapewnienia bezpieczeństwa narodowego. Rząd otrzymał również uprawnienia do nałożenia na przedsiębiorcę telekomunikacyjnego obowiązku wystąpienia o pozwolenie na użytkowanie danego sprzętu lub oprogramowania.
Obecnie trwają prace nad rozporządzeniem określającym szczegółowe zasady uzyskiwania zezwoleń i składania sprawozdań, jak i organów odpowiadających za te działania.

- Niemcy

Organem właściwym w zakresie wyłączania komponentów producenta uznanego za dostawcę wysokiego ryzyka jest Federalne Ministerstwo Spraw Wewnętrznych, Mieszkalnictwa i Budownictwa. Ministerstwo określa także minimalne wymagania dotyczące uzyskiwania zezwoleń na użytkowanie sprzętu i oprogramowania przy infrastrukturze krytycznej w celu zapewnienia bezpieczeństwa narodowego.
Ocena dostawców odbywa się m.in. pod kątem rzetelności w wykonywaniu warunków udzielonego zezwolenia oraz wykorzystywania sprzętu i oprogramowania mogącego negatywnie wpływać na bezpieczeństwo, integralność lub działanie infrastruktury krytycznej.
Dostawcy usług telekomunikacyjnych mający siedzibę poza terytorium Niemiec zostali zobowiązani do utworzenia oddziału i punktu kontaktowego na terytorium RFN.

Federalny Urząd Bezpieczeństwa Informatycznego (Bundesamt für Sicherheit in der Informationstechnik, BSI) posiada uprawnienia do przeprowadzania kontroli bezpieczeństwa federalnych sieci komunikacyjnych i ich komponentów, jak i żądania dostępu do wszelkich danych podlegających przedmiotowi kontroli. BSI określa warunki techniczne sprzętu i oprogramowania kwalifikujące do uzyskania certyfikatów cyberbezpieczeństwa.
Dla produktów uznanych za bezpieczne wprowadzono także możliwość oznaczenia ich znakiem bezpieczeństwa informatycznego.
Za łamanie przepisów przewidziane są kary pieniężne w wysokości od 1 do 20 mln EUR lub 2-4% rocznego obrotu przedsiębiorstwa w zależności od tego, która kwota będzie wyższa.

- Słowacja

Projekt nowelizacji ustawy o cyberbezpieczeństwie zakłada nadanie szeregu nowych uprawnień Urzędowi ds. Cyberbezpieczeństwa (Úrad v oblasti kybernetickej bezpečnosti).
Urząd będzie mógł podjąć decyzję o nakazie wycofania z użytku komponentów określonego producenta przez operatora usługi kluczowej w celu zapewnienia bezpieczeństwa narodowego.
Do kompetencji Urzędu będzie także należało przyznawanie i odbieranie certyfikatów cyberbezpieczeństwa produktów, usług i procesów. Odwołanie od decyzji Urzędu będzie można wnieść w trybie określonym w kodeksie postępowania administracyjnego.
Ponadto operatorzy usług kluczowych, przedsiębiorcy i organy administracji publicznej zostaną zobowiązani do przedstawienia Urzędowi dokumentacji związanej z zapewnianiem cyberbezpieczeństwa.

- Rumunia

Projekt zmian przepisów prawa dot. bezpieczeństwa infrastruktury ICT i zasad wdrażania technologii 5G znajduje się na wczesnym etapie procesu legislacyjnego. Projekt przewiduje, że premier Rumunii po zasięgnięciu wiążącej opinii Najwyżej Rady Obrony Narodowej (CSAT) podejmuje decyzję o przyznaniu zezwolenia lub odmowie na korzystanie z technologii, sprzętu i oprogramowania ICT wykorzystywanych w sieci 5G. Ocenę dostawcy dokona się w oparciu o ryzyko dla bezpieczeństwa narodowego i obrony narodowej. Wniosek o wydanie zezwolenia na użytek sprzętu lub oprogramowania składać będzie producent w Ministerstwie Transportu, Infrastruktury i Łączności. Ministerstwo niezwłocznie przekaże wówczas wniosek do zaopiniowania przez CSAT. Premier wyda decyzję w ciągu 4 miesięcy od dnia złożenia wniosku. Decyzja o przyznaniu zezwolenia na użytek sprzętu i oprogramowania nie jest ostateczna. Po wystąpieniu zagrożeń dla bezpieczeństwa narodowego i obrony narodowej może zostać wycofana przez Premiera Rumunii na wniosek CSAT.
Do wniosku dostawca dołączyć ma list intencyjny podpisany przez przedstawiciela prawnego. Sam wniosek musi zawierać dane indentyfikacyjne wnioskodawcy, strukturę akcjonariatu i grupę kapitałową, do której należy oraz deklarację o spełnianiu następujących warunków: wnioskodawca nie podlega kontroli obcego rządu w przypadku braku niezależnego sądownictwa, ma przejrzystą strukturę akcjonariatu, nie stosował w przeszłości nieuczciwych praktyk handlowych, a ustawodawstwo w państwie pochodzenia wnioskodawcy gwarantuje przejrzystość praktyk handlowych.
Przysługuje procedura odwoławcza zgodnie z Kodeksem Postępowania Administracyjnego. Odwołania składa się do Sądu Apelacyjnego w Bukareszcie w ciągu 30 dni od opublikowania decyzji w rumuńskim Dzienniku Urzędowym, bez przeprowadzania procedury wstępnej.
Okres na wycofanie sprzętu nieposiadającego zezwolenia na użytkowanie wynosi 5 lat od momentu wejścia w życie ustawy.

Ostrzeżenia – doświadczenia z Czech

Czeska agencja ds. cyberbezpieczeństwa NUKIB na podstawie sekcji 12 (1) ustawy o cyberbezpieczeństwie, może wydawać ostrzeżenia do podmiotów. Ostrzeżenia wydawane są w przypadku wysokiego prawdopodobieństwa wystąpienia sytuacji kryzysowej, która może mieć krytyczne znaczenie dla bezpieczeństwa państwa. Ostrzeżenie zawiera także listę rekomendowanych działań, które podmioty powinny wdrożyć celem ograniczenia ryzyk związanych z sytuacją kryzysową. Przykłady rekomendacji: zwrócenie uwagi na określony typ cyberataków np. spear-phishingów, potrzebie zablokowania dostępu do swojej infrastruktury IT, pilnej konieczności dokonania aktualizacji oprogramowania, czy też zwrócenie szczególnej uwagi na wskazane w ostrzeżeniu domeny. Przykładem takiego ostrzeżenia jest dokument wydany 16 kwietnia 2020 r. Szefa agencji NUKIB, na podstawie analizy możliwych zagrożeń wydał ostrzeżenie dla całego państwa, ze szczególnym naciskiem na sektor ochrony zdrowia.

Certyfikacja Cyberbezpieczeństwa

Należy wskazać na wstępie, że inne państwa Unii Europejskiej nie implementowały jeszcze przepisów aktu o cyberbezpieczeństwie w związku z czym przeanalizowane rozwiązania dotyczą ogólnych przepisów związanych z certyfikacją w cyberbezpieczeństwie a nie modeli wdrożenia tego konkretnego aktu prawnego.

KPRM w kontekście zmian prawa w obszarze certyfikacji cyberbezpieczeństwa dokonał analizy rozwiązań przyjętych w następujących państwach:

· Francja

W ramach Francuskiej Agencji Cyberbezpieczeństwa (The National Cybersecurity Agency of France, zwana dalej ANSSI) kwestiami certyfikacji zajmuje się Narodowe Centrum Certyfikacji. Agencja ta zajmuje się również licencjonowaniem laboratoriów w tym zakresie.

Sama certyfikacja czy licencjonowanie nie podlega opłatom. Osoby wnioskujące ponoszą koszty badań laboratoryjnych ich produktów. Wynoszą one zwykle 600-700 euro na dzień a sama certyfikacja trwa ok. 25-35 dni. Podmioty obsługiwane są w kolejności złożenia wniosków co często powoduje, iż zainteresowani muszą czekać na otrzymanie usługi. Certyfikacji można dokonać również u autoryzowanych podmiotów działających na wolnym rynku.

System francuski zasadniczo różni się od przyjętego w niniejszej ustawie. Wynika to przede wszystkim z uwarunkowań instytucjonalnych. Niemiecki urząd wykonuje zadania niezwykle zbliżone do tych wynikających z implementowanego rozporządzenia jak również posiada zadania wykonywane w Polsce przez Agencję Bezpieczeństwa Wewnętrznego. W związku z tym rozwiązania te byłyby bardzo trudne do przeniesienia do polskiego porządku prawnego.

· Wielka Brytania

Przepisy prawa już zostały zaimplementowane. Narodowe Centrum Cyberbezpieczeństwa (The National Cyber Security Cente, NCSC) prowadzi wykaz dostawców wysokiego ryzyka. W celu zapewnienia bezpieczeństwa narodowego i zabezpieczenia krajowych sieci telekomunikacyjnych, NCSC na wniosek rządu wydaje rekomendacje mające na celu ograniczenie lub wyłączenie działalności podmiotu, którzy może zagrozić cyberbezpieczeństwu Wielkiej Brytanii.

· Szwecja

Kwestiami certyfikacji w Szwecji zajmuje się jedna z agencji rządowych - Swedish Defence Materiel Administration. Pobierana są liczne opłaty. Sam wniosek o certyfikację podlega bezzwrotnej opłacie, w wysokości 20 000 koron. Agencja ta zajmuje się również zamówieniami dla szwedzkich sił zbrojnych oraz rozwojem technologii na potrzeby wojska.

To sprzężenie kwestii cyberbezpieczeństwa w wymiarze cywilnym i wojskowym stanowi zasadniczą różnicę między polskim a szwedzkim systemem w tym zakresie.

· Włochy

Przyjęty we Włoszech model certyfikacji oparty jest na działaniach organów administracji publicznej. Certyfikaty wydawane są przez odpowiednią komórkę w Ministerstwie Rozwoju Gospodarczego. W związku z tym, ten rodzaj działalności organów administracji publicznej jest finansowany w całości z budżetu państwa. Równocześnie podmioty ubiegające się o certyfikat nie muszą wnosić opłat w związku z jego wydaniem.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	161	Wykaz OUK	Pozytywne. Motywujące operatorów usługi kluczowej do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o

			cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy. Operatorzy usług kluczowej, w wyniku utworzenia obowiązkowych już CSIRT sektorowych, otrzymają bezpośrednie wsparcie przy reagowaniu na incydenty.
Dostawcy usług cyfrowych	34	Dane własne DC KPRM	Pozytywne. Motywujące dostawców usługi cyfrowej do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy.
Podmioty publiczne	Ok. 4000	Szacunki własne	Pozytywne. Motywujące wszystkie podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Jednostki samorządu terytorialnego	16 województw, 314 powiatów i 2 477 gmin	Dane MSWiA[9]	Pozytywne. Jednostki samorządu terytorialnego będą zgłaszać incydenty w podmiocie publicznym także do wojewody, co

[9] http://administracja.mswia.gov.pl/adm/baza-jst/843,Samorzad-terytorialny-w-Polsce.html

			pozwoli na szybkie uruchomienie procedur zarządzania kryzysowego. Będą też przekazywać do wojewody dane kontaktowe osób wyznaczonych na podstawie art. 21.
Przedsiębiorcy telekomunikacyjni sporządzający plany działań	Ok. 100	Szacunki własne	Pozytywne. Przedsiębiorcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym	201	Rozporządzenie Rady Ministrów z dnia 3 listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym	Pozytywne. Przedsiębiorcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Operatorzy Infrastruktury krytycznej	128	Szacunki własne	Pozytywne. Operatorzy infrastruktury krytycznej będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego

			otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Krajowe instytucje płatnicze	38	Rejestr krajowych instytucji płatniczych	Pozytywne. Instytucje będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Kwalifikowani dostawcy usług zaufania	5	Rejestr kwalifikowanych usług zaufania	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Niekwalifikowani dostawcy usług zaufania	10	Rejestr niekwalifikowanych dostawców usług zaufania	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub

			oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Przedsiębiorcy telekomunikacyjni	4177	Rejestr przedsiębiorców telekomunikacyjnych	Pozytywne. Motywujące. Wobec nich będzie mogło być skierowane ostrzeżenie i polecenie zabezpieczające. Operator sieci komunikacji strategicznej będzie mógł się zwracać o zapewnienie odpłatnego dostępu do infrastruktury w celu świadczenia usług w sieci komunikacji strategicznej
Operator sieci komunikacji strategicznej - przedsiębiorca telekomunikacyjny, jednoosobowa spółka Skarbu Państwa	1	Wynika to z art. 59zd projektu	Będzie mógł świadczyć sieć komunikacji strategicznej.
Podmioty, którym operator sieci komunikacji strategicznej będzie świadczył usługi.	1)Kancelaria Prezydenta RP; 2) Kancelaria Sejmu; 3) Kancelaria Senatu; 4) Kancelaria Prezesa Rady Ministrów; 5) Biuro Bezpieczeństwa Narodowego; 6) urzędy 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	Wynika to z art. 59zd projektu	Pozytywne. Podmioty te będą mogły korzystać z bezpiecznej sieci rządowej komunikacji.

	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) Żandarmeria Wojskowej; 9) instytucje 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		
Państwowe Gospodarstwo Wodne Wody Polskie	1	art. 239 ustawy z dnia 20 lipca 2017 r. Prawo wodne	Pozytywne. Motywujące. Zostanie włączone do krajowego systemie cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Polski Fundusz Rozwoju SA	1	ustawa z dnia 4 lipca 2019 r. o systemie instytucji rozwoju	Pozytywny. Motywujący. Zostanie włączone do krajowego systemie cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do

			obsługi i zgłaszania incydentów w podmiocie publicznym.
Samodzielne Publiczne Zakłady Opieki Zdrowotnej	1282	Sprawozdanie o stanie Krajowego Rejestru Sądowego za sierpień 2020 r.[10]	Pozytywny. Motywujący. Zostaną włączone do krajowego systemie cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
CSIRT sektorowe	Kilka	Szacunki KPRM oparte o obecny wykaz sektorów kluczowych (załącznik 1 ustawy o ksc)	Pozytywne, Operatorzy usług kluczowych otrzymają bezpośrednie wsparcie eksperckich zespołów m.in. w obszarze obsługi incydentu, czy prowadzić dynamiczną ocenę ryzyka na rzecz operatorów.
Potencjalne ISAC	Kilkadziesiąt podmiotów	Szacunki KPRM (obecnie w ramach Partnerstwa dla Cyberbezpieczeństwa funkcjonuje 11 podmiotów, a z kolejnymi 18 trwają ustalenia warunków współpracy)	Pozytywne. Motywujące podmioty krajowego systemu cyberbezpieczeństwa do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy. Podmioty krajowego systemu cyberbezpieczeństwa ustalą zasady współpracy oraz zakres wymiany informacji. Co istotne, ISAC, które znajda się w wykazie prowadzonym przez

[10] https://www.gov.pl/web/sprawiedliwosc/SprawozdaniaKRS dostęp 15.01.2021

			ministra właściwego ds. informatyzacji będą mogły (po zawarciu porozumienia) przystąpić do systemu informacyjnego o którym mowa w art. 46.
Organy właściwe do spraw cyberbezpieczeństwa	6	-	Pozytywne. Motywujące organy właściwe ds. cyberbezpieczeństwa, nadzorujące kluczowe sektory gospodarki, do tworzenia sektorowych CSIRT, których zadaniem będzie bezpośrednie wsparcie operatorów usług kluczowych m.in. w reagowaniu na incydenty.
Wojewodowie	16	-	Pozytywne. Motywujące wojewodów do wzmocnienia współpracy i zapewnienia stałego kanału wymiany informacji m.in. o incydentach, cyberzagrożeniach i dobrych praktykach pomiędzy zespołami CSIRT poziomu krajowego a jednostkami samorządu terytorialnego.
Kolegium ds. Cyberbezpieczeństwa	1	-	Pozytywne. Kolegium otrzyma nowe kompetencje w postaci wydawania opinii w zakresie prowadzonej oceny ryzyka wobec danego dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Ponadto, Kolegium opiniuje i zatwierdza wydawanie ostrzeżeń i poleceń zabezpieczających.

Szef Agencji Wywiadu	1	-	Pozytywne. Szef AW będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Centralnego Biura Antykorupcyjnego	1	-	Pozytywne. Szef CBA będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Służby Wywiadu Wojskowego	1	-	Pozytywne. Szef SWW będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Pełnomocnik Rządu ds. Cyberbezpieczeństwa	1	-	Pozytywne. Motywujące Pełnomocnika do podejmowania aktywnych działań wynikających z otrzymania nowych kompetencji do wydawania ostrzeżeń w sytuacji podejrzenia ryzyka wystąpienia incydentu krytycznego. Ponadto, wzmocniona

			została współpraca Pełnomocnika z zespołami CSIRT poziomu krajowego.
Minister właściwy do spraw informatyzacji	1	-	Pozytywne. Minister właściwy ds. informatyzacji prowadzi wykazy ISAC oraz SOC, dzięki temu podmioty wpisane do wykazu, po zawarciu oddzielnego porozumienia z ministrem właściwym ds. informatyzacji, będą mogły przyłączyć się do systemu informacyjnego, o którym mowa w art. 46. Ponadto, wykazy zmobilizują ministra właściwego ds. informatyzacji do działań promujących korzyść iż przystąpienia do współpracy ws. systemu, o którym mowa w art. 46. Ponadto, minister prowadzi postępowania administracyjne i wydaje oceny ryzyka (po zasięgnięciu opinii Kolegium) dla dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Minister uzyska również uprawnienia kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie też prowadził postępowania administracyjne w sprawach związanych z certyfikacją np. zatwierdzał certyfikatu odnoszące się do poziomu zaufania „wysoki”.

Zespoły CSIRT	3	-	Pozytywne. Motywujące do podejmowania działań wzmacniających odporność systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa m.in. poprzez otrzymanie nowych kompetencji, w tym możliwość wykonywania (w porozumieniu) testów bezpieczeństwa. Ponadto, wzmocniona została współpraca zespołów CSIRT poziomu krajowego z Pełnomocnikiem.
Polskie Centrum Akredytacji	1		Pozytywne. Polskie Centrum Akredytacji uzyska uprawnienia do prowadzenia akredytacji w nowym obszarze tematycznym.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W dniach 30.06-8.07 2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej. Zostały również przeprowadzone konsultacje wewnątrz resortu Ministerstwa Cyfryzacji.
W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium. Powtórzono również konsultacje wewnętrzne.
Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny".
Projekt został wysłany do organizacji branżowych, organów właściwych ds. cyberbezpieczeństwa, operatorów usług kluczowych i partnerów społecznych. Ze względu na poruszaną kwestię współpracy z samorządami, zostanie skierowany do opiniowania przez stowarzyszenia zrzeszające jednostki samorządu terytorialnego.
Uzgodnienia międzyresortowe, opiniowanie oraz konsultacje publiczne trwały od 8 września do 6 października 2020 r.
Ponadto, projekt zostanie przekazany do zaopiniowania związkom zawodowym i organizacjom pracodawców. W ramach konsultacji publicznych zgłoszono 750 uwag od 114 podmiotów.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2020 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0,02	0,021	0,022	0,023	0,024	0,025	0,027	0,028	0,029	0,031	0,25
budżet państwa	0	0,02	0,021	0,022	0,023	0,024	0,025	0,027	0,028	0,029	0,031	0,25

JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	18,941	70,625	61,887	60,370	61,487	67,471	73,355	85,245	87,556	81,902	85,212	754,05
budżet państwa	18,941	70,625	61,887	60,370	61,487	67,471	73,355	85,245	87,556	81,902	85,212	754,05
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	-18,941	-70,605	-61,866	-60,348	-61,464	-67,447	-73,33	-85,218	-87,528	-81,873	-85,181	-753,8
budżet państwa	-18,941	-70,605	-61,866	-60,348	-61,464	-67,447	-73,33	-85,218	-87,528	-81,873	-85,181	-753,8
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki na ten cel z budżetu państwa w części 27 –Informatyzacja oraz w części 57 – Agencja Bezpieczeństwa Wewnętrznego a także z rezerwy celowej powstałą na budowę i funkcjonowanie CSIRT sektorowych. Wydatki z rezerwy celowej w kwocie łącznej 429,53 mln zł, na którą składają się: · Koszty budowy CSIRT sektorowych – w 2021 r. 0 zł a w 2022 r. ok 45,46 mln zł co łącznie w latach 2021 – 2031 wyniesie 429,53 mln zł Wydatki części 27 – Informatyzacja w kwocie łącznej ok. 754 mln zł, na którą składają się: · koszty obsługi i rozbudowy systemu S46, które łącznie w latach 2021 – 2031 wyniosą 166,23 mln zł · wzrost dotacji podmiotowej dla Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego – 0,425 mln zł w 2021 r. a w następnych latach wzrost dotacji o 5%, co łącznie w latach 2021 – 2031 wyniesie 33,30 mln zł. · Koszty dodatkowego wynagrodzenia dla 10 osób zatrudnionych w Kancelarii Prezesa Rady Ministrów oraz NASK-PIB w wysokości 42 000 zł brutto/osoba co daje łącznie ok. 5,1 mln zł w 2021 r. a w latach 2021 -2031 koszt ok 70 mln zł. · Stworzenie 10 stanowisk pracy w Kancelarii Prezesa Rady Ministrów w wysokości 16,89 mln zł w latach 2021-2031 w tym: w tym: wynagrodzenie roczne w wysokości 0,65 mln w 2021 r. oraz 0,95 mln od 2022 r., dodatkowe wynagrodzenie roczne w 2022 r w wysokości 0,06 mln, a od 2023 r – 0,08 mln, pochodne w wysokości 0,13 mln w 2021 r a od 2022 r. - 0,2 mln. Z tego:

	o 3 stanowiska pracy do postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka i nakładania kar administracyjnych – łącznie ok. 4,09 mln zł, o 7 stanowisk pracy do nadzoru nad Krajowym Systemem Certyfikacji Cyberbezpieczeństwa – łącznie ok 9,01 mln zł w latach 2021-2031 o koszt organizacji stanowisk pracy w wysokości 0,09 mln , w tym w 2021: 0,063 mln i w 2022: 0,027 mln. · Koszty umów zlecenia bądź umów o dzieło z ekspertami tworzącymi propozycje krajowych programów certyfikacji cyberbezpieczeństwa wyniosą w 2022 r. 0,3 mln zł, a w kolejnych latach kwota będzie zwiększać się o 5%. Łącznie w latach 2021-2031 koszty wyniosą ok 3,8 mln zł. Wydatki części 57 – Agencja Bezpieczeństwa Wewnętrznego w kwocie łącznej ok. 34,80 mln zł, na którą składają się: · dodatkowe wynagrodzenie dla 5 osób zatrudnionych lub pełniących służbę w Agencji Bezpieczeństwa Wewnętrznego w wysokości 42 000 zł brutto/osoba co daje w 2021 r. koszt ok. 2,5 mln zł w 2021 r.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Konieczne będzie sfinansowanie zadań ustawowych, przygotowania Autonomicznego Pomieszczenia Konferencyjnego (do posiedzeń niejawnych), budowę CSIRT sektorowych. Budynek Kancelarii Prezesa Rady Ministrów przy ul. Królewskiej 27 – miejsce urzędowania Pełnomocnika oraz Sekretarza Kolegium - nie posiada możliwości do prowadzenia spotkań o klauzuli „tajne". **Przystosowanie sali oraz zakup sprzętu na potrzeby posiedzeń Kolegium** to koszt 350 000 zł (2022 – 175 000 i 2023 – 175 000). W związku z nałożeniem nowych zadań dla Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego przewiduje się wzrost kwoty dotacji podmiotowej. Dotychczasowa kwota dotacji 8 500 000 zł będzie wzrastała co roku o 5%. W związku z obowiązkiem korzystania przez: · Pełnomocnika · zespoły CSIRT poziomu krajowego · Prezesa Urzędu Komunikacji Elektronicznej · zespoły CSIRT sektorowe z systemu, o którym mowa w art. 46 ustawy KSC przewidziano wzrost kwoty na dotację celową na rozwój tego systemu. Urządzenia dla Systemów Brzegowych Uczestnika (SBU) są finansowane ze środków budżetowych. SBU są w istocie elementami systemu S46 i muszą pozostawać pod kontrolą utrzymującego system. Po stronie Uczestnika pozostaną koszty związane z utrzymywaniem łączy telekomunikacyjnych do Centrów Operacyjnych systemu S46. Uczestnicy/Partnerzy (Operatorzy Usług Kluczowych, Dostawcy Usług Cyfrowych lub Podmioty Publiczne, którzy są zdefiniowani w Ustawie o Krajowym Systemie Cyberbezpieczeństwa) w związku z podłączeniem się do S46 będą musieli dedykować odpowiednie zasoby ludzkie do obsługi systemu. Koszty organizacyjne dodatkowo podnosi obsługa procesów związanych z szacowaniem ryzyka na potrzeby S46. W przypadku konieczności dodatkowego finansowania zakupu SBU, Uczestnicy mogą zrezygnować z podłączenia się do systemu S46.

Centralne finansowanie SBU zapewnia interoperacyjność sprzętu, umożliwia lepsze serwisowanie, zmniejsza koszt zakupu, usprawnia instalację logistycznie (SBU programuje i administruje nim operator S46).

Koszty transmisji pomiędzy Centrami Operacyjnymi będą finansowane ze środków budżetowych.

Komunikacja pomiędzy Centrami Operacyjnymi jest niezbędnym elementem, mającym na celu zapewnienie wysokiej dostępności S46. Organy Właściwe do spraw cyberbezpieczeństwa, uprawnione do korzystania z systemu S46, są podmiotami z sektora administracji publicznej. Zakłada się podłączanie interesariuszy ze środków dotacji przeznaczonej na rozwój S46, co upraszcza serwisowanie i logistykę podłączania. Po stronie Organu Właściwego znajdzie się koszt utrzymywania łącza telekomunikacyjnego do Centrum Operacyjnego.

Powstanie zespół na potrzeby całościowej analizy obrazu sytuacyjnego i analizy ryzyka na poziomie kraju.

Jednym z celów wytworzenia systemu S46 jest uzyskanie całościowego obrazu sytuacyjnego i szacowania ryzyka na poziomie kraju. Przetwarzanie i analizowane informacji na tym poziomie przez poszczególne CSIRT'y wiązałoby się z budowaniem kompetencji w modelu wyspowym. Co więcej doświadczenie pokazuje, że poszczególne sektory niechętnie dzielą się informacjami z własnego constituency. Wskazuje to na potrzebę zorganizowania centralnego zespołu analityków, którzy zajmowaliby się analizą danych, ich korelacją, normalizowaniem itp. - w systemie S46, na poziomie całego Państwa.
Pożądanym byłoby, aby analitycy byli zlokalizowani w podmiocie odpowiedzialnym za utrzymanie i rozwój S46.

Ilość dołączanych SBU w ciągu roku

Szacowanie liczby dołączonych SBU ma duże znaczenie dla budżetu. Założono harmonogram podłączeń, w ramach którego do maksymalnie 2023 roku będą dołączone wszystkie podmioty KSC, a następnie będą podłączane jedynie instytucje nowe lub realizujące nowe lub zmodyfikowane przedsięwzięcia, gdy zmiana powoduje, że spełniają one kryteria podłączenia do s46.

Budowa 7 zespołów CSIRT sektorowych będzie kosztownym przedsięwzięciem, które pozwoli zapełnić lukę w reagowaniu na incydenty w najbardziej narażonych sektorach gospodarki, w których incydenty mogą mieć katastrofalne skutki. W skład usług oferowanych przez CSIRT sektorowy będą usługi tzw. CERTowe (analityczne) oraz SOCowe (reagowania na incydenty).
Do obliczeń przyjęto utworzenie trzech rodzajów CSIRT sektorowych, w zależności od liczby operatorów usług kluczowych w danym sektorze i poziomu skomplikowania systemów informacyjnych w sektorze. Czasochłonność analityki kształtuje się następująco:

Rodzaj CSIRT	Średnia ilość roboczodni na miesiąc	Kosz roczny w zł	Sektory w których zostaną utworzone CSIRT sektorowe danego rodzaju
Mały CSIRT	50	594 000	· Infrastruktura cyfrowa · Zaopatrzenie w wodę i jej dystrybucja

Średni CSIRT	81	962 280	· Transport wodny · Transport lądowy i powietrzny
Duży CSIRT	111	1 318 680	· Energia · Bankowość i infrastruktura rynków cyfrowych · Ochrona zdrowia

Na potrzeby obliczeń założono wynagrodzenie rynkowe specjalistów w CSIRT sektorowych w wysokości 18 000 zł brutto m/c.

Zakłada się realizowanie następujących usług analitycznych (obliczenia czasochłonności poszczególnych zadań dokonano we współpracy z Fundacją Bezpieczeństwa Cyberprzestrzeń):

1. USŁUGA – ANALIZA ARTEFAKTÓW.	
OPIS USŁUGI	**Roboczodni**
Usługa związana ze zrozumieniem możliwości i celów działania znalezionych śladów/próbek (np. złośliwego oprogramowania, exploitów, spamu i plików konfiguracyjnych), a także sposobu ich dostarczenia, wykrywania i neutralizacji.	3-7 roboczodni
2. USŁUGA – ANALIZA POWŁAMANIOWA (INFORMATYKA ŚLEDCZA)	
OPIS USŁUGI	**Roboczodni**
Usługi obejmujące analizę danych z systemów, sieci, pamięci cyfrowych i nośników wymiennych w celu lepszego zrozumienia sposobu zapobiegania, wykrywania i/lub neutralizacji podobnych lub powiązanych incydentów. Usługi te mogą dostarczać informacji do opinii prawnych, kryminalistycznych, przeglądów zgodności lub innych przeglądów informacji historycznych.	2-6 roboczodni
3. USŁUGA – ANALIZA PODATNOŚCI	
OPIS USŁUGI	**Roboczodni**
Usługi świadczone w celu lepszego zrozumienia luk w zabezpieczeniach, które były przyczyną incydentów	4-8 roboczodni
4. USŁUGA – ROZWÓJ ORAZ ZARZĄDZANIE ŹRÓDŁAMI I DANYMI THREAT INTELLIGENCE	
OPIS USŁUGI	**Roboczodni**
Usługi świadczone na rzecz wewnętrznego lub zewnętrznego constituency w celu rozwoju i koordynowania zewnętrznych źródeł informacji dotyczących cyberzagrożeń. Usługi mogą obejmować analizę, rozwój, dystrybucję i zarządzanie informacjami o bezpieczeństwie. Dotyczą wskaźników kompromitacji, warunków logicznych detekcji, takich jak reguły i sygnatury antymalware oraz taktyki, techniki i procedury przeciwników. Usługi te zależą od działań związanych z wymianą informacji, które są zdefiniowane w obszarze usługowym numer 5 "Komunikacja".	15-20 roboczodni
5. USŁUGA – PODNOSZENIE ŚWIADOMOŚCI O ZAGROŻENIACH	
OPIS USŁUGI	**Roboczodni**
Usługi mające na celu podnoszenie świadomości o cyberzagrożeniach oraz podniesienie kompetencji w zakresie obrony przed zagrożeniami u interesariuszy.	8-15 roboczodni

6. USŁUGA – DORADZTWO W ZAKRESIE POLITYK I STRATEGII CYBERBEZPIECZEŃSTWA.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na Konsultacjach w dziedzinie polityk bezpieczeństwa, również doradzanie *constituency* w zakresie prawnych aspektów reagowania na incydenty.	1-5 roboczodni
7. USŁUGA - DZIELENIE SIĘ INFORMACJĄ I UPUBLICZNIANIE JEJ.	
OPIS USŁUGI	**Roboczodni**
Usługa dotycząca szerokiej komunikacji, uwzględniającej powiadomienia dla constituency, w celu poprawy jakości procesów biznesowych. Niektóre z przykładów to komunikaty dotyczące szkoleń, wydarzeń, nowych polityk i procedur.	1-5 roboczodni
8. USŁUGA – SZKOLENIA I EDUKACJA.	
OPIS USŁUGI	**Roboczodni**
Zdolność do realizacji określonych działań jest istotą usług CSIRT, osiąganie zdolności oznacza również szkolenia i edukację odbiorców usług CSIRT oraz samego CSIRT w tematach związanych z cyberbezpieczeństwem, zabezpieczeniem informacji i reagowaniem na incydenty. Kompetencje oznaczają zdolność do realizacji działań na pewnym poziomie dojrzałości.	2-5 roboczodni
9. USŁUGA – ORGANIZACJA ĆWICZEŃ.	
OPIS USŁUGI	**Roboczodni**
Usługi oferowane przez organizację na rzecz przedstawicieli constituency wspierające przygotowanie, przeprowadzenie i ocenę ćwiczeń w cyberprzestrzeni, mających na celu szkolenie i/lub ocenę możliwości poszczególnych przedstawicieli constituency i interesariuszy jako całości.	1-5 roboczodni
10. USŁUGA – DORADZTWO TECHNICZNE.	
OPIS USŁUGI	**Roboczodni**
Usługa, która koncentruje się na rekomendowaniu, opracowywaniu, dostarczaniu i nabywaniu dla interesariuszy infrastruktury, narzędzi i usług związanych z cyberbezpieczeństwem. Wszystkie te systemy i narzędzia odnoszą się do CSIRT/bezpieczeństwa, a nie ogólnie do technologii informacyjnych; systemy te mogą obejmować portale powiadamiania/ostrzegania. Należy zwrócić uwagę, że zespół CSIRT może dostarczyć zainteresowanym stronom pewne narzędzia jako usługę.	5-10 roboczodni
11. USŁUGA – GROMADZENIE I WYKORZYSTANIE NABYTYCH DOŚWIADCZEŃ	
OPIS USŁUGI	**Roboczodni**
Obsługa incydentów jest działaniem reaktywny. W większości przypadków czas na reakcję jest krótki, a początkowa sytuacja niejasna. Pierwotne przyczyny wielu incydentów są ukryte i wymagają usunięcia na późniejszym etapie. Usługa ta ma na celu zapobieganie podobnym incydentom i poprawie reakcji na podobną lub ogólniejszą sytuację.	1-5 roboczodni
12. USŁUGA – ROZWÓJ METODYK ZARZĄDZANIA PODATNOŚCIAMI.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na definiowaniu, identyfikacji zdolności i ulepszaniu metodyk świadczenia usług związanych z podatnościami lub koordynacji działań innych podmiotów w tym zakresie.	2-6 roboczodni
13. USŁUGA – ROZWÓJ TECHNOLOGII I PROCESÓW THREAT INTELLIGENCE.	
OPIS USŁUGI	**Roboczodni**

Usługa polegająca na definiowaniu, identyfikacji zdolności i ulepszaniu metodyk niezbędnych do wykonywania usług analizy i rozpowszechniania informacji, związanych z threat intelligence.	3-8 roboczodni
14. USŁUGA – ROZWÓJ WŁASNYCH NARZĘDZI CYBERBEZPIECZEŃSTWA.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na rozwijaniu, identyfikacji nowych zdolności i współdzieleniu pomysłów dotyczących nowych narzędzi w celu zautomatyzowania procesów CSIRT-u.	2-6 roboczodni
Razem	50-111

Usługi SOCowe w ramach CSIRT sektorowego zakładają stopniowe budowanie trzech linii wsparcia (od 14 pracowników w pierwszym roku działania do 21 pracowników w trzecim):

SOC – etaty			2021		2022		2023	
Typ stanowiska	Koszt miesięczny		FTE[11])	Roczny budżet	FTE	Roczny budżet	FTE	Roczny budżet
Operator I linii		12 000,00	10	1 440 000,00	15	2 160 000,00	15	2 160 000,00
Analityk II linii		16 000,00	2	384 000,00	2	384 000,00	3	576 000,00
Ekspert III linii	Etatowy	20 000,00	1	240 000,00	2	480 000,00	2	480 000,00
	Koszty zewnętrzne:	20 000,00		240 000,00		240 000,00		240 000,00
Administrator SOC		15 000,00	1	180 000,00	1	180 000,00	1	180 000,00
SUMA		83 000,00	14	2 484 000,00	20	3 444 000,00	21	3 636 000,00

Źródło: analizy własne DC KPRM.

Do kosztów działania usług SOCowych w ramach CSIRT sektorowych należy doliczyć koszty administracyjne i sprzętu (3 mln zł w pierwszym roku i potem 30% rocznie na aktualizację i wymianę sprzętu).

Dodatkowe wynagrodzenia dla ekspertów z zakresu cyberbezpieczeństwa

Ustawa pozwoli na przyznanie dodatkowego wynagrodzenia w wysokości nie wyższej niż 15-krotność wynagrodzenia minimalnego dla 20 osób zatrudnionych lub pełniących służbę w CSIRT MON, CSIRT NASK, CSIRT GOV oraz w urzędzie obsługującym Pełnomocnika Rządu do spraw cyberbezpieczeństwa. Umożliwi to zatrudnienie na stawkach rynkowych wysoko wykwalifikowanych specjalistów, którzy będą mogli dokonywać analiz na zlecenie Pełnomocnika i Kolegium. Kwota wynagrodzenia dodatkowego zostanie ustalona w rozporządzeniu Rady Ministrów.

Wsparcie osobowe Kancelarii Prezesa Rady Ministrów

Aby zapewnić efektywność postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka oraz postępowań w sprawach nałożenia administracyjnych kar pieniężnych za nie wycofanie produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka przewiduje się wzmocnienie Kancelarii Prezesa Rady Ministrów o 3 etaty.

11) FTE – Full Time Equivalent.

Utworzenie wydziału krajowego systemu certyfikacji cyberbezpieczeństwa

W ramach przyjęcia nowych zadań przez ministra właściwego do spraw informatyzacji konieczne jest wzmocnienie urzędu obsługującego ten organ. W celu sprawnego wykonywania nowych zadań konieczne będzie utworzenie nowego wydziału i zatrudnienie pracowników. W pierwszym roku obowiązywania nowej ustawy konieczne będzie zatrudnienie 4 osób. Pracownicy tworzonego wydziału będą zajmować się przede wszystkim prowadzeniem postępowań administracyjnych, analizą rynku i współpracą międzynarodową. W związku z rozwojem rynku certyfikacji konieczne będzie również wzmocnienie nowoutworzonego wydziału w kolejnych latach – przewidujemy konieczność zatrudnienia kolejnych 3 osób w kolejnym roku.

Od 2022 r. podjęte zostaną prace nad tworzeniem krajowych programów certyfikacji cyberbezpieczeństwa. W ich ramach konieczne będzie wypracowanie standardów technicznych oraz wymagań na kilka poziomów uzasadnienia zaufania, co w praktyce oznacza konieczność przygotowania kilku szczegółowych dokumentów technicznych w ramach jednego krajowego programu certyfikacji cyberbezpieczeństwa. Zadania to będzie zlecane na rynek w formie zamówienia publicznego. Ponadto krajowe programy certyfikacji cyberbezpieczeństwa będą stanowiły nowy rodzaj dokumentów technicznych, co potencjalnie wpływa na wzrost ceny. Wypracowane rozwiązania muszą też uwzględniać stan wiedzy technicznej i najlepsze praktyki w dziedzinie cyberbezpieczeństwa. Koszt obejmuje również przeniesienie majątkowych praw autorskich do wypracowanych dokumentów. Biorąc pod uwagę, że dotychczas podobne usługi związane ze wsparciem ekspertów kosztowały ok. 100 000 zł, mając równocześnie dużo mniejszy zakres czynności, przyjęto, że koszty wykonania tego zadani będzie wynosił 300 000 zł.

Powstanie operatora sieci komunikacji rządowej
Oszacowanie skutków finansowych dla budżetu państwa w zakresie korzystania przez najważniejsze urzędy w państwie oraz służby specjalne czy też służby bezpieczeństwa i porządku publicznego, a także ochrony granic, ochronę zdrowia nie możliwe do oszacowania na tym etapie.
Jednakże, mając na uwadze, że działalność operatora sieci komunikacji strategicznej polegać będzie na świadczeniu zcentralizowanych usług, które w tej chwili świadczone są przez różne podmioty, spodziewane są w tym zakresie znaczne oszczędności. Podobnie należy spodziewać się oszczędności dla budżetu państwa w związku z centralizacją zakupów licencji na oprogramowanie niezbędne dla prawidłowego funkcjonowania usług komunikacji elektronicznej czy też zakupów niezbędnych urządzeń. Dodatkowym, niemierzalnym skutkiem dla budżetu państwa jest zapewnienie takiego funkcjonowania bezpiecznego ekosystemu sieci telekomunikacyjnej dla najważniejszych osób, urzędów i służb w państwie, który do minimum ograniczy incydenty bezpieczeństwa i konieczność reagowania na nie.

Dochody budżetu państwa

Przewidujemy dwa postępowania o zatwierdzenie certyfikatów poziomu uzasadnienia zaufania wysoki w ciągu roku. Przeciętna opłata za zatwierdzenie takiego certyfikatu będzie wynosić 10 000 zł. W kolejnych latach przewidujemy wzrost opłat o ok. 5% w skali rocznej.

Nie można w tej chwili oszacować ile wpływów do budżetu państwa przyniosą wpływy z kar administracyjnych za niewycofanie sprzętu lub oprogramowania dostawcy wysokiego ryzyka. Nie można określić w tej chwili ile podmiotów i kiedy będzie musiało wycofać sprzęt lub oprogramowanie dostawcy wysokiego ryzyka, ponieważ żaden dostawca nie został uznany za

	dostawcę wysokiego ryzyka. W konsekwencji trudno oszacować, kiedy i ile podmiotów podlegałoby karze za nie wycofanie sprzętu lub oprogramowania dostawcy wysokiego ryzyka. Nie można w tej chwili oszacować ile wpływów do budżetu państwa przyniosą wpływy z kar administracyjnych za niedostosowanie się do polecenia zabezpieczającego. Ten środek prawny będzie wydawany po wystąpieniu incydentu krytycznego. Trudno przewidzieć czy i kiedy taki incydent wystąpi. Dlatego też nie jest możliwe oszacowanie ile podmiotów oraz kiedy podlegałoby karze za niedostosowanie się do polecenia zabezpieczającego. **Do wszystkich kosztów dodano spodziewany wzrost cen, zgodnie z tabelami makroekonomicznymi MF.**

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki									
Czas w latach od wejścia w życie zmian			0	1	2	3	5	10	*Łączne (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)		duże przedsiębiorstwa	-	-	-	-	-	-	-
		sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
		rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
		(dodaj/usuń)	-	-	-	-	-	-	-
W ujęciu niepieniężnym		duże przedsiębiorstwa	Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa spowodują konieczność wypracowania przez operatorów usług kluczowych procedur kontaktu z zespołami CSIRT sektorowymi Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się podmiotami prowadzącymi SOC na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji SOC będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Oznaczać to będzie, że wprowadzone środki techniczne i organizacyjne będą mogły różnić się od dotychczas wprowadzonych, ponieważ to SOC będzie o nich decydował. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorstwami) w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka). Podkreślenia wymaga, że wycofaniu będzie podlegał produkty, usługi, procesy określone w decyzji – a więc nie wszystkie produkty (usługi, procesy) oferowane przez dostawcę wysokiego ryzyka.						

			Natomiast przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa Państwa funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku. Podmioty zobowiązane do wycofania produktów, usług i procesów pochodzących od dostawcy wysokiego ryzyka nie będą mogły ich zamawiać poprzez Prawo zamówień publicznych, jeżeli do nich stosuje się ta ustawa. Ponadto, w wyniku wydania decyzji administracyjnej ws. polecenia administracyjnego, podmioty krajowego systemu cyberbezpieczeństwa, których będzie dotyczyła ta decyzja m.in. zakazującej korzystania z określonego oprogramowania, które zostało wskazane jako stanowiące zagrożenie dla wystąpienia incydentu krytycznego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Nowelizacja wprowadza kary za niedostosowanie się do obowiązku wycofania produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka a także za niedostosowanie się do obowiązku wykonania określonego zachowania zawartym w poleceniu zabezpieczającym. Kary te wyniosą do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Oczywiście znajdą tutaj zastosowanie przepisy dotyczące administracyjnych kar pieniężnych z Kodeksu postępowania administracyjnego.
		sektor mikro-, małych i średnich przedsiębiorstw	Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa spowodują konieczność wypracowania przez operatorów usług kluczowych procedur kontaktu z zespołami CSIRT sektorowymi Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się podmiotami prowadzącymi SOC na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji SOC będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Oznaczać to będzie, że wprowadzone środki techniczne i organizacyjne będą mogły różnić się od dotychczas wprowadzonych, ponieważ to SOC będzie o nich decydował. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny

			ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka). Obowiązek wycofania produktów, usług i procesów dostawcy wysokiego ryzyka nie będzie dotyczył mikro-, małych i średnich przedsiębiorców telekomunikacyjnych, ponieważ będzie on dotyczył wyłącznie przedsiębiorców telekomunikacyjnych sporządzających plany działań w sytuacji szczególnego zagrożenia, których w tej chwili jest około 100. Są to najwięksi przedsiębiorcy telekomunikacyjni w Polsce. Ponadto, w wyniku wydania decyzji administracyjnej ws. polecenia administracyjnego, podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni (wszyscy), operatorzy infrastruktury krytycznej, przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym, dostawcy usług zaufania których będzie dotyczyła ta decyzja m.in. zakazującej korzystania z określonego oprogramowania, które zostało wskazane jako stanowiące zagrożenie dla wystąpienia incydentu krytycznego.
		rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów.
		Jednostki samorządu terytorialnego	Jednostki samorządu terytorialnego będą zobowiązane przekazać do wojewody zgłoszenie o incydencie w podmiocie publicznym równocześnie ze zgłoszeniem do właściwego zespołu CSIRT poziomu krajowego. Obowiązkiem tych jednostek będzie także przekazanie do wojewody danych kontaktowych do osoby odpowiedzialnej za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa. Każdy wojewoda zapewni współpracę na linii administracja rządowa – administracja samorządowa, w tym usprawnienie wymiany informacji o incydentach, cyberzagrożeniach i podatnościach. JST, poprzez wojewodę, otrzymają dostęp do rekomendacji, zaleceń oraz zestawów poradników i dobrych praktyk, wydawanych przez zespoły CSIRT poziomu krajowego oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Wprowadzone przepisy w zakresie certyfikacji zapewnią większą dostępność rozwiązań technicznych zapewniających bezpieczeństwo indywidualnym użytkownikom Jednostki samorządu terytorialnego są zobowiązane na podstawie paragrafu 20 rozporządzenia o Krajowych Ramach Interoperacyjności[12)] do przeprowadzania zarządzania ryzykiem. Wobec tego będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w

[12)] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

			celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Natomiast decyzja o uwzględnieniu tych środków będzie należała wyłącznie do nich. .
Niemierzalne		Koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym w związku z wycofaniem produktów, usług i procesów pochodzących od dostawców wysokiego ryzyka ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
		Koszty związane z wykonaniem polecenia zabezpieczającego	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania polecenia zabezpieczającego w formie decyzji administracyjnej. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, dostawcy usług zaufania, krajowe instytucje płatnicze ponieważ polecenie zabezpieczające będzie wydawane po wystąpieniu incydentu krytycznego. Będzie wskazywało obowiązek zachowania adekwatny do charakteru incydentu krytycznego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń			Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu (operator usług kluczowych, dostawca usług cyfrowych, SOC, przedsiębiorców telekomunikacyjnych) i sektora.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:
Ustawa spowoduje zmniejszenie w niektórych obszarach (SOC) obciążeń regulacyjnych, za to wprowadzi nowe – dla ISAC, wojewodów oraz dostawców sprzętu lub oprogramowania.

Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.

Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa.

Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka).

Podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, dostawcy usług zaufania, krajowe instytucje płatnicze będą podlegali polecenia zabezpieczającego, jeżeli zostanie wydane.

Dobrowolny charakter certyfikacji sprawia, że nie dojdzie do zmiany obciążeń regulacyjnych spoczywających na przedsiębiorcach. Uczestnicy krajowego systemu certyfikacji cyberbezpieczeństwa będą musieli stosować przepisy niniejszej ustawy związane z kontrolą zarówno ze strony Polskiego Centrum Akredytacji jak i ministra właściwego do spraw informatyzacji. Udział w tym systemie jest jednak całkowicie dobrowolny.

9. Wpływ na rynek pracy

Sektor cyberbezpieczeństwa jest jednym z najbardziej dynamicznych sektorów gospodarki. W I kwartale 2019 roku odnotował on wzrost o 14,2 %. Cyberprzestępstwa wskazywane są jako jedne z pięciu najistotniejszych zagrożeń dla firm obok m.in. katastrof naturalnych. Na tak szybko zmieniającym się rynku certyfikaty w zakresie cyberbezpieczeństwa będą cenną pomocą co do wyboru określonych produktów ICT. Przyczyni się to do większego wykorzystania bezpiecznych rozwiązań w sektorze przedsiębiorstw.

Projekt wygeneruje konieczność zatrudnienia wysoko wykwalifikowanych specjalistów zajmujących się cyberbezpieczeństwem a także przekwalifikowania dotychczas posiadanej kadry. Ponadto, pojawi się okazja do rekwalifikacji kadr oraz systemowego podnoszenia kompetencji i wiedzy osób zatrudnionych w podmiotach krajowego systemu cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☒ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☒ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Ustawa zwiększy poziom bezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, w tym spółek Skarbu Państwa i jednostek samorządu terytorialnego. Projekt spełnia wymagania interoperacyjności, czyli zdolność systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach. Projekt spełnia również wymogi neutralności technologicznej, wykorzystania danych z rejestrów publicznych oraz ochrony danych osobowych.

11. Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie po upływie 30 dni od ogłoszenia.

Z chwilą wejścia w życie ustawy:

1. wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej staną się SOC powołanymi w ramach operatora usługi kluczowej;
2. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę staną się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;
3. sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym stanie się CSIRT sektorowym.
4. Podmioty publiczne wyznaczają osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.
5. Organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na ustanowienie CSIRT sektorowego

Pierwszym krokiem jest stworzenie jednolitych procedur akredytacji i certyfikacji na potrzeby cyberbezpieczeństwa. Równocześnie utworzony zostanie organ nadzoru, który będzie monitorował rozwój rynku certyfikacji. Odpowiednie działania zostaną podjęte w Kancelarii Prezesa Rady Ministrów. Zatrudnione zostaną dodatkowe osoby, które będą prowadziły postępowania administracyjne oraz przeprowadzały kontrole zgodnie z niniejszą ustawą. Działania te zostaną rozpoczęte w 2021 roku, a zgodnie z przewidywaniami ta komórka organizacyjna osiągnie pełną skład osobowy w 2020 roku.
Przyznanie uprawnień akredytacyjnych, w tym zakresie, PCA pozwoli w możliwie krótkim horyzoncie czasowym rozpocząć akredytację jednostek certyfikacyjnym i jednostek oceniających zgodność.

Organ nadzoru będzie również w stanie określić czy istnieje potrzeba wprowadzenia krajowych programów certyfikacyjnych. Początkowo certyfikacja odbywać się będzie w ramach europejskich programów certyfikacji.

6. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ustawa będzie podlegać ocenie w ramach prac nad przeglądem Strategii Cyberbezpieczeństwa RP na lata 2019-2024. Regularny przegląd aktów prawnych kształtujących funkcjonowanie krajowego systemu cyberbezpieczeństwa jest stałym zadaniem wpisanym do Planu działania na rzecz wdrożenia Strategii Cyberbezpieczeństwa.

7. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Dokumenty źródłowe:

1. *Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques*
2. Telecommunications (Security) Bill https://services.parliament.uk/bills/2019-21/telecommunicationssecuritybill.html
3. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) https://www.zakonyprolidi.cz/cs/2014-181
4. The EU's Cybersecurity Strategy for the Digital Decade https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade