Projekt z dnia 7 września 2020 r.

U S T A W A

z dnia …… 2020 r.

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

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 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:
      „4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;”,
   b) w ust. 2 uchyla się pkt 1 i 2;
2) w art. 2:
   a) po pkt 3 dodaje się pkt 3a-3e 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) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej;
      3c) ISAC – centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;
      3d) SOC – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie;
      3e) dostawca sprzętu lub oprogramowania – oznacza producenta, upoważnionego przedstawiciela, importera i dystrybutora, o których mowa w rozporządzeniu (WE) nr 765/2008:
      a) produktów ICT, usług ICT i procesów ICT w rozumieniu art. 2 pkt 12-14 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 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151, s. 15),

b) produktów i usług dla infrastruktury telekomunikacyjnej, o której mowa w art. 2 pkt 14 ustawy z dnia … – Prawo komunikacji elektronicznej;”,

b) po pkt 8 dodaje się pkt 8a-8g w brzmieniu:

„8a) incydent telekomunikacyjny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej;

8b) przedsiębiorca komunikacji elektronicznej – podmiot, o którym mowa w art. 2 pkt 41 ustawy z dnia … – Prawo komunikacji elektronicznej;

8c) dostarczanie sieci telekomunikacyjnej – działalność, o której mowa w art. 2 pkt 6 ustawy z dnia … – Prawo komunikacji elektronicznej;

8d) usługi komunikacji elektronicznej – usługi, o których mowa w art. 2 pkt 76 ustawy z dnia … – Prawo komunikacji elektronicznej;

8e) telekomunikacyjne urządzenia końcowe – urządzenia, o których mowa w art. 2 pkt 71 ustawy z dnia … – Prawo komunikacji elektronicznej;

8f) bezpieczeństwo sieci i usług -– zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:

a) tych sieci lub usług,

b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,

c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;

8g) sytuacja szczególnego zagrożenia – sytuacja, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej;”;

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) po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) przedsiębiorców komunikacji elektronicznej;”,

b) po pkt 5 dodaje się pkt 5a w brzmieniu:

„5a) CSIRT Telco;”,

c) 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 i 9”,

d) po pkt 7 dodaje się pkt 7a-7c w brzmieniu:

„7a) Urząd Komisji Nadzoru Finansowego;

7b) podmioty wskazane w art. 7 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);

7c) ISAC;”,

e) pkt 16 otrzymuje brzmienie:

„16) SOC;”;

5) po art. 4 dodaje się art. 4a w brzmieniu:

„Art. 4a. 1. W ramach krajowego systemu cyberbezpieczeństwa może funkcjonować ISAC, do którego zadań należy w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów.

2. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC.

3. Wykaz ISAC zawiera:

1) nazwę (firmę) ISAC;

2) imię i nazwisko osoby reprezentującej ISAC wraz z danymi kontaktowymi;

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 CSIRT MON, CSIRT NASK lub CSIRT GOV. 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 na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji.

9. ISAC współpracują z CSIRT MON, CSIRT NASK lub CSIRT GOV oraz przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.

10. 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.”;

6) 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.”;

7) 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,”;

8) w art. 10 w ust. 2 pkt 2 otrzymuje brzmienie:

„2) ochronę dokumentów przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”;

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 cyberbezpieczeństwa 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 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. 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 właściwości, w tym:
   a) oferowany rodzaj wsparcia,
   b) zasady współpracy i wymiany informacji,
   c) politykę komunikacji i uwierzytelniania informacji;
3) oferowane usługi, w tym 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 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 organowi właściwemu do spraw cyberbezpieczeństwa, 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) Policji;
2) Żandarmerii Wojskowej;
3) Straży Granicznej;
4) Centralnemu Biuru Antykorupcyjnemu;
5) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
6) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
7) sądom;
8) prokuraturze;
9) organom Krajowej Administracji Skarbowej;
10) dyrektorowi Rządowego Centrum Bezpieczeństwa;
11) Służbie Ochrony Państwa.”;

12) po rozdziale 4 dodaje się rozdział 4a w brzmieniu:

„Rozdział 4a

Obowiązki przedsiębiorców komunikacji elektronicznej

Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia.

2. Przedsiębiorca komunikacji elektronicznej:

1) przeprowadza systematyczną ocenę ryzyka wystąpienia sytuacji szczególnego zagrożenia;
2) podejmuje środki techniczne i organizacyjne zapewniające poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:
   a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, o której mowa w art. 2 pkt 14 ustawy z dnia … – Prawo komunikacji elektronicznej,
   b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia,

c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,

d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej

– przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków;

3) dokumentuje czynności, o których mowa w pkt 1 i 2.

3. Przedsiębiorca komunikacji elektronicznej, o którym mowa w art. 2 pkt 42 ustawy – Prawo komunikacji elektronicznej, sporządzający plan, o którym mowa w art. 47 ust. 1 tej ustawy, dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2.

4. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności, biorąc pod uwagę skalę działalności, wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, lub sposób ich dokumentowania, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci i usług.

Art. 20b. Przedsiębiorca komunikacji elektronicznej:

1) zapewnia obsługę incydentu;

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań.

Art. 20c. 1. Przedsiębiorca komunikacji elektronicznej, sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy – Prawo komunikacji elektronicznej:

1) klasyfikuje incydent jako incydent telekomunikacyjny na podstawie progów uznania incydentu za telekomunikacyjny;

2) zgłasza incydent telekomunikacyjny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

3) współdziała podczas obsługi incydentu telekomunikacyjnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.

3. Przedsiębiorca komunikacji elektronicznej niezależnie od zadań określonych w ust. 1:

1) przekazuje jednocześnie CSIRT Telco w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 2;
2) współdziała z CSIRT Telco podczas obsługi incydentu telekomunikacyjnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;
3) zapewnia CSIRT Telco dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.

4. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia progi incydentu telekomunikacyjnego, których przekroczenie powoduje powstanie obowiązku zgłoszenia incydentu, uwzględniając:

1) liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ,
2) czas trwania skutków incydentu telekomunikacyjnego,
3) obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego,
4) zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług,
5) wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej,
6) wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
7) wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych, o których mowa w art. 2 pkt 29 ustawy z dnia … – Prawo komunikacji elektronicznej,
8) wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków, o których mowa w art. 47-62 ustawy z dnia … – Prawo komunikacji elektronicznej

– kierując się rekomendacjami lub wytycznymi Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA) oraz koniecznością zapewnienia Prezesowi Urzędu Komunikacji Elektronicznej informacji niezbędnych do właściwego realizowania jego

obowiązku, o którym mowa w art. 382 ust. 1 pkt 11 ustawy z dnia … – Prawo komunikacji elektronicznej.

Art. 20d. 1. Zgłoszenie, o którym mowa w art. 20c ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, jeśli został nadany;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu telekomunikacyjnego na świadczenie usługi komunikacji elektronicznej, w tym:
   a) usługi komunikacji elektronicznej zgłaszającego, na które incydent telekomunikacyjny miał wpływ,
   b) liczbę użytkowników usługi komunikacji elektronicznej, na których incydent telekomunikacyjny miał wpływ,
   c) moment wystąpienia i wykrycia incydentu telekomunikacyjnego oraz czas jego trwania,
   d) zasięg geograficzny obszaru, którego dotyczy incydent telekomunikacyjny,
   e) wpływ incydentu telekomunikacyjnego na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
   f) przyczynę zaistnienia incydentu telekomunikacyjnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi komunikacji elektronicznej;
5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;
6) w przypadku incydentu, który mógł mieć wpływ na świadczenie usługi komunikacji elektronicznej, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;
7) informacje o podjętych działaniach zapobiegawczych;
8) informacje o podjętych działaniach naprawczych;
9) inne istotne informacje.

2. Przedsiębiorca komunikacji elektronicznej przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu telekomunikacyjnego.

3. Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20c ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco.

4. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco może zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu.

5. W zgłoszeniu przedsiębiorca komunikacji elektronicznej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 20e. 1. Przedsiębiorca komunikacji elektronicznej wykonujący działalność na rynku detalicznym, w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego, informuje o nim swoich użytkowników, na których takie zagrożenie może mieć wpływ, w tym o możliwych środkach, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach.

2. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 1, informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.

Art. 20f. W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, może zastosować środki polegające na:

1) zablokowaniu przesłania takiego komunikatu,
2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu

- w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.

13) w art. 22 w ust. 1 po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) będący jednostką samorządu terytorialnego, niezależnie od obowiązku, o którym w pkt 2, zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego wojewody; ”;

14) po art. 24 dodaje się art. 24a w brzmieniu:

„24a. Wojewoda:

1) zapewnia wymianę informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dotyczących podmiotów publicznych w województwie;
2) prowadzi listę danych kontaktowych osób z poszczególnych podmiotów publicznych 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 w 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.

15) w art. 26:

a) ust 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek podmiotów krajowego systemu cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów. ”,

b) w ust. 3 w pkt 16 kropkę zastępuje się średnikiem i dodaje się pkt 17-21 w brzmieniu:

„17) gromadzenie informacji dotyczących zagrożeń cyberbezpieczeństwa, podatności i incydentów;
18) przygotowywanie na zlecenie Pełnomocnika analiz w zakresie zagrożeń cyberbezpieczeństwa, 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 cyberbezpieczeństwa 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 zagrożeniach cyberbezpieczeństwa.”,

c) w ust. 4 wyrazy „sektorowymi zespołami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowymi i CSIRT Telco”,

d) użyte w art. 26 w ust. 3 w pkt 16 oraz w art. 49 w ust. 3 w pkt 2 w różnej liczbie i różnym przypadku, wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa”;

16) art. 32 ust. 4 otrzymuje brzmienie:

„4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco 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.”;

17) art. 34 ust. 1 otrzymuje brzmienie:

„1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco oraz SOC współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”;

18) po art. 34 dodaje się art. 34a w brzmieniu:

„Art. 34a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco współpracują z Prezesem Urzędu Komunikacji Elektronicznej podczas trwania incydentu telekomunikacyjnego i na żądanie Prezesa Urzędu Komunikacji Elektronicznej przekazują informacje o incydencie telekomunikacyjnym.

2. Informacje przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco raz na pół roku przygotowują sprawozdania dotyczące liczby i rodzajów incydentów telekomunikacyjnych.”;

19) w art. 36 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 jego posiedzenia. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej.”;

20) w art. 39:

a) użyte w ust. 1-3 i ust. 5-9, w różnej liczbie i różnym przypadku wyrazy „i sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy i CSIRT Telco”,

b) w ust. 3 pkt 2 otrzymuje brzmienie:

„2) dotyczące telekomunikacyjnych urządzeń końcowych;”,

c) w ust. 4 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) gromadzone przez przedsiębiorców komunikacji elektronicznej.”;

21) użyte w art. 40, w różnej liczbie i różnym przypadku wyrazy “sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami “CSIRT sektorowy i CSIRT Telco”;

22) w art. 41 pkt 4 otrzymuje brzmienie:

„4) dla sektora bankowego i infrastruktury rynków finansowych - Urząd Komisji Nadzoru Finansowego;”;

23) w art. 42 w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji” zastępuje się wyrazami „Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa”;

24) 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 zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo;
4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację 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 wymianę informacji o zagrożeniach.”,

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 zagrożeń cyberbezpieczeństwa;
2) koordynować w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które dotyczą różnych podmiotów w danym sektorze lub podsektorze.”,

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, a także mając na względzie;
2) konieczność współpracy tego podmiotu z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV;
3) poziom cyberbezpieczeństwa i liczbę podmiotów w danym sektorze oraz incydenty, które w nim wystąpiły.”;

25) po art. 44 dodaje się art. 44a w brzmieniu:

„Art. 44a. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie CSIRT Telco działającego analogicznie do CSIRT sektorowego.

2. Minister właściwy do spraw informatyzacji może powierzyć jednostce podległej lub nadzorowanej prowadzenie CSIRT Telco.

3. CSIRT Telco wspiera przedsiębiorców komunikacji elektronicznej w realizacji ich obowiązków określonych w rozdziale 4a.

4. Do zadań CSIRT Telco należy:

1) przyjmowanie zgłoszeń o incydentach telekomunikacyjnych;
2) reagowanie na incydenty telekomunikacyjne;
3) gromadzenie informacji o podatnościach i zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo;
4) współpraca z przedsiębiorcami komunikacji elektronicznej w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację 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 telekomunikacyjne i krytyczne oraz wymianę informacji o zagrożeniach.”.

5. CSIRT Telco może, w szczególności:

1) zapewniać dynamiczną analizę ryzyka i incydentów oraz wspomagać podnoszenie świadomości zagrożeń cyberbezpieczeństwa;
2) koordynować w uzgodnieniu z przedsiębiorcami komunikacji elektronicznej obsługę incydentów, które dotyczą różnych przedsiębiorców komunikacji elektronicznej.”;

26) w art. 46:

a) ust. 2 otrzymuje brzmienie:

„2. 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 oraz CSIRT Telco 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, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na

podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”;

27) w art. 62 w ust. 1 w pkt 6 kropkę zastępuje się przecinkiem i dodaje się pkt 7 w brzmieniu:
„7) wydawanie ostrzeżeń i poleceń zabezpieczających.”;

28) w art. 65 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7-8 w brzmieniu:
„7) oceny ryzyka dostawcy sprzętu i oprogramowania;
8) wydawania ostrzeżeń i poleceń zabezpieczających.”;

29) po art. 66 dodaje się art. 66a-66c w brzmieniu:

„Art. 66a. 1. Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.

2. Wniosek o sporządzenie oceny zawiera wskazanie:

1) danych identyfikujących dostawcę sprzętu lub oprogramowania;
2) możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego.

3. Wniosek o sporządzenie oceny może określać:

1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub,
2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa

- które uwzględnia się przy sporządzeniu oceny dostawcy sprzętu lub oprogramowania.

4. W sporządzania oceny przeprowadza się w szczególności:

1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;
2) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą:
   a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,
   b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka,

c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,

d) strukturę własnościową dostawcy sprzętu lub oprogramowania,

e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;

3) liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów;

4) stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

5) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.

5. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania określa:

a) wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe, albo

b) umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo

c) niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo

d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.

6. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania przekazywana jest Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

7. W przypadku określenia umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego dotyczy ta ocena dostawcy sprzętu lub oprogramowania, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium może zmienić ocenę.

8. Dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.

9. W przypadku wystąpienia nowych okoliczności, mogących mieć wpływ na ocenę ryzyka dostawcy sprzętu lub oprogramowania, członek Kolegium może złożyć wniosek o zmianę oceny przez Kolegium.

Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:

1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;
2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie.

2. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:

1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;
2) mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania.”;

Art. 66c 1. W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.

2. Plan i harmonogram podlega zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora, a w przypadku przedsiębiorcy komunikacji elektronicznej z Prezesem UKE.

30) po art. 67 dodaje się art. 67a-67c w brzmieniu:

„Art. 67a. 1. Pełnomocnik może wydać:

1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,
2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego

– po zatwierdzeniu przez Kolegium.

2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu.

3. Pełnomocnik, przed wydaniem ostrzeżenia lub polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, analizę uzasadniającą jego wydanie, obejmującą:

1) istotność zagrożenia cyberbezpieczeństwa;
2) prawdopodobieństwo wystąpienia incydentu krytycznego;
3) rodzaje ryzyk;
4) skutki finansowe, społeczne i prawne wydania ostrzeżenia lub polecenia zabezpieczającego;
5) skuteczność alternatywnych metod zapewnienia cyberbezpieczeństwa.

4. Ostrzeżenie i polecenie zabezpieczające może dotyczyć:

1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) 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;
3) 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;
4) 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);
5) kwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 20 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.).

5. Przed wydaniem ostrzeżenia lub polecenia zabezpieczającego Pełnomocnik może przeprowadzić konsultacje z podmiotami, o których mowa w ust. 4, lub podmiotami, na które ostrzeżenie lub polecenie zabezpieczające mogą mieć wpływ.

6. Pełnomocnik ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikaty o wydanych i odwołanych ostrzeżeniach i poleceniach zabezpieczających. W komunikacie uwzględnia się elementy wskazane w art. 67b ust. 1 oraz 67c ust 3.

7. Jeżeli przemawia za tym interes publiczny, informacja o zastosowanym ostrzeżeniu może być udostępniona za pomocą środków masowego przekazu.

8. W przypadku odmowy zatwierdzenia przez Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje inne ostrzeżenie lub polecenie zabezpieczające.

Art. 67b. 1. Ostrzeżenie, o którym mowa w art. 67a ust. 1 pkt 1 zawiera:

1) wskazanie rodzajów ryzyk;
2) wskazanie rodzajów podmiotów, których dotyczy;
3) wskazanie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu;
4) datę wejścia w życie i okres obowiązywania;
5) uzasadnienie zawierające wyniki analizy, o której mowa w art. 67a ust. 3.

2. Ostrzeżenie stosuje się na okres nie dłuższy niż dwa lata. Pełnomocnik może jednokrotnie przedłużyć okres obowiązywania ostrzeżenia nie dłużej niż o kolejne dwa lata, przy czym przedłużenie ostrzeżenia z jednoczesnym uzupełnieniem go w zakresie elementów, o których mowa w ust. 1 pkt 1-3, uznaje się za nowe ostrzeżenie.

3. Przez wskazanie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu, rozumie się:

1) 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.

Art. 67c. 1. Pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu.

2. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego, nie dłużej niż dwa lata.

3. Polecenie zabezpieczające zawiera:
1) wskazanie 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 art. 67a ust. 3.

4. Przez wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenieniu, rozumie się:
1) zachowania określone w art. 67b ust. 3;
2) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;
3) zabezpieczenie określonych informacji, w tym dzienników systemowych;
4) wytworzenie obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

5. Polecenie zabezpieczające jest niezwłocznie doręczane podmiotom, których dotyczy, oraz publikowane w sposób, o którym mowa w art. 67a ust. 6”.

31) w art. 73:
a) w ust. 1 w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 w brzmieniu:
„14) nie zastosował polecenia zabezpieczającego, o którym mowa w art. 67a ust. 1 pkt 2.”,
b) po ust. 2 dodaje się ust. 2a w brzmieniu:
„2a. Karze pieniężnej podlega podmiot krajowego systemu cyberbezpieczeństwa, który nie dostosował się do obowiązków określonych w art. 66b.”,
c) w ust. 3:
- w pkt 9 po wyrazie „wynosi” dodaje się wyraz „do”,

- dodaje się pkt 14 w brzmieniu:

„14) ust. 2a wynosi:

a) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 1 w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 2 w wysokości do 1% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,

c) w przypadku podmiotów publicznych do 100 000 zł”;

32) w art. 74 dodaje się ust. 1a w brzmieniu:

„1a. Karę pieniężną określoną w art. 73 ust. 2a nakłada w drodze decyzji:

1) w przypadku podmiotów określonych w art. 4 pkt 7-15 – organ nadzorujący;

2) w przypadku podmiotów określonych w art. 4 pkt 1 – 2 – organy właściwe do spraw cyberbezpieczeństwa;

3) w przypadku podmiotów określony w art. 4 pkt 2a – Prezes UKE;

4) w przypadku podmiotów wpisanych do wykazu SOC, wykonujących usługi na zlecenie operatora usług kluczowych – organy właściwe do spraw cyberbezpieczeństwa.”;

33) w art. 93 uchyla się ust. 8 i ust. 23.

Art. 2. W ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. poz. 2019) wprowadza się następujące zmiany:

1) w art. 96 w ust. 2 w pkt 2 w lit. f kropkę zastępuje się przecinkiem i dodaje się pkt 3 w brzmieniu:

„3) poziomu ryzyka, jaki stanowi dostawca sprzętu lub oprogramowania, stwierdzonego oceną, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369).”;

2) w art. 109 w ust. 1 w pkt 10 kropkę zastępuje się średnikiem i dodaje się pkt 11 w brzmieniu:

„11) który jest dostawcą sprzętu lub oprogramowania, wobec którego stwierdzono wysokie ryzyko, w ramach oceny, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”;

3) w art. 110 w ust. 2 wyrazy „pkt 2-10” zastępuje się wyrazami „pkt 2-11”.

Art. 3. 1. Organ właściwy ustanawia CSIRT sektorowy zgodnie z art. 44 ust. 5 w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Minister właściwy do spraw informatyzacji powołuje CSIRT Telco, o którym mowa w art. 44a, w terminie 18 miesięcy od dnia wejścia w życie ustawy.

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 2020 r. - 0 zł;
2) w 2021 r. - 0 zł;
3) w 2022 r. - 52,43 mln zł;
4) w 2023 r. - 43,31 mln zł;
5) w 2024 r. - 44,68 mln zł;
6) w 2025 r. - 46,11 mln zł;
7) w 2026 r. - 47,53 mln zł;
8) w 2027 r. - 49,01 mln zł;
9) w 2028 r. - 50,53 mln zł;
10) w 2029 r. – 52,09 mln zł.

2. 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 ograniczeniu finansowania działalności wyznaczonego CSIRT sektorowego wskazanego przez ministra właściwego do spraw informatyzacji.

3. 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. 2, dokonuje minister właściwy do spraw informatyzacji.

Art. 5. Ustawa wchodzi w życie z dniem 21 grudnia 2020 r., z wyjątkiem art. 1 pkt 24 lit. c w zakresie ust. 6 oraz art. 2, które wchodzą w życie z dniem 1 stycznia 2021 r.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
REDAKCYJNYM I LEGISLACYJNYM
Iwona Szulc
Zastępca Dyrektora Departamentu Prawnego
w Ministerstwie Cyfryzacji
/- podpisano elektronicznie/

UZASADNIENIE

Ustawa o krajowym systemie cyberbezpieczeństwa[1)] (zwana dalej „ustawą o KSC”), przyjęta w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. W tym zakresie jest to implementacja dyrektywy NIS[2)].

Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, operatorzy 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 do ustawy. 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.

[1)] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2248, z 2020 r. poz. 695 i 875.

[2)] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE.L 2016 Nr 194, str. 1.

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 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 budową krajowego systemu cyberbezpieczeństwa, a doświadczenia zebrane przez dwa lata jej obowiązywania wskazały potrzebę wprowadzenia zmian na poziomie ustawowym.

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Dla podniesienia skuteczności reagowania na incydenty zachodzi konieczność ustanowienia CSIRT sektorowych dla każdego z sektorów. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami.

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

Jednym z najczęściej występujących problemów jest brak właściwych struktur u operatorów usług kluczowych lub zakres posiadanych kwalifikacji oraz 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 o wynikach kontroli[3)] 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[4)]. 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 nie powstały w Polsce centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa (ang. Information Sharing and Analysis Center, dalej zwane: ISAC), gromadzące informacje o podatnościach i zagrożeniach bezpieczeństwa informacyjnego. Pierwsze ISAC powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku.

Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym. Centra ISAC stanowią platformę takiej

---

[3)] Najwyższa Izba Kontroli, *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego,* Warszawa 2019 https://www.nik.gov.pl/kontrole/P/18/006/ dostęp 10.07.2020

[4)] Ibidem Str. 11

współpracy poprzez wymianę informacji na temat przyczyn, incydentów, zagrożeń jak również dzielenie się doświadczeniem wiedzą i analizami.

Cybersecurity Act zachęca do tworzenia ISAC poprzez nałożenie na ENISA obowiązku 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 na całym świecie.

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). 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 stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa europejskich sieci 5G.

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

- zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych,
- oceniania profili ryzyka dostawców,
- stosowania odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe,
- wdrożenia strategii mających na celu zapewnienie dywersyfikacji dostawców, w celu unikania uzależnienia od dostawców stwarzających wysokie ryzyko.

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia postanowień tego dokumentu.

Zgodność projektu ustawy z celami strategicznymi Rady Ministrów

Projekt ustawy służy realizacji celu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej

na lata 2019-2024[5)] 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.

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 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 nie. Zakres obowiązków zostanie więc poszerzony - obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi cyfrowej w reagowaniu na incydenty. CSIRT sektorowy będzie również dokonywał dynamicznej analizy ryzyka i incydentów jak również gromadził informacje o zagrożeniach cyberbezpieczeństwa.

Nowe obowiązki przedsiębiorców komunikacji elektronicznej i CSIRT Telco

Ustawa wdraża postanowienia Europejskiego Kodeksu Łączności Elektronicznej[6)] (dalej „EKŁE"). Przedsiębiorcy komunikacji elektronicznej staną się częścią krajowego systemu cyberbezpieczeństwa. Zostanie im udzielone wsparcie w reagowaniu na incydenty.

Wprowadzona zostanie nowa kategoria incydentu – incydent telekomunikacyjny. Zgłoszenia o incydentach telekomunikacyjnych wzmocnią świadomość sytuacyjną zespołów CSIRT poziomu krajowego i usprawnią koordynację reagowania na incydenty.

Dla wsparcia przedsiębiorców komunikacji elektronicznej zostanie powołany odrębny CSIRT Telco, którego zadania będą analogiczne do zadań CSIRT sektorowych w innych sektorach. CSIRT Telco będzie prowadził minister właściwy do spraw informatyzacji.

ISAC

ISAC (centra wymiany i analiz informacji), tworzone jako inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o zagrożeniach i podatnościach

---

[5)] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, M. P. 2019 r. poz. 1037.

[6)] Dz. Urz. UE L 321 z 17.12.2018 r., str. 36.

oraz wymiana informacji o najlepszych praktykach.

Centra ISAC będą przekazywały wyniki analiz zespołom CSIRT poziomu krajowego.

SOC

Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: „SOC". Zastąpią one poprzednie struktury odpowiedzialne za cyberbezpieczeństwo operatora usług kluczowych. Centra 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 tworzyli struktury SOC wewnątrz organizacji lub zawierali umowę z zewnętrznym podmiotem świadczącym usługi SOC. SOC będzie dokonywał szacowanie ryzyka, wykrywał oraz reagował na incydenty. Minister właściwy do spraw informatyzacji będzie prowadził wykaz operacyjnych centrów bezpieczeństwa.

Koordynacja zadań na poziomie wojewódzkim

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 wymianie informacji pomiędzy zespołami CSIRT poziomu krajowego i Pełnomocnikiem a podmiotami publicznymi w województwie. Ułatwi to wymianę informacji o zagrożeniach cyberbezpieczeństwa incydentach. 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.

Wprowadzenie oceny ryzyka dostawców sprzętu lub oprogramowania

Odporność na cyberzagrożenia zależy w dużym stopniu od bezpieczeństwa sprzętu, oprogramowania i usług. Dotyczy to zarówno systemów teleinformatycznych, sieci telekomunikacyjnych oraz automatyki przemysłowej. Ocena profili ryzyka dostawców sprzętu lub oprogramowania prowadzona będzie przez Kolegium na wniosek jego członków. W ramach oceny będą brane pod uwagę zarówno aspekty techniczne jak i pozatechniczne, mające wpływ na bezpieczeństwo narodowe. Podkreślić należy, że ocena profili ryzyka dostawców jest jednym z narzędzi strategicznych uzgodnionych w 5G Toolbox przez państwa członkowskie Unii Europejskiej, Komisję Europejską i ENISA.

Efektem oceny prowadzonej przez Kolegium będzie określenie, w jakim stopniu sprzęt lub

oprogramowanie danego dostawcy stanowi ryzyko dla systemów, sieci i usług podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności usług kluczowych, cyfrowych i telekomunikacyjnych.

Podmioty krajowego systemu cyberbezpieczeństwa, zarządzając ryzykiem w swoich systemach informacyjnych, zobowiązane będą do uwzględnienia treści ocen poziomu ryzyka dostawców sprzętu i oprogramowania.

Szczególne działania muszą być podjęte wobec sprzętu i oprogramowania pochodzącego od dostawców wysokiego ryzyka. Podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły wprowadzać do użytkowania sprzętu, oprogramowania i usług stwarzających wysokie ryzyko oraz będą musiały wycofać z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie.

Dostawca sprzętu lub oprogramowaniu będzie mógł się odwołać do Przewodniczącego Kolegium w przedmiocie sporządzonej oceny. Ponadto, jeżeli wystąpią nowe okoliczności, które mogą mieć wpływ na ocenę, dostawca będzie mógł złożyć wniosek o zmianę oceny.

Zapobieganie i zwiększenie skuteczności reagowania na incydenty krytyczne

W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne Pełnomocnik będzie mógł wydawać:

1) ostrzeżenia - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,

2) polecenia zabezpieczające - w przypadku wystąpienia incydentu krytycznego.

Ostrzeżenia i polecenia zabezpieczające będą podlegały zatwierdzeniu przez Kolegium.

Przewidywane skutki społeczne, gospodarcze, prawne i finansowe wprowadzanych zmian

Skutki społeczne

Dodanie CSIRT sektorowych, CSIRT Telco, SOC i ISAC pozwoli na większą skuteczność działań krajowego systemu cyberbezpieczeństwa.

Powołanie CSIRT sektorowych pozwoli na stworzenie jednostki, która będzie lepiej orientowała się w zagrożeniach i podatnościach danego sektora. Dzięki temu incydenty w sektorze będą obsługiwane szybciej, z uwzględnieniem szczególnych uwarunkowań danego sektora. To samo będzie dotyczyć CSIRT Telco w odniesieniu do przedsiębiorców komunikacji elektronicznych. Centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa.

Skutki gospodarcze

Celem krajowego systemu cyberbezpieczeństwa jest zapewnienie bezpieczeństwa w cyberprzestrzeni. Poprzez nałożenie różnych 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 osób trzecich 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.

Skutki finansowe

Powołanie nowych podmiotów krajowego systemu cyberbezpieczeństwa będzie wymagało dodatkowych nakładów finansowych. Należy jednak podkreślić, że jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są bardzo częste. 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 charakter finansowy. Inwestycja w rozbudowę krajowego systemu cyberbezpieczeństwa pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a gdy już zaistniały – znacznie je zmniejszyć. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Skutki prawne

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

Wojewoda stanie się 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.

Kolegium będzie mogło dokonywać oceny ryzyka dostawców sprzętu i oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.

Pełnomocnik uzyska nowe narzędzia w celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne

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 przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosił MON, NASK 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.

Projekt zostanie wysłany do organizacji branżowych i partnerów społecznych. Ze względu na poruszaną kwestię współpracy z samorządami, zostanie skierowany do opiniowania przez stowarzyszenia zrzeszające jednostki samorządu terytorialnego.

Uzasadnienie poszczególnych przepisów materialnych

W związku z dodaniem przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa proponuje się uchylić art. 1 ust 1, który wyłączał stosowanie ustawy do przedsiębiorców telekomunikacyjnych. Również proponuje się uchylenie wyłączenia z art. 1 ust. 2 pkt 2 ponieważ wobec dostawcy usług zaufania będą korzystali z ocen ryzyka dostawców sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.

Artykuł 2 obecnie obowiązującej ustawy zawiera słowniczek pojęć używanych w ustawie, stąd niezbędne było dodanie do niego w projektowanych punktach 3a-3e definicji CSIRT sektorowych, CSIRT Telco, ISAC i SOC, a także dostawcy sprzętu lub oprogramowania. W związku ze zmianą nazwy proponuje się w nowelizacji zamianę frazy „sektorowy zespół cyberbezpieczeństwa” na CSIRT sektorowy.

Proponuje się wprowadzenie do ustawy nową definicję dostawcy sprzętu lub oprogramowania. Definicja obejmuje producenta, upoważnionego przedstawiciela, importera i dystrybutora produktów, usług i procesów technologii informacyjno-telekomunikacyjnych (ICT) a także produktów i usług dla infrastruktury telekomunikacyjnej. Definicja odnosi się do definicji zamieszczonych w prawie europejskim i w ustawie - Prawo komunikacji

elektronicznej[7)].

Zdefiniowano nowy rodzaj incydentu, czyli incydentu telekomunikacyjnego, który ma wpływ na usługę komunikacji elektronicznej. Dla spójności systemu prawa nowelizacja odwołuje się do definicji przedsiębiorcy komunikacji elektronicznej, dostarczania sieci telekomunikacyjnej, usług komunikacji elektronicznej, telekomunikacyjnych urządzeń końcowych i sytuacji szczególnego zagrożenia zawartych w ustawie - Prawie komunikacji elektronicznej. Nie ma potrzeby dublowania definicji.

Kluczowym terminem jest bezpieczeństwo sieci i usług. Rozumie się przez to zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania działań naruszających dostępność, autentyczność integralność lub poufność tych sieci, usług jak i przetwarzanych danych.

W nowelizacji artykułu 4, który wymienia podmioty krajowego systemu cyberbezpieczeństwa proponuje się dodać nowe podmioty: przedsiębiorców komunikacji elektronicznej**,** Urząd Komisji Nadzoru Finansowego (w związku ze zmianą ustawy o nadzorze nad rynkiem finansowym zmienił formę prawną działania[8)]; wyszczególniono uczelnie wyższe odwołując się do Prawa o szkolnictwie wyższym i nauce. Dodano także ISAC i CSIRT Telco. Zgodnie ze zmianą nazewnictwa dotychczasowe podmioty świadczące usługi cyberbezpieczeństwa zmieniono na SOC.

W projektowanym artykule 4a wskazano (w otwartym katalogu) zadania ISAC. Będą to: wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów. Dodano przepisy odnośnie prowadzenia wykazu ISAC, wpisu do niego oraz wykreślenia. Wpis do wykazu będzie odbywał się po uzyskaniu pozytywnej opinii jednego z trzech zespołów CSIRT poziomu krajowego. ISAC ma współpracować z zespołami CSIRT poziomu krajowego a także składają sprawozdanie ze swojej działalności ministrowi właściwemu ds. informatyzacji. Jeżeli ISAC prowadzi

---

[7)] W zakresie:

producenta, upoważnionego przedstawiciela, importera i dystrybutora odwołuje się do 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

produktów ICT, usług ICT, procesów ICT odwołuje się do 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 (akt o cyberbezpieczeństwie)

infrastruktury telekomunikacyjnej odwołuje się do Prawa komunikacji elektronicznej

[8)] 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).

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 propozycji nowelizacji artykułu 7 ust. 5 dodaje się możliwość podpisania wniosku o wpisanie operatora usługi kluczowej 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). 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 nowelizowanym art. 10 ust. 2 pkt 2 rozszerzono obowiązki nadzoru nad dokumentacją o ochronę dokumentów przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem.

Sugerowana zmiana art. 11 ust. 3 pkt 1-3 polega na dostosowaniu przepisu do nowych CSIRT sektorowych.

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 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 usługi.

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 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.

W celu umożliwienia wykonywania swoich zadań dane z wykazu SOC są udostępniane organom właściwym, 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.

Proponuje się dodanie rozdziału 4a „Obowiązki przedsiębiorców komunikacji elektronicznej", w którym będą uregulowane kwestie dotyczące obowiązku stosowania przez przedsiębiorców komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i usług.

W art. 20a nakładany jest na przedsiębiorcę komunikacji elektronicznej ogólny obowiązek brania pod uwagę w swojej działalności możliwości wystąpienia sytuacji szczególnego zagrożenia. Katalog tych zagrożeń jest katalogiem zamkniętym obejmującym stan nadzwyczajny, sytuację kryzysową oraz bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług. Ustawa odsyła tutaj do definicji z art. 2 pkt 65 ustawy – Prawo komunikacji elektronicznej.

Określone zostały obowiązki przedsiębiorców komunikacji elektronicznej dotyczące stosowania – po przeprowadzeniu oceny ryzyka - środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa proporcjonalny do stopnia ryzyka, co stanowi implementację art. 40 ust. 1 EKŁE. Wskazane zostały obligatoryjne obszary tych środków, wynikające z motywu 94 EKŁE. Podobnie jak w obecnie obowiązujących przepisach ustawy – Prawo telekomunikacyjne, minister właściwy do spraw informatyzacji będzie mógł określić minimalny zakres środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa sieci i usług.

Każdy przedsiębiorca będzie dokumentował prowadzenie analizy ryzyka oraz podejmowanie powyższych środków bezpieczeństwa. Przedsiębiorcy sporządzający plan działania w sytuacji szczególnego zagrożenia, dokumentują te czynności w tym planie.
W art. 20b uregulowano obowiązki informacyjne przedsiębiorcy komunikacji elektronicznej po wykryciu incydentu bezpieczeństwa. Obsługuje on incydent, klasyfikuje go, jako incydent telekomunikacyjny na podstawie progów uznania incydentu za telekomunikacyjny. Zgłasza incydent telekomunikacyjny do właściwego zespołu CSIRT poziomu krajowego i współdziała z nim. Stanowi to implementację art. 40 ust. 2 zdanie pierwsze EKŁE.
Dodatkowo zgłoszenie jest przekazywane do zespołu CSIRT Telco, z którym przedsiębiorca również współpracuje podczas obsługi incydentu telekomunikacyjnego, jak i krytycznego.
Przepis art. 20c reguluje zasady zgłaszania incydentów przez przedsiębiorców sporządzających plan działania w sytuacji szczególnego zagrożenia. Będą oni przekazywać informację o wystąpieniu incydentu bezpieczeństwa nie później niż w ciągu 24 godzin od chwili jego wystąpienia, według aktualnej wiedzy jaką dysponuje w tym czasie. Informację tę uzupełnia w trakcie obsługi incydentu bezpieczeństwa.
W rozporządzeniu ministra właściwego do spraw informatyzacji określone zostaną progi incydentu telekomunikacyjnego, których spełnienie spowoduje powstanie obowiązku informacyjnego.
Przepis art. 20d zawiera szczegóły dotyczące zawartości zgłoszenia incydentu telekomunikacyjnego.
Art. 20e reguluje obowiązki informacyjne przedsiębiorcy komunikacji elektronicznej wykonującego działalność na rynku detalicznym. W przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu bezpieczeństwa przedsiębiorca ten będzie miał obowiązek informować o nim użytkowników, na których takie zagrożenie może mieć wpływ, w tym o możliwych środkach, które użytkownicy ci mogą podjąć oraz związanych z tym kosztach, co stanowi implementację art. 40 ust. 3 zdanie pierwsze EKŁE.
Ponadto, przedsiębiorca ten będzie zobowiązany informować o incydencie bezpieczeństwa i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny, co stanowi implementację art. 40 ust. 3 zdanie drugie EKŁE.
W art. 20f uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej do blokowania komunikatu oraz ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu. Takie działanie możliwe jest w przypadku stwierdzenia zagrożenia dla bezpieczeństwa sieci i

usług oraz tylko w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny zagrożenia.
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.
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 podmiotów.
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 zagrożeń cyberbezpieczeństwa, 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 zagrożeniach cyberbezpieczeństwa.
Zmiana art. 32 polega na umożliwieniu zespołowi CSIRT Telco przekazania podmiotom krajowego systemu cyberbezpieczeństwa informacji o podatnościach i ich sposobach usunięcia, jeżeli informacje te zostały uzyskane o podmiotów systemu.
Nowe brzmienie art. 34 umożliwi współpracę CSIRT Telco oraz CSIRT sektorowego z organami ścigania, wymiarem sprawiedliwości, a także ze służbami specjalnymi przy wykonywaniu ustawowych zadań.
Nowy artykuł 34a umożliwia współpracę zespołów CSIRT poziomu krajowego z Prezesem UKE podczas trwania incydentu telekomunikacyjnego. Przepis ten jest implementacją art. 41 ust. 4 i 5 EKŁE.
Proponowane zmiany w art. 39 umożliwiają zespołowi CSIRT Telco przetwarzanie danych osobowych przy wykonywaniu zadań ustawowych. Zmiana w art. 39 ust. 3 pkt 2 jest techniczna, wynika z uchylenia dotychczasowego Prawa telekomunikacyjnego. Dzięki dodaniu art. 39 ust. 4 pkt 4 minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik oraz organy właściwe do spraw cyberbezpieczeństwa

będą mogli w celu realizacji zadań ustawowych przetwarzać dane osobowe pozyskanych w związku z incydentami i zagrożeniami cyberbezpieczeństwa od przedsiębiorców komunikacji elektronicznej.

Zmiana art. 40 umożliwi współpracę zespołu CSIRT Telco z organami ścigania i przetwarzanie danych stanowiących tajemnice prawnie chronione, przy zachowaniu tajemnicy informacji.

Proponowana w nowelizacji nowa treść art. 44 wprowadza obowiązek powołania przez organ właściwy CSIRT sektorowego dla sektora lub podsektora, który będzie obsługiwał operatorów usług kluczowych tego sektora. 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 zagrożeniach. Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze.

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.

W art. 44a uregulowano obowiązki zespołu CSIRT Telco. Będzie on prowadzony przez ministra właściwego do spraw informatyzacji. Minister będzie mógł powierzyć prowadzenie zespołu jednostce podległej lub nadzorowanej. Zadania CSIRT Telco są analogiczne do zadań CSIRT sektorowego, ale odnoszą się do działań w zakresie wsparcia przedsiębiorców komunikacji elektronicznej.

Proponowana w nowelizacji zmiana art. 46 określa dostęp podmiotów krajowego systemu cyberbezpieczeństwa do tworzonego na podstawie tego samego artykułu systemu teleinformatycznego. Zespoły CSIRT poziomu krajowego będą miały stały i nieograniczony dostęp do tego systemu. Zespoły CSIRT sektorowe i zespół CSIRT Telco 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.

Nowelizacja przyzna (w nowym art. 66a) Kolegium do spraw cyberbezpieczeństwa nową

kompetencję, jaką będzie możliwość oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Wniosek o sporządzenie oceny składa członek Kolegium. Należy w nim wskazać dane identyfikujące dostawcę sprzętu lub oprogramowania a także obszary, w których jego działalność może stwarzać zagrożenie dla bezpieczeństwa narodowego. Dodatkowo we wniosku będą mogły być wskazane rodzaje sieci telekomunikacyjnych, systemów teleinformatycznych, produktów, usług i procesów technologii informacyjno-komunikacyjnych a także kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, które uwzględnia się w postępowaniu i sporządzeniu oceny.
W ramach sporządzania oceny uwzględnia się analizę zagrożeń bezpieczeństwa narodowego, wpływ państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego na dostawcę, incydenty oraz ich czas likwidacji, nadzór dostawcy nad wytwarzaniem i dostarczania sprzętu oraz oprogramowania a także treść rekomendacji Pełnomocnika dotyczących stosowania sprzętu lub oprogramowania danego dostawcy sprzętu lub oprogramowania.
Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania określa:
a) wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe, albo
b) umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo
c) niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi umiarkowane lub niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo
d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.
Jeżeli ocena danego dostawcy sprzętu lub oprogramowania określi ryzyko jako umiarkowane lub niskie to dostawca może przedstawić środki zaradcze i plan naprawczy. Jeżeli Kolegium zaakceptuje tę propozycję, to ocena ryzyka tego dostawcy może być zmieniona.
Wprowadzono środek odwoławczy od oceny określającej wysokie ryzyko. Dostawca sprzętu lub oprogramowania będzie mógł odwołać się w ciągu 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium będzie miało 2 miesiące od otrzymania odwołania na jego rozpatrzenie.

Jeżeli pojawią się nowe okoliczności, które mogą mieć wpływ na ocenę ryzyka, członek Kolegium będzie mógł złożyć wniosek o zmianę oceny.
Obowiązkiem Pełnomocnika będzie ogłoszenie w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitorze Polskim" ocenie ryzyka w postaci komunikatu.
Artykuł 66b wprowadza skutki sporządzonej oceny ryzyka. W przypadku oceny ryzyka określającej wysokie ryzyko podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania. Z kolei dotychczas używany sprzęt, oprogramowanie i usługi określone w ocenie podmioty te będą musiały wycofać w ciągu 5 lat od ogłoszenia komunikatu o ocenie.
W przypadku określenia ryzyka jako umiarkowanego, to podmioty krajowego systemu cyberbezpieczeństwa nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; będą mogły jedynie kontynuować używanie dotychczas posiadanego sprzętu, usług lub oprogramowania wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania.
W szczególnych wypadkach (art. 66c) Pełnomocnik będzie mógł zobowiązać podmioty krajowego systemu cyberbezpieczeństwa, do których zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy planu z harmonogramem wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania. Plan będzie podlegał zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora a w przypadku przedsiębiorców komunikacji elektronicznej z Prezesem UKE.
W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne proponuje się dodanie nowych artykułów (art. 67a-67c) zawierających nowe kompetencje Pełnomocnika - możliwość wydawania ostrzeżeń i poleceń zabezpieczających. Stosuje się je po zatwierdzeniu przez Kolegium. W sytuacjach szczególnych Pełnomocnik może, na wniosek Zespołu Incydentów Krytycznych, wydać ostrzeżenie lub polecenie bez zatwierdzenia przez Kolegium. W takiej sytuacji ogłoszone ostrzeżenia lub polecenia wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu.
Pełnomocnik ma obowiązek przeprowadzić z Zespołem Incydentów Krytycznych analizę uzasadniającą wydanie ostrzeżenia lub polecenia zabezpieczającego. Obejmuje ona:

1. istotność zagrożenia cyberbezpieczeństwa;
2. prawdopodobieństwo wystąpienia incydentu krytycznego;

3. skutki finansowe, społeczne i prawne wydania ostrzeżenia lub polecenia zabezpieczającego;
4. skuteczność alternatywnych metod zapewnienia cyberbezpieczeństwa.

Ostrzeżenie stosuje się w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, które może skutkować wystąpieniem incydentu krytycznego. Nie jest decyzją administracyjną. W jego ramach wskazuje się rodzaje podmiotów, których dotyczy, określone zachowanie, które zmniejszy ryzyko, datę wejścia w życie i okres obowiązywania, a także uzasadnienie. Wydaje się je na okres nie dłuższy niż 2 lata, choć Pełnomocnik będzie mógł jednokrotnie przedłużyć jego okres obowiązywania nie dłużej niż o kolejne dwa lata.
Polecenie zabezpieczające jest decyzją administracyjną, która ma rygor natychmiastowej wykonalności. Stosuje je Pełnomocnik w razie wystąpienia incydentu krytycznego. Zawiera wskazanie podmiotów, których dotyczy, wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu, datę wejścia w życie i uzasadnienie. W razie nie zastosowania się do polecenia zabezpieczającego operator usługi kluczowej podlega administracyjnej karze pieniężnej.
Dodana zostanie administracyjna kara pieniężna nakładana na podmioty krajowego systemu cyberbezpieczeństwa za nie stosowanie się do obowiązków do obowiązków określonych w art. 66b. W przypadku operatorów usług kluczowych, dostawców usług kluczowych nie stosujących się do obowiązków z art. 66b ust. 1 kara wynosi do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego podczas gdy dla obowiązków z art. 66b ust. 2 kara wynosi do 1% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Ze względu na brak obrotu, podmioty publiczne nie stosujące się do art. 66b otrzymają określoną widełkami karę pieniężną w wysokości do 100 000 zł.
Karę nałoży:

- dla podmiotów publicznych – organ nadzorujący,
- dla operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa,
- dla przedsiębiorców komunikacji elektronicznej – Prezes UKE.

Zmiany w obowiązujących przepisach

Niniejszy projekt wprowadza zmiany w przepisach tzw. nowego Prawa Zamówień

Publicznych[9]. Wynikają one z wprowadzenia oceny ryzyka dostawców sprzętu i oprogramowania.

Przepisy przejściowe i przepis końcowy

W art. 3 ustawy nowelizującej przewidziano termin 18 miesięcy od dnia wejścia w życie ustawy na powołanie przez organy właściwe CSIRT sektorowych. Taki sam termin otrzyma minister właściwy do spraw informatyzacji na powołanie CSIRT Telco.

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 sprowadzenie wysoko kwalifikowanej kadry zespołów.

Zgodnie z przepisem końcowym ustawa weszłaby w życie 21 grudnia 2020 r. to jest wraz z ustawą - Prawo komunikacji elektronicznej. Niniejsza ustawa wielokrotnie odwołuje się do Prawa komunikacji elektronicznej, wobec tego zasadne jest, aby weszła w życie w tym samym dniu, aby uniknąć luki prawnej.

Natomiast art. 1 pkt 24 lit. c w zakresie art. 44 ust. 6 ustawy o Krajowym systemie cyberbezpieczęństwa dotyczącego możliwości powierzenia realizacji zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych oraz art. 2 zmieniający ustawę - Prawo zamówień publicznych wszedłby w życie 1 stycznia 2021 r., wraz z wejściem w życie nowej regulacji dotyczącej zamówień publicznych.

Pozostałe informacje

Wpływ projektu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców

Zawarte w projekcie regulacje nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2019 r. poz. 1292, z późn. zm.).

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

---

[9] Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. poz. 2019), które wejdzie w życie z dniem 1 stycznia 2021 r.

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 nie zawiera przepisów technicznych w rozumieniu 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.) i nie podlega notyfikacji Komisji Europejskiej.

Nazwa projektu Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Marek Zagórski, Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Jakub Dysarz, naczelnik wydziału, e-mail: jakub.dysarz@mc.gov.pl; tel. 22 245 58 38	**Data sporządzenia** 7 września 2020 r. **Źródło:** Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 **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., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. W tym zakresie jest to implementacja dyrektywy NIS.
Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, operatorzy 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 do ustawy. 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 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 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.

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

Przebudowany zostanie model współpracy w ramach krajowego systemu cyberbezpieczeństwa. CSIRT sektorowe i SOC (operacyjne centra bezpieczeństwa) zastąpią dotychczasowe sektorowe zespoły cyberbezpieczeństwa i podmioty świadczące usługi z zakresu cyberbezpieczeństwa.
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 nadanie konkretnych uprawnień do wydawania ostrzeżeń i poleceń zabezpieczających.
Dostawcy sprzętu lub oprogramowania będą mogli zostać poddani procedurze sprawdzającej pod kątem zagrożeń dla społeczno-ekonomicznego bezpieczeństwa państwa. W przypadku, w którym zostaną zidentyfikowani jako źródło zagrożenia, zostaną wyłączeni z systemu zamówień publicznych w Polsce. Skutkiem sporządzonej oceny będzie mogło być zobowiązanie podmiotów krajowego systemy cyberbezpieczeństwa do ograniczenia z korzystania produktów, oprogramowania i usług danego dostawcy sprzętu lub oprogramowania.

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

Ze względu na charakter wprowadzanych zmian, nie dokonano analizy prawno-porównawczej w obrębie krajów OECD/EU.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	163	Rejestr OUK	Zmiana regulacji

			dotyczących realizacji zadań ustawowych
Dostawcy usług cyfrowych	50	Dane własne MC	Zmiana regulacji dotyczących realizacji zadań ustawowych
Podmioty publiczne	Ok. 4000	Szacunki własne	Konieczność współpracy z wojewodą.
Przedsiębiorcy telekomunikacyjni	4177	Rejestr przedsiębiorców telekomunikacyjnych	Zgłaszanie incydentów do zespołów CSIRT, zamiast do UKE
Potencjalne ISAC	Kilkadziesiąt podmiotów	Szacunki MC (obecnie w ramach Partnerstwa dla Cyberbezpieczeństwa funkcjonuje 11 podmiotów, a z kolejnymi 18 trwają ustalenia warunków współpracy)	Możliwość wpisu do rejestru ISAC i korzystania z systemu S46
Organy właściwe	7	-	Konieczność powołania CISRT sektorowych
Wojewodowie	16	-	Konieczność zapewnienia współpracy z jednostkami samorządu terytorialnego w zakresie cyberbezpieczeństwa.
Kolegium ds. Cyberbezpieczeństwa	1	-	Realizacja nowego zadania – oceny ryzyka dostawców sprzętu lub oprogramowania
Pełnomocnik Rządu ds. Cyberbezpieczeństwa	1	-	Realizacja nowych zadań
Minister właściwy do spraw informatyzacji	1	-	Powołanie CSIRT Telco
Zespoły CSIRT	3	-	Opiniowanie wniosków ISAC do wpisu do wykazu ISAC prowadzonego przez ministra właściwego ds.
5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji			
W dniach 30.06-8.07 przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds.			

Cyberbezpieczeństwa. Swoje uwagi zgłosił MON, NASK 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 zostanie wysłany do organizacji branżowych i partnerów społecznych. Ze względu na poruszaną kwestię współpracy z samorządami, zostanie skierowany do opiniowania przez stowarzyszenia zrzeszające jednostki samorządu terytorialnego.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2020 r.)		Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]										
	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
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	0	0	52,43	43,31	44,68	46,11	47,53	49,01	50,53	52,09	53,66	439,35
budżet państwa	0	0	52,43	43,31	44,68	46,11	47,53	49,01	50,53	52,09	53,66	439,35
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	0	0	-52,43	-43,31	-44,68	-46,11	-47,53	-49,01	-50,53	-52,09	-53,66	-439,35
budżet państwa	0	0	-52,43	-43,31	-44,68	-46,11	-47,53	-49,01	-50,53	-52,09	-53,66	-439,35
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.											

<table>
<tr>
<td>Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń</td>
<td>
Konieczne będzie sfinansowanie zadań ustawowych, przygotowania Autonomicznego Pomieszczenia Konferencyjnego (do posiedzeń niejawnych, budowę CSIRT sektorowych Ministerstwo Cyfryzacji nie posiada możliwości prowadzenie spotkań o klauzuli „tajne”. Przystosowanie sali oraz zakup sprzętu na potrzeby posiedzeń Kolegium to koszt 350 000 zł (2022 – 175 tys. i 2023 – 175 tys.).
Budowa CSIRT sektorowych i CSIRT Telco będzie kosztownym przedsięwzięciem, które pozwoli zapełnić lukę w reagowaniu na incydenty w najbardziej narażonych sektorach gospodarki, gdzie 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:
- mały CSIRT – dla sektorów infrastruktura cyfrowa i zaopatrzenie w wodę i jej dystrybucja – wymagający ok. 50 roboczodni na m/c; co daje koszt roczny 594 000 zł;
- średni CSIRT– dla sektorów związanych z transportem (wodny oraz lądowy i powietrzny) – wymagający ok. 81 roboczodni na m/c; co daje koszt roczny 962 280 zł;
- duży CSIRT– dla przedsiębiorców telekomunikacyjnych, sektora energii, bankowości i ochrony zdrowia – wymagający ok. 111 roboczodni na m/c, co daje koszt roczny 1 318 680 zł.
Na potrzeby obliczeń założono wynagrodzenie rynkowe specjalistów w CSIRT 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):

<table>
<tr><th colspan="2">1. USŁUGA – ANALIZA ARTEFAKTÓW.</th></tr>
<tr><th>OPIS USŁUGI</th><th>Roboczodni</th></tr>
<tr><td>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.</td><td>3-7 roboczodni</td></tr>
<tr><th colspan="2">2. USŁUGA – ANALIZA POWŁAMANIOWA (INFORMATYKA ŚLEDCZA)</th></tr>
<tr><th>OPIS USŁUGI</th><th>Roboczodni</th></tr>
<tr><td>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.</td><td>2-6 roboczodni</td></tr>
<tr><th colspan="2">3. USŁUGA – ANALIZA PODATNOŚCI</th></tr>
<tr><th>OPIS USŁUGI</th><th>Roboczodni</th></tr>
<tr><td>Usługi świadczone w celu lepszego zrozumienia luk w zabezpieczeniach, które były przyczyną incydentów</td><td>4-8 roboczodni</td></tr>
<tr><th colspan="2">4. USŁUGA – ROZWÓJ ORAZ ZARZĄDZANIE ŹRÓDŁAMI I DANYMI THREAT INTELLIGENCE</th></tr>
<tr><th>OPIS USŁUGI</th><th>Roboczodni</th></tr>
<tr><td>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</td><td>15-20 roboczodni</td></tr>
</table>
</td>
</tr>
</table>

	procedury przeciwników. Usługi te zależą od działań związanych z wymianą informacji, które są zdefiniowane w obszarze usługowym numer 5 "Komunikacja".	
	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	1-5 roboczodni

na późniejszym etapie. Usługa ta ma na celu zapobieganie podobnym incydentom i poprawie reakcji na podobną lub ogólniejszą sytuację.	
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 zakładają stopniowe budowanie trzech linii wsparcia (od 14 pracowników w pierwszym roku działania do 20 pracowników w trzecim):

SOC - etaty			2021		2022		2023	
Typ stanowiska	Koszt miesięczny		FTE	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 lini	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	..	180 000,00		180 000,00
SUMA			14	2 484 000,00	19	3 444 000,00	20	3 636 000,00

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

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	*Łącznie (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	-						
		sektor mikro-, małych i średnich przedsiębiorstw	Przedsiębiorcy telekomunikacyjni będą zgłaszali incydenty do zespołów CSIRT poziomu krajowego oraz do CSIRT Telco, zamiast do regulatora, co zapewni im wsparcie zespołów reagowania na incydenty poziomu krajowego.						
		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.						
		Jednostki samorządu terytorialnego	Każdy wojewoda zapewni współpracę na linii administracja rządowa – administracja samorządowa, w tym usprawnienie wymiany informacji o incydentach, zagrożeniach cyberbezpieczeństwa i podatnościach.						
Niemierzalne		(dodaj/usuń)	-						
		(dodaj/usuń)	-						
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 komunikacji elektronicznej) 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 i dla przedsiębiorców komunikacji

elektronicznych.

9. Wpływ na rynek pracy

Projekt wygeneruje konieczność zatrudnienia wysoko wykwalifikowanych specjalistów zajmujących się cyberbezpieczeństwem a także przekwalifikowania dotychczas posiadanej kadry.

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 21 grudnia 2020 r. to jest wraz z ustawą - Prawo komunikacji elektronicznej. Niniejsza ustawa wielokrotnie odwołuje się do Prawa komunikacji elektronicznej, wobec tego zasadne jest, aby weszła w życie w tym samym dniu, aby uniknąć luki prawnej.
Natomiast art. 1 pkt 24 lit. c w zakresie art. 44 ust. 6 ustawy o Krajowym systemie cyberbezpieczęństwa dotyczącego możliwości powierzenia realizacji zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych oraz art. 2 zmieniający ustawę - Prawo zamówień publicznych wszedłby w życie 1 stycznia 2021 r., wraz z wejściem w życie nowej regulacji dotyczącej zamówień publicznych.

12. 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.

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

Nie dotyczy.