projekt z dnia 28 czerwca 2016 r.

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia lipca 2016 r.

w sprawie trybu i warunków przeprowadzania oceny bezpieczeństwa w celu realizacji zadań związanych z zapobieganiem zdarzeniom o charakterze terrorystycznym

Na podstawie art. 32a ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r. poz. 1929, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) warunki przeprowadzania oceny bezpieczeństwa, o której mowa w art. 32a ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej „ustawą";
2) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w pkt 1;
3) czynności niezbędne do przeprowadzania oceny bezpieczeństwa, o której mowa w pkt 1;
4) tryb dokonywania uzgodnień ramowych warunków przeprowadzania oceny bezpieczeństwa, o której mowa w pkt 1, z organami administracji publicznej, właścicielami, posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r. poz. 1166, z 2015 r. poz. 1485 oraz z 2016 r. poz. 266).

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) ocena bezpieczeństwa - ocenę, o której mowa w art. 32a ust. 1 ustawy;
2) system - systemy teleinformatyczne, sieci teleinformatyczne i dane, o których mowa w art. 32a ust. 1 ustawy, podlegające ocenie bezpieczeństwa;
3) architektura systemu - opis składników systemu teleinformatycznego lub sieci teleinformatycznej oraz powiązań i relacji pomiędzy tymi składnikami;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 2023 oraz z 2016 r. poz. 147, 437 i 904.

4) usługa sieciowa - właściwość systemu teleinformatycznego polegającą na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze;
5) podmiot zarządzający systemem - podmiot, o którym mowa w art. 32a ust. 3 ustawy;
6) roczny plan – roczny plan przeprowadzania oceny bezpieczeństwa, o którym mowa w art. 32a ust. 2 ustawy.

§ 3. 1. W ramach oceny bezpieczeństwa przeprowadza się następujące czynności:
1) pasywne zbieranie informacji - zbieranie w sieci Internet informacji związanych z funkcjonowaniem systemu, wpływających na jego bezpieczeństwo;
2) półpasywne zbieranie informacji - zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, na zasadach właściwych dla użytkownika tego systemu, z wyłączeniem uprawnień wymagających uwierzytelnienia w tym systemie; czynności te mogą być uzupełnione zbieraniem informacji wynikających z analizy architektury systemu;
3) aktywne zbieranie informacji - zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, w sposób przekraczający uprawnienia użytkownika systemu, w tym wymagających uwierzytelnienia w systemie, w szczególności polegających na enumeracji usług, portów, wykrywaniu urządzeń pośredniczących, wykrywaniu systemów IDS/IPS oraz zapór ogniowych;
4) identyfikacja podatności architektury systemu i usług sieciowych – podejmowanie czynności mających na celu identyfikację podatności, o której mowa w art. 32a ust. 4 ustawy, dokonywanych na podstawie informacji uzyskanych w ramach czynności, o których mowa w pkt 1-3, oraz informacji na temat architektury systemu udostępnionych przez podmiot zarządzający systemem.

2. W ramach oceny bezpieczeństwa, poza czynnościami, o których mowa w ust. 1, mogą być również przeprowadzane, za zgodą podmiotu zarządzającego systemem, następujące czynności:
1) wykorzystanie podatności - podejmowanie w systemie czynności nakierowanych na użycie podatności zidentyfikowanych w ramach czynności, o której mowa w ust. 1 pkt 4, celem ominięcia zabezpieczeń systemu oraz identyfikacji podatności, których identyfikacja jest niemożliwa w ramach czynności, o której mowa w ust. 1 pkt 4;

2) analiza wpływu wykorzystania czynników inżynierii społecznej - wykorzystanie ogólnych metod inżynierii społecznej mających na celu uzyskanie informacji na temat zachowania użytkowników systemu, celem weryfikacji procedur bezpieczeństwa badanego systemu realizowanych przez tych użytkowników; czynności mogą być wykonywane z zastosowaniem narzędzi, o których mowa w art. 32a ust. 7 ustawy;
3) analiza odporności systemu na działania narzędzi, o których mowa w art. 32a ust. 7 ustawy - zaplanowane wykorzystanie narzędzi, o których mowa w art. 32a ust. 7 ustawy, w celu zbadania możliwości wykorzystania luk w zabezpieczeniach systemu, poprzez badanie odporności systemu na możliwość wykorzystania go do popełniania przestępstw, o których mowa w art. 32a ust. 7 ustawy.

§ 4. 1. Przed przeprowadzeniem oceny bezpieczeństwa Agencja Bezpieczeństwa Wewnętrznego, zwana dalej „ABW", zwraca się do podmiotu zarządzającego systemem o przekazanie informacji dotyczących systemu, które mogą obejmować:
1) architekturę systemu, w tym informacje o urządzeniach wchodzących w skład infrastruktury systemu;
2) adresację sieciowej infrastruktury systemu;
3) informację o posiadaniu aktualnej kopii bezpieczeństwa systemu i zasad jej aktualizacji;
4) określenie wymaganego czasu przywrócenia systemu z kopii bezpieczeństwa systemu;
5) informację o posiadaniu środowiska testowego i jego zakresu;
6) zabezpieczenia teleinformatyczne systemu;
7) procedury bezpieczeństwa systemu;
8) dane osoby wyznaczonej przez podmiot zarządzający systemem do bieżącego kontaktu z ABW w czasie przeprowadzania oceny bezpieczeństwa;
9) dane osoby upoważnionej do reprezentacji podmiotu zarządzającego systemem.

2. Podmiot zarządzający systemem przekazuje informacje, o których mowa w ust. 1, w terminie:
1) 14 dni od dnia otrzymania wystąpienia ABW - w przypadku systemu ujętego w rocznym planie;
2) 7 dni od dnia otrzymania wystąpienia ABW - w przypadku systemu nieujętego w rocznym planie.

§ 5. 1. ABW dokonuje analizy informacji, o których mowa w § 4, w celu przygotowania propozycji oceny bezpieczeństwa.

2. ABW, w terminie 30 dni od dnia otrzymania informacji, o których mowa w § 4, przekazuje podmiotowi zarządzającemu systemem projekt porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa obejmujące, w szczególności:

1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;

2) zakres przeprowadzanych testów, w tym czynności, o których mowa w § 3;

3) rodzaj przeprowadzanych testów, o których mowa w zarządzeniu Szefa ABW wydanym na podstawie art. 32a ust. 12 ustawy.

§ 6. 1. Podmiot zarządzający systemem, w terminie 14 dni od dnia otrzymania projektu porozumienia, o którym mowa w § 5, może wnieść zastrzeżenia do jego treści, wraz z uzasadnieniem tych zastrzeżeń.

2. Zastrzeżenia, o których mowa w ust. 1, mogą obejmować w szczególności rodzaj i zakres przeprowadzanych testów z uwzględnieniem konieczności minimalizacji zakłócenia pracy systemu lub ograniczenia jego dostępności bądź nieodwracalnego zniszczenia danych przetwarzanych w systemie.

§ 7. 1. ABW odnosi się do zastrzeżeń, o których mowa w § 6, w terminie 14 dni od dnia ich otrzymania.

2. W przypadku, gdy uwzględnienie zastrzeżeń, o których mowa w § 6, może spowodować, iż ocena bezpieczeństwa stanie się niekompletna lub zwiększy możliwość wystąpienia zakłócenia pracy systemu lub ograniczenia jego dostępności, bądź nieodwracalnego zniszczenia danych przetwarzanych w systemie, ABW odstępuje od jej przeprowadzenia.

3. Podmiot zarządzający systemem, w terminie 7 dni od dnia otrzymania informacji o odstąpieniu od przeprowadzenia oceny bezpieczeństwa, może zwrócić się z pisemnym wnioskiem do ABW, , o przeprowadzenie tej oceny w przypadkach, o których mowa w ust. 2, akceptując niekompletność oceny bezpieczeństwa lub możliwość wystąpienia negatywnych następstw oceny bezpieczeństwa związanych z zakłóceniem pracy systemu lub ograniczenia jego dostępności.

§ 8. 1. ABW odstępuje od przeprowadzenia oceny bezpieczeństwa, w sytuacji gdy:

1) podmiot zarządzający systemem przekaże informację o braku posiadania aktualnej kopii bezpieczeństwa systemu;

2) z analizy, o której mowa w § 5, wynika, że:

a) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie, który będzie podlegał ocenie bezpieczeństwa,

b) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność,

c) podczas przeprowadzania oceny bezpieczeństwa może dojść do uszkodzenia urządzeń wchodzących w skład infrastruktury tego systemu oraz innych systemów teleinformatycznych podmiotu zarządzającego systemem,

d) istnieje zagrożenie ograniczenia dostępności usług świadczonych drogą elektroniczną przez podmiot zarządzający systemem.

2. ABW informuje podmiot zarządzający systemem o odstąpieniu, o którym mowa w ust. 1, oraz okolicznościach i przyczynach tego odstąpienia.

3. Podmiot zarządzający systemem, w terminie 7 dni od dnia otrzymania informacji o odstąpieniu od przeprowadzenia oceny bezpieczeństwa, może zwrócić się z pisemnym wnioskiem do ABW, , o przeprowadzenie tej oceny, pomimo zaistnienia zagrożeń, o których mowa w ust. 1 pkt 2 lit. b-d, akceptując możliwość wystąpienia tych zagrożeń i ich negatywnych następstw.

§ 9. W sytuacji, gdy z analizy, o której mowa w § 5, wynika konieczność dostępu do pomieszczeń lub urządzeń wchodzących w skład infrastruktury systemu przez funkcjonariusza lub pracownika ABW przeprowadzającego tą ocenę, ABW uzgadnia z podmiotem zarządzającym systemem sposób ich udostępniania.

§ 10. 1. Po przeprowadzeniu uzgodnień, o których mowa w § 4-9, Szef ABW i podmiot zarządzający systemem zawierają porozumienie o przeprowadzeniu oceny bezpieczeństwa.

2. Porozumienie, o którym mowa w ust. 1, zawiera w szczególności:

1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;

2) zakres przeprowadzanych testów, w tym czynności, o których mowa w § 3;

3) rodzaj przeprowadzanych testów, o których mowa w zarządzeniu Szefa ABW wydanym na podstawie art. 32a ust. 12 ustawy;

4) zgodę podmiotu zarządzającego systemem na przeprowadzenie oceny bezpieczeństwa w sytuacji, o której mowa w § 7 ust. 3 lub § 8 ust. 3;

5) sposób udostępniania pomieszczeń lub urządzeń wchodzących w skład infrastruktury tego systemu;

6) dane osoby wyznaczonej, o której mowa w § 4 ust. 1 pkt 8;

7) dane osoby upoważnionej, o której mowa w § 4 ust. 1 pkt 9.

3. Wzór porozumienia, o którym mowa w ust. 1, stanowi załącznik do rozporządzenia.

§ 11. Podmiot zarządzający systemem jest obowiązany do utrzymywania, za pośrednictwem osoby wyznaczonej, o której mowa w § 4 ust. 1 pkt 8, stałego kontaktu z funkcjonariuszem lub pracownikiem ABW przeprowadzającym ocenę bezpieczeństwa, w celu bieżącej konsultacji związanej z przebiegiem przeprowadzanej oceny bezpieczeństwa, w tym przekazywania informacji o zidentyfikowanych w systemie zakłóceniach wywołanych przeprowadzaną oceną bezpieczeństwa.

§ 12. 1. Funkcjonariusz lub pracownik ABW przeprowadzający ocenę bezpieczeństwa wstrzymuje prowadzenie czynności w sytuacji:

1) otrzymania od osoby wyznaczonej, o której mowa w § 4 ust. 1 pkt 8, informacji o zakłóceniach w prawidłowym funkcjonowaniu systemu, które mogą skutkować zagrożeniami, o których mowa w § 8 ust. 1 pkt 1 i 2 lit. a, c i d;
2) pojawienia się jednego z zagrożeń, o których mowa w § 8 ust. 1 pkt 1 lub pkt 2 lit. a, c lub d, albo uzasadnionego podejrzenia ich wystąpienia.

2. ABW informuje podmiot zarządzający o wstrzymaniu prowadzenia czynności, o którym mowa w ust. 1, oraz okolicznościach i przyczynach tego wstrzymania.

3. Podmiot zarządzający systemem może zwrócić się z pisemnym wnioskiem do ABW w terminie 2 dni roboczych od daty poinformowania, o którym mowa w ust. 2, o dalsze prowadzenie czynności w ramach oceny bezpieczeństwa, pomimo zaistnienia zagrożeń, o których mowa w § 8 ust. 1 pkt 2 lit. c lub d, akceptując możliwość wystąpienia tych zagrożeń lub ich negatywnych następstw.

4. W przypadku nieotrzymania wniosku, o którym mowa w ust. 3, ABW odstępuje od dalszego przeprowadzania oceny bezpieczeństwa.

§ 13. 1. Po przeprowadzeniu oceny bezpieczeństwa, ABW opracowuje w terminie 60 dni od dnia zakończenia oceny bezpieczeństwa, raport z przeprowadzonej oceny bezpieczeństwa.

2. Raport, o którym mowa w ust. 1, zawiera w szczególności:

1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;
2) zakres przeprowadzonych testów, w tym czynności, o których mowa w § 3;
3) rodzaj przeprowadzonych testów, o których mowa w zarządzeniu Szefa ABW wydanym na podstawie art. 32a ust. 12 ustawy;

4) informację o zgodzie podmiotu zarządzającego systemem na przeprowadzenie oceny bezpieczeństwa w sytuacji, o której mowa w § 7 ust. 3, § 8 ust. 3 lub o braku tej zgody;
5) informację o zaistnieniu okoliczności, o których mowa w § 12 ust. 1, oraz informację o otrzymaniu wniosku, o którym mowa w § 12 ust. 3, lub informację o odstąpieniu od przeprowadzania oceny bezpieczeństwa, o której mowa w § 12 ust. 4;
6) informację o aktualności wyników przeprowadzonej oceny bezpieczeństwa w odniesieniu do czasu jej przeprowadzenia i zakończenia;
7) wyniki przeprowadzonej oceny bezpieczeństwa zawierające wykaz zidentyfikowanych podatności oraz poziom ich zagrożenia dla ocenianego systemu;
8) zalecenia i rekomendacje.

§ 14. Rozporządzenie wchodzi w życie w dniu następującym po dniu ogłoszenia.

PREZES RADY MINISTRÓW

za zgodność
pod względem prawnym,
legislacyjnym i redakcyjnym

Jarosława Maćkowiak
p.o. Dyrektora
Departament Bezpieczeństwa Narodowego
Kancelaria Prezesa Rady Ministrów
20. 06. 2016

Wydział Obsługi Legislacyjnej i Prawnej I
Naczelnik
Michał Frączkiewicz
30. 06. 2016

Kancelaria Prezesa Rady Ministrów
Departament Prawny
zastępca dyrektora
Przemysław Myszakowski
radca prawny
30.06.2016

Załącznik do rozporządzenia
Rady Ministrów
z dnia lipca 2016 r. (poz.)

.....
(klauzula tajności po wypełnieniu)

Porozumienie
o przeprowadzeniu oceny bezpieczeństwa

§ 1.

1. Przedmiotem porozumienia jest przeprowadzenie przez ABW oceny bezpieczeństwa, w rozumieniu art. 32a ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r. poz. 1926, z późn. zm.), zwanej dalej „ustawą", następujących systemów teleinformatycznych lub danych przetwarzanych w tych systemach lub sieci teleinformatycznych Podmiotu Zarządzającego Systemem:
   .....
   .....
   .....
   .....,
   zwanych dalej „systemem".
2. Ocena bezpieczeństwa rozpocznie się z dniem ..... r.

§ 2.

1. Celem realizacji przedmiotu porozumienia ABW wykona czynności określone w § 3 ust. 1 rozporządzenia Rady Ministrów wydanego na podstawie delegacji ustawowej, o której mowa w art. 32a ust. 14 ustawy, zwanego dalej „rozporządzeniem".
2.* Podmiot Zarządzający Systemem działając w trybie przepisu § 3 ust. 2 rozporządzenia, wyraża zgodę na dokonanie przez ABW, w ramach oceny bezpieczeństwa, następujących czynności:
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....

.....
(klauzula tajności po wypełnieniu)

.....
(klauzula tajności po wypełnieniu)

2.* Podmiot Zarządzający Systemem, wyraża zgodę na dokonanie przez ABW, w ramach oceny bezpieczeństwa, następujących testów bezpieczeństwa[1)]:

.....

.....

.....

.....

3. ABW po wykonaniu oceny bezpieczeństwa sporządza i przekazuje Podmiotowi Zarządzającego Systemem, w terminie o którym mowa w § 13 ust. 1 rozporządzenia, raport, o którym mowa w art. 32a ust. 10 ustawy, spełniający wymagania określone w § 13 ust. 2 rozporządzenia.

§ 3.

Podmiot zarządzający systemem oświadcza, że systemy teleinformatyczne wskazane do przeprowadzenia oceny bezpieczeństwa, pozostają w jego faktycznej oraz prawnej dyspozycji oraz, że posiada on wszelkie prawa do wdrożenia we wskazanych systemach takich testów w zakresie i na zasadach określonych w niniejszym porozumieniu.

§ 4.

1. Podmiot Zarządzający Systemem w terminie, o którym mowa w § 4 ust. 2 pkt 1/§ 4 ust. 2 pkt 2* rozporządzenia, przekazuje ABW informacje, o których mowa w § 4 ust. 1 rozporządzenia.
2. Podmiot Zarządzający Systemem może zwrócić się do ABW, w trybie § 7 ust. 3 lub § 8 ust. 3 rozporządzenia, z pisemnym wnioskiem o przeprowadzenie oceny bezpieczeństwa, pomimo wystąpienia jednej z przesłanek, o których mowa w § 7 ust. 2 lub § 8 ust. 1 pkt 2 lit. b-d rozporządzenia.

§ 5.

W przypadku wyrażenia zgody na przeprowadzenie przez ABW czynności i testów, o których mowa odpowiednio w § 2 ust. 2 i § 2 ust. 3 porozumienia, lub dokonania przez ABW oceny bezpieczeństwa, o której mowa w § 3 ust. 2 porozumienia, odpowiedzialność za negatywne skutki ich przeprowadzenia przez ABW ponosi Podmiot Zarządzający Systemem.

.....
(klauzula tajności po wypełnieniu)

[1)] Rodzaje testów bezpieczeństwa dokonywanych przez ABW są określone w zarządzeniu Szefa ABW wydanym na podstawie delegacji ustawowej, o której mowa w art. 32a ust. 12 ustawy, i opublikowanym przez Szefa ABW w Dzienniku Urzędowym Agencji Bezpieczeństwa Wewnętrznego.

.....
(klauzula tajności po wypełnieniu)

§ 6.

Ustanawia się następujący harmonogram oceny bezpieczeństwa:

.....

.....

.....

.....

§ 7.

* Ustanawia się sposób udostępniania do pomieszczeń lub urządzeń wchodzących w skład systemu Podmiotu Zarządzającego Systemem:

.....

.....

§ 8.

W ramach realizacji porozumienia Podmiot Zarządzający Systemem:

1) upoważnia Pana/Panią*.....,
   dane kontaktowe: .....,
   do jego reprezentowania przed ABW w ramach oceny bezpieczeństwa;
2) wyznacza Pana/Panią*.....,
   dane kontaktowe: .....,
   do bieżącego kontaktu oraz udzielania wyjaśnień i przekazywania ABW informacji dotyczących funkcjonowania systemu.

§ 9.

Podmiot Zarządzający Systemem oświadcza, że o ile przeprowadzenie oceny bezpieczeństwa systemów teleinformatycznych przez ABW wymaga podjęcia jakichkolwiek dodatkowych czynności formalno-prawnych lub organizacyjnych, w szczególności uzyskania stosownych zgód właściwych podmiotów, czy też ich poinformowania o prowadzonych działaniach, podmiot zarządzający systemem ponosi odpowiedzialność za właściwą realizację takich czynności.

§ 10.

1. Porozumienie zawiera się na czas przeprowadzenia oceny bezpieczeństwa.
2. Wszelkie zmiany niniejszego porozumienia mogą być dokonywane wyłącznie za zgodną wolą stron, z zachowaniem formy pisemnej pod rygorem nieważności.

.....
(klauzula tajności po wypełnieniu)

.....
(klauzula tajności po wypełnieniu)

§ 11.

Porozumienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla ABW i Podmiotu Zarządzającego Systemem.

§ 12.

Porozumienie wchodzi w życie z dniem podpisania.

*niepotrzebne skreślić

.....
(klauzula tajności po wypełnieniu)

UZASADNIENIE

Projekt rozporządzenia Rady Ministrów w sprawie warunków i trybu przeprowadzania oceny bezpieczeństwa w celu realizacji zadań związanych z zapobieganiem zdarzeniom o charakterze terrorystycznym, zwany dalej „projektem", został opracowany na podstawie upoważnienia ustawowego z art. 32a ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r. poz. 1929, z późn. zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw (Dz. U. poz. 904) przewiduje powierzenie Agencji Bezpieczeństwa Wewnętrznego zadań w zakresie rozpoznawania, zapobiegania i wykrywania zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. Ocena bezpieczeństwa będzie polegać na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji podatności, przez które rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływających na integralność, poufność, rozliczalność i dostępność tego systemu. W celu przeprowadzenia oceny Bezpieczeństwa Agencja Bezpieczeństwa Wewnętrznego będzie mogła m.in. wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 1997 r. poz. 553, z późn. zm.).

Projekt określa tryb i warunki przeprowadzenia przez Agencję Bezpieczeństwa Wewnętrznego oceny bezpieczeństwa, zakres czynności niezbędnych do przeprowadzenia oceny bezpieczeństwa, a także zakres sposób uzgadniania z organami administracji publicznej, właścicielami, posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r. poz. 1166, z 2015 r. poz. 1485 oraz z 2016 r. poz. 266), ramowych warunków przeprowadzenia oceny bezpieczeństwa. Projektowany akt wykonawczy w § 2 definiuje użyte w projekcie pojęcia tj. architektura systemu, usługa sieciowa oraz podmiot zarządzający systemem.

Projekt określa w § 3 zakres czynności wykonywanych w ramach oceny bezpieczeństwa wskazując jednocześnie, te czynności, które wymagają zgody podmiotu zarządzającego systemem, na ich przeprowadzenie.

Ponadto, w § 4 projekt określa przykładowy zakres informacji dotyczących ocenianego systemu jakie podmiot zarządzający tym systemem ma obowiązek przedstawienia Agencji Bezpieczeństwa Wewnętrznego przed przystąpieniem ABW do przeprowadzenia oceny bezpieczeństwa oraz terminy przekazania przedmiotowych informacji. Na podstawie informacji przekazanych przez podmiot zarządzający systemem, Agencja Bezpieczeństwa Wewnętrznego przedstawi podmiotowi zarządzającemu systemem projekt porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa, które zostały określone w § 5 projektu. W projektowanym § 6, przewidziano również uprawnienie dla podmiotu zarządzającego systemem do wniesienia zastrzeżeń do przedstawionego przez ABW projektu porozumienia, a także tryb w jakim ABW odnosi się do wniesionych zastrzeżeń, który został uregulowany w § 7 projektu.

Projekt określa w § 8 okoliczności, w których ABW odstępuje od przeprowadzenia oceny bezpieczeństwa, wskazując w szczególności sytuacje, gdy podmiot zarządzający systemem przekaże informację o braku posiadania aktualnej kopii bezpieczeństwa systemu, a także sytuacje gdy z analizy informacji przekazanych przez podmiot zarządzający wynika, iż istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie mającym podlegać ocenie bezpieczeństwa, czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność, jak również istnieją inne zagrożenie dla działania tego systemu. W § 9 projektu określono sposób uzgadniania z podmiotem zarządzającym systemem warunki dostępu do pomieszczeń lub urządzeń wchodzących w skład infrastruktury systemu przez funkcjonariusza ABW lub pracownika ABW przeprowadzającego ocenę bezpieczeństwa tego systemu.

W § 10 projektu wskazano jako sposób uregulowania wszelkich kwestii dotyczących przeprowadzeni oceny bezpieczeństwa systemu, obowiązek zawarcia pomiędzy Szefem ABW a podmiotem zarządzającym systemem porozumienia w którym mają zostać w szczególności uregulowane kwestie dotyczące dat rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogramu, zakresu i rodzajów przeprowadzanych testów oraz zasady dostępu do pomieszczeń lub urządzeń wchodzących w skład infrastruktury tego systemu. Wzór porozumienia stanowi załącznik do rozporządzenia.

Projektodawca w § 11 projekt nałożono na podmiot zarządzający systemem obowiązek utrzymywania, za pośrednictwem osoby wyznaczonej, stałego kontaktu z funkcjonariuszem ABW lub pracownikiem ABW przeprowadzającymi ocenę bezpieczeństwa, w celu bieżącej konsultacji związanej z przebiegiem przeprowadzanej oceny bezpieczeństwa, w tym przekazywania informacji o zidentyfikowanych w systemie zakłóceniach wywołanych przeprowadzaną oceną bezpieczeństwa.

Projektowany § 12 określa przesłanki wstrzymania prowadzenia czynności w ramach prowadzonej oceny bezpieczeństwa, w przypadku otrzymania informacji o zakłóceniach w prawidłowym funkcjonowaniu systemu lub pojawienia się innego zagrożenia dla właściwego funkcjonowania systemu albo uzasadnionego podejrzenia jego wystąpienia, a także tryb postępowania w przypadku wystąpienia takiej sytuacji.

Wynikiem przeprowadzonej oceny bezpieczeństwa będzie sporządzony przez Agencję Bezpieczeństwa Wewnętrznego raport, którego termin sporządzenia oraz zakres został uregulowany w projektowanym § 13.

Rozporządzenie wejdzie w życie w dniu następującym po dniu ogłoszenia. Zgodnie z art. 4 ust. 2 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów prawnych i niektórych innych aktów prawnych (Dz. U. z 2011 r. poz. 1172, z późn. zm.), w uzasadnionych przypadkach akty normatywne mogą wejść w życie w terminie krótszym niż czternaście dni.

Projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego sytemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Projekt nie był przedstawiany instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu, celem uzyskania opinii, dokonania konsultacji albo uzgodnienia, ponieważ przepisy przedmiotowego projektu rozporządzenia pozostają poza zakresem prawa Unii Europejskiej.

Projekt będzie podlegał udostępnieniu na stronie podmiotowej Kancelarii Prezesa Rady Ministrów w Biuletynie Informacji Publicznej, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.).

Zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. poz. 979 oraz z 2015 r. poz. 1063) projekt będzie podlegał udostępnieniu w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Przedmiot projektowanej regulacji pozostaje poza zakresem prawa Unii Europejskiej.

Nazwa projektu Projekt rozporządzenia Rady Ministrów w sprawie warunków i trybu przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych w celu realizacji zadań związanych z zapobieganiem zdarzeniom o charakterze terrorystycznym **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Minister – Członek Rady Ministrów Mariusz Kamiński - Koordynator Służb Specjalnych **Kontakt do opiekuna merytorycznego projektu** Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów, Sekretarz Kolegium do Spraw Służb Specjalnych – Maciej Wąsik tel. 22 621 55 64, e-mail:bkss@kprm.gov.pl	**Data sporządzenia** 28 czerwca 2016 r. **Źródło:** upoważnienie ustawowe art. 32a ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r. poz. 1929 i 2023 oraz z 2016 r. poz. 147, 437 i 904) **Nr w wykazie prac:**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projekt rozporządzenia Rady Ministrów w sprawie warunków i trybu przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych w celu realizacji zadań związanych z zapobieganiem zdarzeniom o charakterze terrorystycznym stanowi wykonanie delegacji ustawowej określonej w art. 32a ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.), nowelizowanej w ramach ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Zgodnie z art. 32a. ust. 1 ww. ustawy, w celu zapobiegania, przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym występujących w cyberprzestrzeni RP w rozumieniu art. 2 pkt 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, Agencja Bezpieczeństwa Wewnętrznego przeprowadza ocenę bezpieczeństwa systemów teleinformatycznych, o których mowa w art. 5 ust. 1 pkt 2a, zwaną dalej „oceną bezpieczeństwa".

Ze względu na wrażliwy charakter systemów teleinformatycznych wskazanych w art. 5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.), obejmujących katalog:

- systemów istotnych z punktu widzenia ciągłości funkcjonowania państwa;
- systemów albo sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej;
- systemów teleinformatycznych posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 i 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r., poz. 1166, z późn. zm .)"

konieczne jest doprecyzowanie zasad współpracy Agencji Bezpieczeństwa Wewnętrznego z podmiotami odpowiedzialnymi za zarządzanie nimi.

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

Przedmiotowy projekt rozporządzenia określa procedurę współpracy Agencji Bezpieczeństwa Wewnętrznego z podmiotami odpowiedzialnymi za zarządzanie systemami poddawanymi „ocenie bezpieczeństwa", określonymi w art. 5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.). Proponowana w przedmiotowym zakresie procedura, obok zapobiegania, przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym występujących w cyberprzestrzeni RP, jest zorientowana na minimalizację ryzyka wystąpienia zakłócenia pracy systemu lub ograniczenia jego dostępności, bądź

nieodwracalnego zniszczenia danych przetwarzanych w systemie. Mając na względzie przywołane powyżej wymagania, proponowana procedura „oceny bezpieczeństwa" obejmuje następujące kroki:

- wniosek Szefa ABW do zarządzającego systemem o udostępnienie informacji istotnych z punktu widzenia jego bezpieczeństwa;
- uzgodnienie zakresu „oceny bezpieczeństwa" w drodze dedykowanego porozumienia (z opcją odstąpienia od przeprowadzenia testów w przypadku wystąpienia uwarunkowań określonych w § 8 projektu niniejszego rozporządzenia);
- przeprowadzenie „oceny bezpieczeństwa" zgodnie z podejściem etapowym opisanym w § 3 projektu niniejszego rozporządzenia, z uwzględnieniem dostępu do obiektów i infrastruktury na zasadach określonych w rozdziale 5 projektu niniejszego rozporządzenia;
- sporządzenie raportu z „oceny bezpieczeństwa" na zasadach określonych w rozdziale 4 projektu niniejszego rozporządzenia.

W zakresie planowanych narzędzi interwencji zakłada się wykorzystanie środków obejmujących:

- pozyskanie informacji nt. systemu, ze szczególnym uwzględnieniem elementów mających istotny wpływ na jego bezpieczeństwo;
- identyfikację podatności systemu;
- opcjonalną analizę możliwości wykorzystania zidentyfikowanych podatności systemu, w tym obejmującą weryfikację odporności systemu na działania narzędzi, o których mowa w art. 32a ust. 7 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.);
- opracowanie zaleceń i rekomendacji proponowanych do wdrożenia przez zarządzającego systemem.

Oczekiwanym efektem opisanych powyżej działań będzie podniesienie poziomu bezpieczeństwa systemów poddanych „ocenie bezpieczeństwa", które zostanie osiągnięte poprzez:

- pozyskanie przez zarządzających systemem wiedzy nt. zidentyfikowanych przez ABW podatności opisanych w raporcie z przeprowadzonej oceny bezpieczeństwa zgodnie z §11 ust. 2 pkt 7;
- wdrożenie przez zarządzającego systemem zaleceń i rekomendacji wydanych przez ABW i opisanych w raporcie z przeprowadzonej oceny bezpieczeństwa zgodnie z §11 ust. 2 pkt 8.

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

Brak jest informacji jak kwestie prowadzenia oceny bezpieczeństwa systemów teleinformatycznych zostały uregulowane w innych krajach.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty sektora publicznego i prywatnego odpowiedzialne za zarządzanie: ▪ systemami istotnymi z punktu widzenia ciągłości funkcjonowania państwa; ▪ systemami albo sieciami teleinformatycznymi objętymi jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej; ▪ systemami teleinformatycznymi posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 i 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu	Brak danych	Brak źródła	Realizacja zadań z obszarów: ▪ analiza stanu bezpieczeństwa systemów teleinformatycznych; ▪ identyfikacja podatności systemów teleinformatycznych; ▪ analiza odporności systemów teleinformatycznych; ▪ podnoszenie poziomu bezpieczeństwa systemów teleinformatycznych w drodze wdrażania wydanych zaleceń i rekomendacji.

kryzysowym (Dz. U. z 2013 r., poz. 1166, z późn. zm.)"			

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

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2015 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Wydatki ogółem	-	3,5	5,5	5,5	6,5	7,5	8	9	9	9,5	9,5	73,5
budżet państwa	-	3,5	5,5	5,5	6,5	7,5	8	9	9	9,5	9,5	73,5
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Saldo ogółem	-	3,5	5,5	5,5	6,5	7,5	8	9	9	9,5	9,5	73,5
budżet państwa	-	3,5	5,5	5,5	6,5	7,5	8	9	9	9,5	9,5	73,5
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-

Źródła finansowania	Budżet państwa
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	W zakresie szacowania kosztów wykonania przepisów procedowanego rozporządzenia bazowano na wiedzy eksperckiej funkcjonariuszy Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL. Składowymi pozycji kosztowych w tym zakresie są przede wszystkim zakupy sprzętu i specjalistycznego oprogramowania wspomagającego funkcjonariuszy ABW w zakresie: ▪ automatyzacji procesów pozyskiwania informacji nt. systemów teleinformatycznych poddawanych „ocenie bezpieczeństwa"; ▪ automatyzacji procesów pozyskiwania informacji nt. podatności systemów teleinformatycznych poddawanych „ocenie bezpieczeństwa"; ▪ automatyzacji procesów badania odporności systemów teleinformatycznych poddawanych „ocenie bezpieczeństwa"; ▪ kompleksowego zarządzania procesami „oceny bezpieczeństwa" w odniesieniu do wszystkich systemów wskazanych w art. 5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.). Dodatkowo celem realizacji zadania Szef ABW zapewni obsługę etatową i wyszkoli docelowo 40 funkcjonariuszy ABW. Łączny koszt wzrostu uposażeń wyniesie wraz z kosztami wyszkolenia w ciągu 10 lat ok. **40 mln PLN**. Sumaryczny koszt pozyskania ww. rozwiązań w okresie 10 lat wyniesie **73,5 mln PLN**.

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	-						
	rodzina, obywatele oraz gospodarstwa domowe	-						
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)	Podniesienie poziomu bezpieczeństwa: ▪ systemów istotnych z punktu widzenia ciągłości funkcjonowania państwa; ▪ systemów albo sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej; ▪ systemów teleinformatycznych posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 i 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r., poz. 1166, z późn. zm.)"						
	(dodaj/usuń)							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

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

X 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:

9. Wpływ na rynek pracy

Brak wpływu

10. Wpływ na pozostałe obszary

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

Omówienie wpływu	Wejście w życie rozporządzenia doprecyzuje obszar współpracy ABW z podmiotami zarządzającymi systemami określonymi w art. 5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.). Efektywne i skuteczne współdziałanie w przedmiotowym zakresie w zamierzeniu będzie skutkować istotnym podniesieniem poziomu bezpieczeństwa wybranych zasobów teleinformatycznych, kluczowych dla Rzeczypospolitej Polskiej.

11. Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów rozporządzenia nastąpi w dniu jego wejścia w życie.

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

Oszacowanie efektów projektu rozporządzenia Rady Ministrów będzie następować sukcesywnie, wraz z postępującym zakresem przeprowadzanych przez ABW „ocen bezpieczeństwa".

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

Brak załączników