Warszawa, dnia 14 stycznia 2020 r.

Poz. 54

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 2 stycznia 2020 r.

w sprawie warunków i trybu prowadzenia, koordynacji i wdrażania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet

Na podstawie art. 32aa ust. 9 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) warunki i tryb:

   a) wdrażania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwanego dalej „systemem ostrzegania", w tym czynności niezbędne do uruchomienia systemu ostrzegania w infrastrukturze podmiotu, o którym mowa w art. 32aa ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanego dalej „Uczestnikiem",

   b) prowadzenia, w tym utrzymania, systemu ostrzegania,

   c) koordynacji systemu ostrzegania;

2) wzór porozumienia w sprawie technicznych aspektów uczestnictwa w systemie ostrzegania oraz modelu konfiguracji systemu, zwanego dalej „porozumieniem".

§ 2. 1. Agencja Bezpieczeństwa Wewnętrznego, zwana dalej „ABW", przekazuje Uczestnikowi, u którego wdrożenie systemu ostrzegania następuje zgodnie z rocznym planem wdrożenia, informacje o:

1) technicznych aspektach uczestnictwa w systemie ostrzegania niezbędnych do wdrożenia systemu ostrzegania, w szczególności jego uruchomienia, zwanych dalej „technicznymi aspektami uczestnictwa";

2) proponowanym terminie wdrożenia systemu ostrzegania.

2. ABW przekazuje informacje Uczestnikowi w terminie do dnia 1 grudnia roku poprzedzającego rok, na który został opracowany roczny plan wdrożenia systemu ostrzegania, o którym mowa w art. 32aa ust. 2 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej „ustawą".

3. ABW przekazuje podmiotowi, o którym mowa w art. 32aa ust. 2 zdanie drugie ustawy, który złożył wniosek o wdrożenie systemu ostrzegania z pominięciem rocznego planu wdrożenia systemu ostrzegania wraz z uzasadnieniem, informację o sposobie jego rozpatrzenia w terminie 3 miesięcy od dnia złożenia tego wniosku.

4. W przypadku pozytywnego rozpatrzenia wniosku ABW przekazuje Uczestnikowi, w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, informacje o technicznych aspektach uczestnictwa.

§ 3. Uczestnik, w terminie 14 dni od dnia otrzymania informacji o technicznych aspektach uczestnictwa, przekazuje do ABW, w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, informację o:

1) spełnieniu technicznych aspektów uczestnictwa albo

2) niespełnianiu technicznych aspektów uczestnictwa na dzień przekazania informacji oraz o terminie, do którego dostosuje użytkowaną infrastrukturę do technicznych aspektów uczestnictwa.

§ 4. W przypadku przekazania informacji, o której mowa w § 3 pkt 2, gdy termin, w którym Uczestnik przekazujący informację dostosuje posiadaną infrastrukturę do technicznych aspektów uczestnictwa, zostanie określony w sposób:

1) umożliwiający wdrożenie systemu ostrzegania, w szczególności jego uruchomienie, zgodnie z planem, o którym mowa w art. 32aa ust. 2 ustawy, Uczestnik niezwłocznie po dostosowaniu posiadanej infrastruktury informuje ABW w postaci elektronicznej, a w przypadku braku możliwości przekazania informacji w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, o spełnieniu technicznych aspektów uczestnictwa;

2) uniemożliwiający wdrożenie systemu ostrzegania, w szczególności jego uruchomienie, zgodnie z planem, o którym mowa w art. 32aa ust. 2 ustawy, ABW informuje o tym fakcie podmiot go nadzorujący, o którym mowa w art. 32aa ust. 8 ustawy, oraz uwzględnia tego Uczestnika w planie wdrożenia na rok następny.

§ 5. 1. Uczestnictwo w systemie ostrzegania wymaga:

1) niezwłocznego usuwania awarii infrastruktury sieciowej i zasilającej system ostrzegania w celu zachowania pełnej sprawności systemu ostrzegania;

2) monitorowania i analizy we własnym zakresie informacji generowanych przez system ostrzegania w celu podjęcia działań naprawczych i zabezpieczających będących w jego zakresie;

3) nieprzekazywania innym podmiotom:

   a) informacji dotyczących systemu ostrzegania,

   b) całości ani części udostępnionego przez ABW oprogramowania ani platformy sprzętowej,

   c) informacji o platformie sprzętowej wchodzącej w skład systemu ostrzegania oraz aspektach technicznych związanych z budową i funkcjonowaniem systemu ostrzegania.

2. W uzasadnionych przypadkach ABW może wyrazić zgodę na przekazanie przez Uczestnika innemu podmiotowi informacji dotyczących systemu ostrzegania lub udostępnienie całości lub części oprogramowania albo platformy sprzętowej wchodzącej w skład tego systemu.

3. Zgoda może zostać wydana przez ABW na uzasadniony wniosek Uczestnika, przekazany w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, zawierający:

1) pełne dane podmiotu, który miałby otrzymać informacje, oprogramowanie albo platformę sprzętową;

2) szczegółowy zakres przekazywanych informacji lub oprogramowania.

4. ABW, z uwagi na bezpieczeństwo narodowe, może odmówić, bez podania przyczyny, udzielenia zgody na przekazanie przez Uczestnika innemu podmiotowi informacji lub udostępnienie oprogramowania.

§ 6. 1. W przypadku przekazania informacji, o której mowa w § 3 pkt 1 albo § 4 pkt 1, ABW uzgadnia z Uczestnikiem sposób i termin zawarcia porozumienia.

2. Wzór porozumienia jest określony w załączniku do rozporządzenia.

§ 7. 1. Przed rozpoczęciem wdrożenia systemu ostrzegania Uczestnik przekazuje ABW, w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, wypełniony wniosek o nadanie uprawnień do systemu ostrzegania.

2. Wniosek zawiera:

1) nazwę Uczestnika;

2) adres korespondencyjny Uczestnika;

3) publiczne adresy IP, z których będzie realizowany dostęp do graficznego interfejsu użytkownika (GUI) systemu ostrzegania;

4) imiona i nazwiska co najmniej dwóch osób wyznaczonych przez Uczestnika, dla których będą utworzone konta dostępowe w systemie ostrzegania, zwanych dalej „osobami wyznaczonymi”;

5) dane kontaktowe osób wyznaczonych, zawierające adresy poczty elektronicznej i numery telefonów.

3. ABW tworzy konta dostępowe w systemie ostrzegania na podstawie danych przekazanych we wniosku o nadanie uprawnień do systemu ostrzegania.

4. Informacja o utworzeniu konta dostępowego w systemie ostrzegania oraz dane niezbędne do logowania do tego systemu są przekazywane osobom wyznaczonym przy wykorzystaniu poczty elektronicznej.

§ 8. 1. W ramach wdrożenia systemu ostrzegania ABW:

1) użycza Uczestnikowi platformę sprzętową albo instaluje elementy systemu ostrzegania na platformie sprzętowej użytkowanej przez Uczestnika;

2) konfiguruje system ostrzegania;

3) sprawdza poprawność funkcjonowania systemu ostrzegania.

2. ABW niezwłocznie usuwa awarie programowe i sprzętowe platformy sprzętowej użyczonej Uczestnikowi przez ABW.

§ 9. 1. ABW przeprowadza serwisowanie platformy sprzętowej użyczonej Uczestnikowi, w tym wymianę na nową platformę sprzętową w przypadku jej trwałego uszkodzenia.

2. Uczestnik zwraca użyczoną platformę sprzętową na żądanie ABW.

3. Użyczenia albo zwrotu użyczonej Uczestnikowi platformy sprzętowej dokonuje się na podstawie protokołów użyczenia albo zwrotu platformy sprzętowej określających nazwę, liczbę, numer fabryczny i lokalizację użyczonych składników majątku.

§ 10. ABW w ramach wdrożenia systemu ostrzegania określa, w uzgodnieniu z Uczestnikiem, zakres:

1) czynności niezbędnych do przeprowadzenia wdrożenia, w szczególności instalacji platformy sprzętowej w użytkowanej przez Uczestnika infrastrukturze, albo

2) instalacji elementów systemu ostrzegania na platformie sprzętowej użytkowanej przez tego Uczestnika

– które zostaną zrealizowane przez tego Uczestnika.

§ 11. 1. W ramach prowadzenia systemu ostrzegania, w szczególności w zakresie utrzymania tego systemu, ABW:

1) wykonuje czynności administrowania systemem ostrzegania i koordynuje jego działanie;

2) monitoruje poprawność funkcjonowania systemu ostrzegania oraz poszczególnych elementów systemu ostrzegania zainstalowanych w infrastrukturze Uczestnika, w szczególności łączności z siecią Internet;

3) monitoruje alarmy przekazywane przez elementy systemu ostrzegania zainstalowane w infrastrukturze Uczestnika;

4) dokonuje aktualizacji systemu ostrzegania oraz mechanizmów alarmowych;

5) dokonuje analizy wydajności platformy sprzętowej i informuje Uczestnika o potrzebie modernizacji platformy sprzętowej użytkowanej przez tego Uczestnika;

6) uzgadnia z Uczestnikiem kwestie związane z modernizacją platformy sprzętowej użytkowanej przez tego Uczestnika.

2. W przypadku stwierdzenia w ramach czynności, o których mowa w ust. 1 pkt 2, nieprawidłowości w funkcjonowaniu systemu ostrzegania ABW:

1) informuje Uczestnika o rodzaju stwierdzonej nieprawidłowości;

2) przekazuje Uczestnikowi instrukcje dotyczące postępowania mającego na celu przywrócenie prawidłowego funkcjonowania systemu ostrzegania.

§ 12. Uczestnik w ramach systemu ostrzegania:

1) dokonuje analizy alarmów przekazywanych przez elementy systemu ostrzegania zainstalowane w infrastrukturze tego Uczestnika w celu podjęcia działań naprawczych i zabezpieczających będących w jego zakresie;

2) czuwa nad prawidłowym funkcjonowaniem elementów systemu ostrzegania zainstalowanych w infrastrukturze tego Uczestnika, w szczególności użyczonej platformy sprzętowej;

3) zapewnia łączność elementów systemu ostrzegania zainstalowanych w infrastrukturze tego Uczestnika z siecią Internet zgodnie z technicznymi aspektami uczestnictwa;

4) informuje ABW o:

   a) zamiarze podjęcia działań mogących wpłynąć na prawidłowe funkcjonowanie systemu ostrzegania, w szczególności o zamiarze odłączenia od infrastruktury Uczestnika jakiegokolwiek elementu systemu ostrzegania,

   b) wykrytej lub planowanej przerwie w dostępności łączności elementów systemu ostrzegania zainstalowanych w infrastrukturze tego Uczestnika z siecią Internet,

   c) wykrytych nieprawidłowościach w działaniu systemu ostrzegania;

5) wykonuje działania zgodnie z instrukcjami, o których mowa w § 11 ust. 2 pkt 2, oraz informuje ABW o efektach ich wykonania;

6) nie wykonuje samodzielnie czynności dotyczących elementów systemu ostrzegania zainstalowanych w infrastrukturze tego Uczestnika, w szczególności użyczonej platformy sprzętowej, z wyłączeniem instrukcji, o których mowa w § 11 ust. 2 pkt 2;

7) współpracuje z ABW w zakresie modernizacji oraz bieżących prac związanych z utrzymaniem poprawności funkcjonowania platformy sprzętowej użytkowanej przez tego Uczestnika.

§ 13. 1. W ramach koordynacji systemu ostrzegania, w związku z wykonywaniem czynności, o których mowa w § 11 ust. 1 pkt 3, w przypadku powzięcia przez ABW informacji o wystąpieniu alarmu klasyfikowanego jako pilny, ABW informuje o tym osoby wyznaczone.

2. ABW klasyfikuje alarm jako pilny na podstawie analizy przeprowadzonej przez system ostrzegania.

3. Uczestnik, w przypadku otrzymania informacji, o której mowa w ust. 1, niezwłocznie podejmuje niezbędne działania mające na celu przeciwdziałanie zagrożeniu i informuje ABW o podjętych działaniach oraz o ich wynikach.

§ 14. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów: *M. Morawiecki*

Załącznik do rozporządzenia Prezesa Rady Ministrów
z dnia 2 stycznia 2020 r. (poz. 54)

WZÓR

…….
(klauzula tajności – po wypełnieniu)

…….
(sygnatura literowo-cyfrowa)

Egz. nr …….

POROZUMIENIE

zawarte w dniu _____ w Warszawie

w sprawie technicznych aspektów uczestnictwa w systemie ostrzegania oraz modelu konfiguracji systemu

między:

Szefem Agencji Bezpieczeństwa Wewnętrznego z siedzibą w Warszawie (adres siedziby: ul. Rakowiecka 2A, 00-993 Warszawa), NIP: 5213199092, REGON: 015179728, reprezentowanym przez: …….....
…….,

a

……..
……,
zwanym/-ną dalej „Uczestnikiem”, reprezentowanym/-ną przez: ……...
……..
……..
– zwanych dalej łącznie „Stronami” lub każdy z osobna „Stroną”.

§ 1. Celem porozumienia jest uzgodnienie między Agencją Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW”, a Uczestnikiem kwestii związanych z technicznymi aspektami uczestnictwa Uczestnika w systemie wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, o którym mowa w art. 32aa ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27), zwanym dalej „systemem ostrzegania”.

§ 2. Uczestnik zostaje włączony do systemu ostrzegania na podstawie:
1) planu, o którym mowa w art. 32aa ust. 2 zdanie pierwsze ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*;
2) wniosku, o którym mowa w art. 32aa ust. 2 zdanie drugie ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

* Niepotrzebne skreślić.

…….
(klauzula tajności – po wypełnieniu)

…….
(klauzula tajności – po wypełnieniu)

……. Egz. nr …….
(sygnatura literowo-cyfrowa)

§ 3. Uczestnik oświadcza, iż na dzień podpisania porozumienia spełnia wszystkie aspekty techniczne niezbędne do wdrożenia systemu ostrzegania, w szczególności jego uruchomienia, o których mowa w § 2 ust. 1 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 2 stycznia 2020 r. w sprawie warunków i trybu prowadzenia, koordynacji i wdrażania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet (Dz. U. poz. 54), zwanego dalej „rozporządzeniem”, o których poinformował ABW w formie
…….
……..
w dniu ……...

§ 4. Strony ustaliły, że wdrożenie systemu ostrzegania w infrastrukturze Uczestnika rozpocznie się w dniu ……..…….....

§ 5. 1. W związku z wdrożeniem systemu ostrzegania ABW:
1) użycza Uczestnikowi platformę sprzętową*;
2) nie użycza platformy sprzętowej, gdyż Uczestnik posiada odpowiednią platformę sprzętową*.

2. W przypadku użyczenia Uczestnikowi przez ABW platformy sprzętowej:
1) przekazanie tej platformy odbędzie się na podstawie protokołu przekazania platformy sprzętowej;
2) instalacja tej platformy jest przeprowadzana przez Uczestnika na podstawie wytycznych przekazanych przez ABW.

§ 6. Wdrożenie systemu ostrzegania w infrastrukturze Uczestnika koordynuje ze strony ABW jednostka organizacyjna ABW właściwa do realizacji zadań z zakresu cyberbezpieczeństwa.

§ 7. 1. Koordynatorami wdrożenia systemu ostrzegania w infrastrukturze Uczestnika wyznaczonymi przez Uczestnika są następujące osoby:
1) ……., numer telefonu: ……..., adres e-mail: ……;
2) ……., numer telefonu: ……..., adres e-mail: ……..

2. Zmiana osób lub danych kontaktowych wymaga powiadomienia.

3. Zmienione dane osób lub dane kontaktowe Uczestnik niezwłocznie przekazuje pisemnie ABW.

* Niepotrzebne skreślić.

…….
(klauzula tajności – po wypełnieniu)

…….
(klauzula tajności – po wypełnieniu)

……. Egz. nr …….
(sygnatura literowo-cyfrowa)

§ 8. 1. Po przeprowadzeniu wdrożenia systemu ostrzegania ABW informuje Uczestnika o zakończeniu wdrożenia tego systemu oraz o jego uruchomieniu i sprawdzeniu poprawności działania systemu ostrzegania.

2. Informację, o której mowa w ust. 1, przekazuje się osobom wymienionym w § 7 ust. 1 przy użyciu środków komunikacji elektronicznej.

3. ABW nie ponosi odpowiedzialności za następstwa dysfunkcji w działaniu platformy sprzętowej oraz innych systemów Uczestnika, leżących po stronie Uczestnika.

§ 9. Uczestnik zapewnia, że dostęp programowy do zasobów na platformie sprzętowej, o której mowa w § 5 ust. 1 pkt 1, będzie posiadać wyłącznie ABW.

§ 10. 1. Uczestnik ma prawo dostępu do informacji przetwarzanych w systemie ostrzegania dotyczących tego Uczestnika, w tym raportów wygenerowanych przez system ostrzegania.

2. Raporty, o których mowa w ust. 1, informują o wykrytych nieprawidłowościach w ruchu sieciowym, agregując dostępne dane na potrzeby analizy zdarzeń.

3. Dostęp do informacji, o których mowa w ust. 1, jest wykonywany za pośrednictwem dostępu sieciowego poprzez graficzny interfejs użytkownika (GUI) i wymaga posiadania konta dostępowego, o którym mowa w § 7 ust. 3 rozporządzenia.

4. ABW przetwarza informacje dotyczące zidentyfikowanych anomalii w ruchu sieciowym występujących w infrastrukturze Uczestnika po poddaniu ich procesowi anonimizacji.

5. ABW może udostępniać informacje, o których mowa w ust. 4, innym Uczestnikom systemu ostrzegania, w formie informacji statystycznych wytwarzanych przez system ostrzegania, oraz wykorzystywać te informacje na potrzeby tworzenia sygnatur anomalii ruchu sieciowego.

§ 11. 1. Uczestnik zobowiązuje się do:

1) zachowania w tajemnicy informacji:
   a) uzyskanych w wyniku uczestnictwa w systemie ostrzegania,
   b) dotyczących sposobu działania systemu ostrzegania oraz jego aspektów technicznych;
2) przestrzegania warunków uczestnictwa w systemie ostrzegania określonych w § 5 ust. 1 rozporządzenia oraz wykonywania działań przewidzianych dla Uczestnika w przepisach rozporządzenia.

2. Uczestnik, który na podstawie przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) jest obowiązany do zgłaszania incydentów do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym, prowadzonego przez Ministra Obrony Narodowej albo Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, może przekazywać w ramach przedmiotowych zgłoszeń informacje techniczne uzyskane z systemu ostrzegania.

…….
(klauzula tajności – po wypełnieniu)

…….
(klauzula tajności – po wypełnieniu)

……. Egz. nr …….
(sygnatura literowo-cyfrowa)

§ 12. Porozumienie zostaje zawarte na czas nieokreślony.

§ 13. 1. Zmiany porozumienia wymagają zachowania formy pisemnej pod rygorem nieważności.

2. Zmiany, o których mowa w § 7 ust. 2, nie stanowią zmiany porozumienia.

§ 14. Porozumienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla każdej ze Stron.

§ 15. Porozumienie wchodzi w życie z dniem podpisania przez Strony.

Agencja Bezpieczeństwa Wewnętrznego	Uczestnik
……..	…….

Wykonano w 2 egzemplarzach:

Egz. nr 1: Uczestnik
Egz. nr 2: ABW

Wykonał: ……..

…….
(klauzula tajności – po wypełnieniu)