Warszawa, 17 kwietnia 2019 r.

Poz. 20

ZARZĄDZENIE Nr 20

MINISTRA GOSPODARKI MORSKIEJ I ŻEGLUGI ŚRÓDLĄDOWEJ[1)]

z dnia 16 kwietnia 2019 r.

w sprawie wytycznych dotyczących zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji

Na podstawie art. 42 ust. 1 pkt 5 w związku z art. 41 pkt. 3 i 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), zarządza się, co następuje:

§ 1. Wprowadza się do stosowania „Wytyczne dotyczące zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji”, zwane dalej „wytycznymi”, stanowiące załącznik do zarządzenia.

§ 2. Nadzór nad realizacją wykonania zarządzenia powierza się Dyrektorowi Biura Obrony i Ochrony Informacji Niejawnych w Ministerstwie Gospodarki Morskiej i Żeglugi Śródlądowej.

1) Minister Gospodarki Morskiej i Żeglugi Śródlądowej kieruje działami administracji rządowej: gospodarka morska, gospodarka wodna, rybołówstwo oraz żegluga śródlądowa na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 13 grudnia 2017 r. w sprawie szczegółowego zakresu działania Ministra Gospodarki Morskiej i Żeglugi Śródlądowej (Dz. U. poz. 2324 oraz z 2018 r. poz. 100).

§ 3. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

MINISTER

GOSPODARKI MORSKIEJ

I ŻEGLUGI ŚRÓDLĄDOWEJ

M.GRÓBARCZYK

Załącznik do Zarządzenia Nr 20
Ministra Gospodarki Morskiej
i Żeglugi Śródlądowej
z dnia 16 kwietnia 2019 r.
(Dz. Urz. MGMiŻŚ poz. 20)

WYTYCZNE

dotyczące zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji

Rozdział 1

Przepisy ogólne

§ 1. Wytyczne dotyczące zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji, zwane dalej „Wytycznymi”, określają:

1) rodzaj podmiotu zaliczonego do operatorów usług kluczowych w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji;
2) progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji;
3) progi uznania incydentu za poważny w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji;
4) rodzaje dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną;
5) tryb zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji.

§ 2. Ilekroć w Wytycznych jest mowa o:

1) armatorze w transporcie morskim pasażerów i towarów – należy przez to rozumieć właściciela statku lub jakąkolwiek organizację lub też osobę taką jak zarządca albo czarterujący statek, która przyjęła od właściciela odpowiedzialność za eksploatację statku i która po przyjęciu tej

odpowiedzialności zgodziła się przejąć wszelkie obowiązki i pełny zakres odpowiedzialności przewidzianej w Międzynarodowym kodeksie zarządzania bezpieczną eksploatacją statków i zapobieganiem zanieczyszczaniu (Kodeks ISM), który został przyjęty przez Międzynarodową Organizację Morską rezolucją Zgromadzenia A.741 (18) z dnia 4 listopada 1993 r., z późniejszymi zmianami wprowadzonymi przez rezolucję Komitetu Bezpieczeństwa Morskiego MSC.104 (73) z dnia 5 grudnia 2000 r.;

2) armatorze w żegludze śródlądowej – należy przez to rozumieć właściciela statku lub osobę, która uzyskała od właściciela tytuł prawny do władania statkiem we własnym imieniu;
3) CSIRT GOV – należy przez to rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
4) CSIRT NASK – należy przez to rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
5) Dyrektorze BOiIN – należy przez to rozumieć Dyrektora Biura Obrony i Ochrony Informacji Niejawnych Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej;
6) incydencie – należy przez to rozumieć zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
7) incydencie istotnym – należy przez to rozumieć incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci
i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48);
8) incydencie krytycznym – należy przez to rozumieć incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT GOV lub CSIRT NASK;
9) incydencie poważnym – należy przez to rozumieć incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

10) Ministrze – należy przez to rozumieć Ministra Gospodarki Morskiej i Żeglugi Śródlądowej, który jest organem właściwym do spraw cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji;
11) normie PN-EN ISO 22301 – należy przez to rozumieć standard, który został opublikowany przez Międzynarodowy Komitet Normalizacyjny ISO w maju 2012 r. jako pierwsza międzynarodowa norma zawierająca ramy dla identyfikacji kluczowych czynników ryzyka mających wpływ na organizację oraz na utrzymanie jej działań w najtrudniejszych warunkach;
12) obiekcie portowym – należy przez to rozumieć lokalizację, w której ma miejsce działanie w płaszczyźnie statek/port, w szczególności obszary takie jak kotwicowiska, podejścia od morza oraz miejsca cumowania statków w porcie;
13) OUK – należy przez to rozumieć operatora usługi kluczowej;
14) podmiocie zarządzającym portem – należy przez to rozumieć utworzony na podstawie ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2017 r. poz. 1933), podmiot powołany do zarządzania portem lub przystanią morską;
15) PTW – należy przez to rozumieć podsektor transportu wodnego;
16) Służbie Kontroli Ruchu Statków (VTS) – należy przez to rozumieć aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2018 r. poz. 181, 1137, 1669);
17) SZW – należy przez to rozumieć sektorze zaopatrzenia w wodę pitną i jej dystrybucji.

Rozdział 2

Operatorzy usług kluczowych

§ 3. Podmiotem zaliczonym do operatorów usług kluczowych w PTW jest:

1) armator w transporcie morskim pasażerów i towarów;
2) armator w żegludze śródlądowej;
3) podmiot zarządzający portem;
4) podmiot zarządzający obiektem portowym;
5) podmiot prowadzący działalność na terenie portu wspomagający transport morski;
6) Służba Kontroli Ruchu Statków (VTS).

§ 4. Podmiotem zaliczonym do operatorów usług kluczowych w SZW jest przedsiębiorstwo wodno-kanalizacyjne.

Rozdział 3

Progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej

§ 5. Progami istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej w PTW są:

1) dla armatora w transporcie morskim pasażerów i towarów:
   a) przewóz minimum 100 tys. pasażerów rocznie,
   b) przewóz minimum 1 mln ton towarów rocznie;
2) dla armatora w żegludze śródlądowej:
   a) udział w rynku w realizacji przewozów co najmniej 30% pasażerów rocznie,
   b) udział w rynku w realizacji przewozów co najmniej 40% towarów rocznie;
3) dla organu zarządzającego portem – przynależność do sieci bazowej TEN-T;
4) dla podmiotu zarządzającego obiektem portowym:
   a) obsługa minimum 100 tys. pasażerów rocznie,
   b) obsługa minimum 3 mln ton towarów rocznie,
   c) zależność od sektora energia i podsektora transport kolejowy;
5) dla podmiotu prowadzącego działalność wspomagającą w transporcie morskim – obsługa minimum 3 mln ton towarów rocznie;
6) dla VTS – gromadzenie i dystrybucja informacji związanej z bezpieczeństwem ruchu morskiego na obszarze odpowiedzialności urzędu morskiego.

§ 6. Progami istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej w SZW są:

1) dla ujęć wody – ujmowanie wody dla minimum 500 tys. podłączonych mieszkańców;
2) dla uzdatniania wody – uzdatnianie wody dla minimum 500 tys. podłączonych mieszkańców;
3) dla dostarczania wody – dostarczanie wody dla minimum 500 tys. podłączonych mieszkańców;
4) dla odprowadzania ścieków – obsługa aglomeracji o równoważnej liczbie mieszkańców (RLM) powyżej 500 tys.;

5) dla oczyszczania ścieków – obsługa aglomeracji o równoważnej liczbie mieszkańców (RLM) powyżej 500 tys.

Rozdział 4

Progi uznania incydentu za poważny

§ 7. Progami uznania incydentu za poważny w PTW są:

1) dla armatora w transporcie morskim pasażerów:
   a) podczas żeglugi – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku, stanowiące bezpośrednie niebezpieczeństwo utraty życia lub ciężkiego uszczerbku na zdrowiu lub innego niż ciężkiego uszczerbku na zdrowiu więcej niż jednej osoby lub środowiska naturalnego albo mienia,
   b) podczas cumowania – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 48 godzin;
2) dla armatora w transporcie morskim towarów:
   a) podczas żeglugi – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku, stanowiące bezpośrednie niebezpieczeństwo utraty życia lub ciężkiego uszczerbku na zdrowiu lub innego niż ciężkiego uszczerbku na zdrowiu więcej niż jednej osoby lub środowiska naturalnego albo mienia,
   b) podczas cumowania – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 48 godzin;
3) dla armatora w transporcie wodnym śródlądowym pasażerskim:
   a) incydent, który spowodował zakłócenie świadczenia usługi dla co najmniej 30% pasażerów rocznie,
   b) incydent, który spowodował brak dostępu do systemu teleinformatycznego w czasie dłuższym niż 72 godziny;
4) dla armatora w transporcie wodnym śródlądowym towarów:
   a) incydent, który spowodował zakłócenie świadczenia usługi dla co najmniej 40% towarów rocznie,
   b) incydent, który spowodował brak dostępu do systemu teleinformatycznego w czasie dłuższym niż 72 godziny;
5) dla funkcjonowania organu zarządzającego portem – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 12 godzin;

6) dla bezpieczeństwa organu zarządzającego portem – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania portu, powodujący niedostępność lub ograniczoną dostępność portu;
7) dla funkcjonowania podmiotu zarządzającego obiektem portowym – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 12 godzin;
8) dla bezpieczeństwa podmiotu zarządzającego obiektem portowym – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujący zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego lub mienia albo dla funkcjonowania obiektu portowego;
9) dla funkcjonowania podmiotu prowadzącego na terenie portu działalność wspomagającą transport morski – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 12 godzin;
10) dla bezpieczeństwa podmiotu prowadzącego na terenie portu działalność wspomagającą transport morski – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania portu, powodujący utrudnienia dla funkcjonowania portu;
11) dla funkcjonowania VTS – incydent, który spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 12 godzin;
12) dla bezpieczeństwa VTS – incydent, który spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania VTS, powodujący zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego lub mienia albo dla funkcjonowania portu.

§ 8. Progami uznania incydentu za poważny w SZW są:
1) dla poboru, uzdatniania i dostarczania wody – incydent, który spowodował brak dostępności usługi dla co najmniej 100 tys. użytkowników przez czas dłuższy niż 8 godzin;
2) dla odprowadzania i oczyszczania ścieków – incydent, który spowodował brak dostępności usługi dla co najmniej 100 tys. użytkowników (RLM) przez czas dłuższy niż 8 godzin.

Rozdział 5

Zadania i sposób postępowania operatorów usług kluczowych

§ 9. 1. Podmioty zaliczone do operatorów usług kluczowych w PTW i w SZW opracowują dokumentację cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej.

2. W skład dokumentacji, o której mowa w ust. 1 wchodzą:

1) dokumentacja normatywna, w szczególności:
   a) dokumentacja systemu zarzadzania bezpieczeństwem informacji wytworzona zgodnie z wymogami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, z późn. zm.[2)]),
   b) plan ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa, zawierający:
      – charakterystykę wykorzystywanych obiektów infrastruktury,
      – analizę stopnia zagrożenia dla wykorzystywanych obiektów infrastruktury,
      – ocenę aktualnego stanu ochrony,
      – opis zabezpieczeń technicznych obiektu,
      – zasady organizacji i wykonywania ochrony fizycznej,
      – dane dotyczące specjalistycznej uzbrojonej formacji ochronnej, jeśli występuje,
   c) plan zapewnienia ciągłości działania usługi kluczowej wytworzony zgodnie z wymogami normy PN-EN ISO 22301,
   d) dokumentacja techniczna systemu teleinformatycznego wykorzystywanego do świadczenia usługi kluczowej,
   e) inna dokumentacja – według decyzji podmiotu, wynikająca ze specyfiki świadczonej usługi kluczowej;
2) dokumentacja operacyjna, w szczególności:
   a) procedury oraz instrukcje wynikające z dokumentacji normatywnej,
   b) wzory zapisów dokumentujących wykonanie procedury,
   c) zapisy dokumentujące każdorazowe wykonanie procedury tworzone w postaci papierowej lub elektronicznej.

§ 10. Podmioty zaliczone do operatorów usług kluczowych w PTW i w SZW, które są jednocześnie operatorami infrastruktury krytycznej, obowiązane są do stosowania standardów postępowania w zakresie ochrony osób i mienia określonych w ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2018 r. poz. 2142 i 2245) oraz aktach wykonawczych wydanych na jej podstawie.

§ 11. Do zadań operatora usługi kluczowej w PTW i w SZW w ramach obsługi incydentu należą:

1) zapewnienie obsługi incydentu;

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 1000, 1083, 1669 oraz z 2019 r. poz. 125.

2) zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT w zakresie niezbędnym do realizacji jego zadań;
3) klasyfikacja incydentu jako poważnego na podstawie progów uznawania incydentu za poważny;
4) zgłaszanie incydentu poważnego, o którym mowa w § 4, niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT;
5) współdziałanie podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe;
6) usuwanie podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego oraz informowanie o ich usunięciu Ministra za pośrednictwem Dyrektora BOiIN.

§ 12. Ustala się następujący tryb zgłaszania incydentu, o którym mowa w § 5 i 6, w ramach krajowego systemu cyberbezpieczeństwa:

1) podmioty zaliczone do operatorów usług kluczowych w PTW i w SZW, które są jednocześnie operatorami infrastruktury krytycznej, o której mowa w § 10, zgłaszają incydent do CSIRT GOV, informując o nim jednocześnie Ministra za pośrednictwem Dyrektora BOIN;
2) VTS zgłasza incydent do CSIRT GOV, informując o nim jednocześnie Ministra za pośrednictwem Dyrektora BOiIN;
3) podmioty zaliczane do jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 2 i 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077, z poźń. zm.[3)]), z wyjątkiem podmiotów, o których mowa w pkt 1, zgłaszają incydent do CSIRT NASK, informując o nim jednocześnie Ministra za pośrednictwem Dyrektora BOiIN;
4) podmioty będące spółkami prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827, z 2018 r. poz. 1496, 1693 oraz z 2019 r. poz. 492), z wyjątkiem podmiotów, o których mowa w pkt 1, zgłaszają incydent do CSIRT NASK, informując o nim jednocześnie Ministra za pośrednictwem Dyrektora BOiIN;
5) wszystkie podmioty zaliczone do operatorów usług kluczowych w PTW i w SZW, w przypadku incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730), zgłaszają incydent do CSIRT

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 62, 1000, 1366, 1669, 1693, 2245, 2354, 2500 oraz z 2019 r. poz. 303, 326 i 534.

GOV, informując o nim jednocześnie Ministra za pośrednictwem Dyrektora BOiIN oraz CSIRT NASK, według właściwości.