



DZIENNIK URZĘDOWY

Ministra Gospodarki Morskiej i Żeglugi Śródlądowej

Warszawa, dnia 10 kwietnia 2020 r.

Poz. 20

ZARZĄDZENIE NR 17

MINISTRA GOSPODARKI MORSKIEJ I ŻEGLUGI ŚRÓDLĄDOWEJ¹⁾

z dnia 7 kwietnia 2020 r.

w sprawie warunków organizacyjno-technicznych oraz 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 oraz z 2019 r. poz. 2020 i 2248), zarządza się, co następuje:

§ 1. Wprowadza się do stosowania „Wytyczne w sprawie warunków organizacyjno-technicznych oraz zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji”, stanowiące załącznik do zarządzenia.

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

§ 3. Traci moc zarządzenie nr 20 Ministra Gospodarki Morskiej i Żeglugi Śródlądowej 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 (Dz. Urz. MG MiŻŚ poz. 20).

1) Minister Gospodarki Morskiej i Żeglugi Śródlądowej kieruje działami administracji rządowej: gospodarka morską, gospodarka wodna, rybołówstwo oraz żegluga śródlądowa na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Gospodarki Morskiej i Żeglugi Śródlądowej (Dz. U. poz. 2262).

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

MINISTER GOSPODARKI MORSKIEJ

I ŻEGLUGI ŚRODLĄDOWEJ

M. GRÓBARCZYK

Załącznik
do zarządzenia nr 17
Ministra Gospodarki Morskiej
i Żeglugi Śródlądowej
z dnia 7 kwietnia 2020 r.
(Dz. Urz. MG MiŻŚ poz. 20)

WYTYCZNE

w sprawie warunków organizacyjno-technicznych oraz zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji

Rozdział I

Przepisy ogólne

§ 1. Wytyczne w sprawie warunków organizacyjnych oraz 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, zwanego dalej „PTW”, i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji, zwanym dalej „SZW”;
- 2) warunki organizacyjne i techniczne dla podmiotów świadczących usługi kluczowe z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
- 3) progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej w PTW i w SZW;
- 4) progi uznania incydentu za poważny w PTW i w SZW;
- 5) rodzaje dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej w PTW i w SZW;
- 6) tryb zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w PTW i w SZW.

§ 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 zanieczyszczeniu (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 armatora w rozumieniu art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2019 r. poz. 1568, 1901 i 2170 oraz z 2020 r. poz. 284);
- 3) CSIRT GOV – należy przez to rozumieć zespół w rozumieniu art. 2 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248);
- 4) CSIRT NASK – należy przez to rozumieć zespół w rozumieniu art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 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 incydent w rozumieniu art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 7) incydencie istotnym – należy przez to rozumieć incydent w rozumieniu art. 2 pkt 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 8) incydencie krytycznym – należy przez to rozumieć incydent w rozumieniu art. 2 ust. 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 9) incydencie poważnym – należy przez to rozumieć incydent w rozumieniu art. 2 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 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) obiekcie portowym – należy przez to rozumieć obiekt portowy, o którym mowa w art. 3 ust. 1 pkt 3 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2019 r. poz. 692);
- 12) podmiocie zarządzającym portem – należy przez to rozumieć podmiot zarządzający, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2017 r. poz. 1933 oraz z 2019 r. poz. 1716);
- 13) rozporządzeniu 2017/352 – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady UE 2017/352 z dnia 15 lutego 2017 r. ustanawiające ramy w zakresie świadczenia usług

portowych oraz wspólne zasady dotyczące przejrzystości finansowej portów (Dz. Urz. UE L 57/1 z 03.03.2017, str. 1);

- 14) 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, 1669 i 2245 oraz z 2019 r. poz. 2197 i 2303);
- 15) ustawie – należy przez to rozumieć ustawę z dnia 5 lipca 2018 r. w sprawie krajowego systemu cyberbezpieczeństwa.

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

Warunki organizacyjno-techniczne dla świadczenia usługi kluczowej

§ 5.1. Podmioty zaliczone do operatorów usług kluczowych w PTW i w SZW są obowiązane zgodnie z art. 14 ustawy, do powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z podmiotem zewnętrznym na outsourcing funkcji cyberbezpieczeństwa.

2. Zadaniem struktur wewnętrznych oraz podmiotów zewnętrznych świadczących usługi z zakresu cyberbezpieczeństwa jest realizacja wszystkich obowiązków operatora usług kluczowych, wynikających z ustawy z wyłączeniem audytu.

3. Struktury wewnętrzne oraz podmioty zewnętrzne świadczące usługi z zakresu cyberbezpieczeństwa są obowiązane do:

- 1) spełnienia warunków organizacyjnych i technicznych, które pozwolą na zapewnienie bezpieczeństwa obsługiwanemu operatorowi usług kluczowych;
 - 2) posiadania odpowiednio zabezpieczonych pomieszczeń, w których możliwe jest prawidłowe świadczenie usług z zakresu reagowania na incydenty;
 - 3) posiadania odpowiednich środków bezpieczeństwa, w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji uwzględniających bezpieczeństwo osobowe oraz eksploatację i architekturę systemów.
4. Szczegółowy zakres warunków, o których mowa w ust. 3, określa rozporządzenie Ministra Cyfryzacji z dnia 23 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu świadczenia cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 2479).

Rozdział 4

Progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej

§ 6. Progi 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 na terenie portu działalność wspomagającą w transporcie morskim – każdy podmiot wykonujący usługi, w zakresie bunkrowania, cumowania, pilotażu oraz holowania, o których mowa w rozporządzeniu 2017/352;
- 6) dla VTS – gromadzenie i dystrybucja informacji związanej z bezpieczeństwem ruchu morskiego na obszarze odpowiedzialności urzędu morskiego.

§ 7. 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 5

Progi uznania incydentu za poważny

§ 8. 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.

§ 9. 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 6

Zadania i sposób postępowania operatorów usług kluczowych

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

2. Szczegółowy zakres dokumentacji dotyczący cyberbezpieczeństwa systemów informacyjnych reguluje rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080).

§ 11. 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 z 2019 r. poz. 1495) oraz aktach wykonawczych wydanych na jej podstawie.

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

- 1) zapewnienie obsługi incydentu;
- 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.

§ 13. 1. Ustala się następujący tryb zgłaszania incydentu, o którym mowa w § 6 i 7, 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 § 11, zgłaszają incydent do CSIRT GOV;
- 2) VTS zgłasza incydent do CSIRT GOV;
- 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 2019 r. poz. 869 z późn. zm.²⁾), z wyjątkiem podmiotów, o których mowa w pkt 1, zgłaszają incydent do CSIRT NASK;
- 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 2019 r. poz. 712 i 2020), z wyjątkiem podmiotów, o których mowa w pkt 1, zgłaszają incydent do CSIRT NASK;
- 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 2019 r. poz. 796), zgłaszają incydent do CSIRT GOV.

2. O trybie zgłaszania incydentu, o którym mowa w ust. 1, podmioty informują Ministra, za pośrednictwem Dyrektora BOiIN z wykorzystaniem poczty elektronicznej – ouk.incident@mgm.gov.pl lub, w przypadku braku dostępu do poczty elektronicznej, telefonicznie.

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 1622, 1649, 2020 i 2473 oraz z 2020 r. poz. 284 i 374.