Warszawa, dnia 23 grudnia 2019 r.

Poz. 2479

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 4 grudnia 2019 r.

w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

Na podstawie art. 14 ust. 4 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. 1. Podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest obowiązany spełnić następujące warunki organizacyjne:

1) posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi;

2) zapewnić ciągłość działania usłudze obsługi incydentu oraz wsparcie operatorowi usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej;

3) posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF);

4) w zakresie realizowanych obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, dysponować personelem posiadającym umiejętności:

   a) identyfikowania zagrożeń w odniesieniu do systemów informacyjnych operatora usługi kluczowej oraz proponowania rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,

   b) analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,

   c) wykrywania przełamania lub ominięcia zabezpieczeń systemu informacyjnego operatora usługi kluczowej, prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej,

   d) zabezpieczania informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących:

      – rodzajów usług kluczowych, na które incydent miał wpływ,

      – liczby użytkowników usługi kluczowej, na których incydent miał wpływ,

      – momentu wystąpienia i wykrycia incydentu oraz czas jego trwania,

      – zasięgu geograficznego obszaru, którego dotyczy incydent poważny,

---

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2270).

– wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,

– przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania;

5) dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń – w przypadku realizacji obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

6) przeprowadzić analizę ryzyka mającą na celu dobór adekwatnych środków bezpieczeństwa fizycznego i technicznego pomieszczenia lub zespołu pomieszczeń, w których świadczone są usługi z zakresu cyberbezpieczeństwa, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo, w szczególności:

a) rodzaje informacji przetwarzanych w systemach teleinformatycznych,

b) otoczenie i konstrukcję budynków, w których będą świadczone usługi z zakresu cyberbezpieczeństwa,

c) liczbę osób mających lub mogących mieć dostęp do pomieszczenia lub zespołu pomieszczeń, a także posiadane przez nie uprawnienia oraz uzasadnioną potrzebę dostępu do pomieszczenia lub zespołu pomieszczeń,

d) szacowane zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą.

2. Wewnętrzna struktura organizacyjna operatora usługi kluczowej odpowiedzialna za cyberbezpieczeństwo jest obowiązana spełniać warunki, o których mowa w ust. 1 pkt 1, 2 i 4–6.

§ 2. 1. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo są obowiązane spełniać następujące warunki techniczne:

1) dysponować sprzętem komputerowym oraz wyspecjalizowanymi narzędziami informatycznymi umożliwiającymi:

a) rejestrowanie zgłoszeń incydentów,

b) analizę kodu oprogramowania uznanego za szkodliwe,

c) badanie odporności systemów informacyjnych na przełamanie lub ominięcie zabezpieczeń,

d) zabezpieczanie informacji potrzebnych do analizy powłamaniowej pozwalające na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących:

– rodzajów usług kluczowych, na które incydent miał wpływ,

– liczby użytkowników usługi kluczowej, na których incydent miał wpływ,

– momentu wystąpienia i wykrycia incydentu oraz czasu jego trwania,

– zasięgu geograficznego obszaru, którego dotyczy incydent poważny,

– wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,

– przyczyny zaistnienia incydentu i sposób jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania;

2) dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi, oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

2. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo, które wykonują czynności związane z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, są obowiązane stosować następujące zabezpieczenia pomieszczenia lub zespołu pomieszczeń adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej:

1) ściany i stropy pomieszczenia lub zespołu pomieszczeń, w których będą świadczone usługi z zakresu cyberbezpieczeństwa, powinny mieć klasę odporności ogniowej co najmniej EI 60, określoną w Polskiej Normie PN-EN 13501, a budynek, w którym będą świadczone usługi z zakresu cyberbezpieczeństwa, powinien mieć klasę odporności pożarowej nie niższą niż klasa B, określoną w przepisach wydanych na podstawie art. 7 ust. 2 pkt 1 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2019 r. poz. 1186, z późn. zm.[2)]);

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 1309, 1524, 1696, 1712, 1815, 2166 i 2170.

2) drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia lub zespołu pomieszczeń;

3) konstrukcję pomieszczenia lub zespołu pomieszczeń zapewniającą odporność na próbę nieuprawnionego dostępu;

4) okna spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich niesie nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia lub zespołu pomieszczeń;

5) szafy o podwyższonej odporności ogniowej, zabezpieczające przed próbami włamań oraz pożarami, odpowiednio do wartości danych oraz ewentualnych innych zagrożeń, na podstawie przeprowadzonego szacowanego ryzyka, służące do przechowywania dokumentacji papierowej oraz informatycznych nośników danych mających istotne znaczenie dla prowadzonej działalności;

6) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia kontrolowanego obszaru, w którym co najmniej rozpoznanie osoby uprawnionej następuje w wyniku odczytu identyfikatora lub odczytu cech biometrycznych, oraz rejestrujący zdarzenia;

7) stały nadzór osoby uprawnionej nad osobami niewykonującymi czynności związanych z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przebywającymi w pomieszczeniu lub zespole pomieszczeń, w których wykonywane są te czynności;

8) system sygnalizacji napadu i włamania spełniający co najmniej wymagania systemu stopnia 2 określone w Polskiej Normie PN-EN 50131-1, stale monitorowany przez personel bezpieczeństwa oraz wyposażony w rezerwowe źródło zasilania i obejmujący ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizujący co najmniej:

   a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru,

   b) poruszanie się w chronionym obszarze,

   c) stan systemu, w tym generujący ostrzeżenia i alarmy;

9) system sygnalizacji pożarowej obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, przy czym obiekty wyposażone w stałe urządzenia gaśnicze i objęte całodobowym nadzorem co najmniej jednej osoby nie muszą być wyposażone w system sygnalizacji pożarowej.

§ 3. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo realizujące inne obowiązki niż wymienione w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 lub art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zobowiązane są wprowadzić zabezpieczenia adekwatne do przetwarzanych informacji na podstawie przeprowadzonego szacowanego ryzyka, a także z wykorzystaniem dobrych praktyk, mając na celu skuteczne:

1) monitorowanie i wykrywanie incydentów bezpieczeństwa informacji;

2) reagowanie na incydenty bezpieczeństwa;

3) zapobieganie incydentom bezpieczeństwa informacji;

4) zarządzanie jakością zabezpieczeń systemów, informacji i powierzonych aktywów;

5) aktualizowanie ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.

§ 4. W przypadku wykonywania czynności związanych z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poza pomieszczeniami wyposażonymi w zabezpieczenia opisane w § 2 ust. 2, podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo zapewniają bezpieczny zdalny dostęp do systemu obsługującego usługi z zakresu cyberbezpieczeństwa, przez co najmniej:

1) ustalenie zasad dostępu do systemu;

2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;

3) minimalizację przechowywanych danych poza bezpiecznym środowiskiem.

§ 5. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo dostosują pomieszczenia lub zespoły pomieszczeń do wymogów określonych w przepisach niniejszego rozporządzenia w terminie 6 miesięcy od dnia wejścia w życie rozporządzenia.

§ 6. Traci moc rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 1780).

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

Minister Cyfryzacji: *M. Zagórski*