Warszawa, dnia 17 września 2018 r.

Poz. 1780

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

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

Na podstawie art. 14 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zarządza się, co następuje:

§ 1. 1. Podmiot świadczący usługi z zakresu cyberbezpieczeństwa w zakresie warunków organizacyjnych jest obowiązany:

1) posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001;

2) zapewnić ciągłość działania usłudze reagowania na incydenty, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów informacyjnych zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;

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) zapewnić wsparcie operatorowi usługi kluczowej w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej;

5) dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:

   a) identyfikowania zagrożeń w odniesieniu do systemów informacyjnych,

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

   c) zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

2. Wewnętrzna struktura organizacyjna operatora usługi kluczowej jest obowiązana spełniać warunki, o których mowa w ust. 1 pkt 1, 2, 4 i 5.

§ 2. 1. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo są obowiązane dysponować prawem do wyłącznego korzystania z pomieszczeń, które wyposażone są w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej w:

1) system sygnalizacji włamania i napadu klasy 2 według Polskiej Normy PN-EN 50131-1;

---

1) Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761).

2) system kontroli dostępu klasy 2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia przez rzecz posiadaną przez tą osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem;

3) system wykrywania i sygnalizacji pożaru z powiadamianiem do centrum odbiorczego alarmów pożarowych;

4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych o istotnym znaczeniu dla prowadzonej działalności, klasy S1 spełniającymi wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy wymagają wyższej klasy odporności szaf;

5) zewnętrzne drzwi wejściowe do pomieszczeń o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;

6) wewnętrzne drzwi do pomieszczeń o klasie odporności RC2 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;

7) okna o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia;

8) ściany zewnętrzne o odporności na włamanie równoważnej odporności muru o grubości 25 cm wykonanego z pełnej cegły;

9) ściany wewnętrzne o odporności na włamanie adekwatnej do klasy odporności drzwi.

2. W przypadku, gdy obiekt, w którym znajdują się pomieszczenia wskazane w ust. 1, nie jest wyposażony w system, o którym mowa w ust. 1 pkt 3, dopuszcza się, po wykonaniu szacowania ryzyka i gdy brak jest przeciwwskazań wynikających z innych przepisów, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania i napadu, o ile stacja monitorująca alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów.

§ 3. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo w zakresie spełnienia warunków technicznych dysponują:

1) sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:

   a) automatyczne rejestrowanie zgłoszeń incydentów,

   b) analizę kodu oprogramowania uznanego za szkodliwe,

   c) badanie odporności systemów informacyjnych na przełamanie zabezpieczeń,

   d) zabezpieczanie śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania;

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

§ 4. Rozporządzenie wchodzi w życie z dniem ogłoszenia.

Minister Cyfryzacji: *M. Zagórski*