Warszawa, dnia 29 czerwca 2020 r.

Poz. 1130

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 22 czerwca 2020 r.

w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług

Na podstawie art. 175d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875) zarządza się, co następuje:

§ 1. Rozporządzenie określa minimalne środki techniczne i organizacyjne, zwane dalej „środkami", oraz metody zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług.

§ 2. Przedsiębiorca telekomunikacyjny:

1) opracowuje i aktualizuje dokumentację dotyczącą bezpieczeństwa i integralności sieci i usług zawierającą opis środków, o których mowa w pkt 2–13;

2) opracowuje i aktualizuje wykaz elementów infrastruktury telekomunikacyjnej i systemów informatycznych, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy, zwanych dalej „kluczową infrastrukturą";

3) identyfikuje zagrożenia bezpieczeństwa lub integralności sieci lub usług;

4) ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń na bezpieczeństwo lub integralność sieci lub usług;

5) zapewnia i stosuje środki minimalizujące skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo lub integralność sieci lub usług;

6) ustanawia zasady i procedury dostępu do kluczowej infrastruktury i przetwarzanych danych, obejmujące przypisanie odpowiedzialności za kluczową infrastrukturę w zakresie odpowiednim do realizowanych zadań;

7) zabezpiecza dostęp do kluczowej infrastruktury, monitoruje ten dostęp i wskazuje środki reagowania na nieuprawniony dostęp lub próbę takiego dostępu;

8) ustanawia zasady bezpiecznego zdalnego przetwarzania danych;

9) stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii danych;

10) zawierając umowy mające istotny wpływ na funkcjonowanie sieci lub usług, identyfikuje zagrożenia dla bezpieczeństwa tych sieci lub usług, związane z zawieranymi umowami;

[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).

11) zapewnia monitorowanie i dokumentowanie funkcjonowania sieci i usług telekomunikacyjnych mające na celu wykrycie naruszenia bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, i ustalenie przyczyn takiego naruszenia;

12) ustala wewnętrzne procedury zgłaszania naruszeń bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, oraz umożliwia użytkownikom końcowym dokonywanie zgłoszeń wszelkich naruszeń bezpieczeństwa lub integralności sieci lub usług;

13) przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych:

a) co najmniej raz na dwa lata,

b) po każdym:

– stwierdzonym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym naruszeniem, oraz

– wykryciu podatności zwiększającej poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym wykrytą podatnością.

§ 3. 1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym, realizując środki, o których mowa w § 2 pkt 3–5, w ramach tej sieci:

1) uwzględnia rekomendacje, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. 695 i 875);

2) stosuje strategię skutkującą brakiem uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;

3) zapewnia podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych.

2. Przedsiębiorca telekomunikacyjny prowadzi dokumentację działań, o których mowa w ust. 1.

§ 4. Rozporządzenie wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia.

Minister Cyfryzacji: *M. Zagórski*