Projekt z dnia 24 stycznia 2020 r.

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia …… 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) zarządza się, co następuje:

§ 1. Rozporządzenie określa minimalne środki techniczne i organizacyjne 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 przedsięwzięć, o których mowa w pkt 2-14;
2) opracowuje i aktualizuje wykaz infrastruktury telekomunikacyjnej i oprogramowania służących do świadczenia usług telekomunikacyjnych, obejmujący ich rodzaj i konfigurację;
3) identyfikuje zagrożenia, uwzględniając w szczególności długoterminowe analizy strategiczne cyberzagrożeń i incydentów w celu rozpoznania pojawiających się tendencji i w celu pomocy w zapobieganiu incydentom, o których mowa w art. 9 lit. b i e rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 7.6.2019, str. 15);

[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).

4) ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń, o których mowa w pkt 3, na bezpieczeństwo lub integralność sieci lub usług;
5) zapewnia środki minimalizujące skutki wystąpienia oddziaływań zagrożeń, o których mowa w pkt 3;
6) stosuje środki, o których mowa w pkt 5, w przypadku wystąpienia zagrożeń, o których mowa w pkt 3;
7) ustanawia zasady i procedury dostępu do kluczowych zasobów systemowych i przetwarzanych danych, obejmujących przypisanie odpowiedzialności za infrastrukturę telekomunikacyjną i oprogramowanie mających istotny wpływ na funkcjonowanie sieci lub usług telekomunikacyjnych w zakresie odpowiednim do realizowanych zadań;
8) zabezpiecza dostęp do kluczowych zasobów infrastruktury telekomunikacyjnej, monitoruje ten dostęp i wskazuje środki reagowania na nieuprawniony dostęp lub próbę takiego dostępu;
9) ustanawia zasady gwarantujące bezpieczeństwo zdalnego przetwarzania danych;
10) zabezpiecza dane w sposób znacząco redukujący możliwość ich nieuprawnionego przetwarzania;
11) zawierając umowy mające istotny wpływ na funkcjonowanie sieci lub usług, identyfikuje zagrożenia dla bezpieczeństwa tych sieci lub usług, związane z zawieranymi umowami;
12) zapewnia monitorowanie i dokumentowanie funkcjonowania sieci i usług telekomunikacyjnych mających na celu wykrycie naruszenia bezpieczeństwa i ustalenie przyczyn takiego naruszenia;
13) ustala procedury umożliwiające zgłaszanie naruszeń bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
14) przeprowadza okresową ocenę bezpieczeństwa sieci i usług telekomunikacyjnych, co najmniej raz na rok lub po każdym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług albo po każdym wykryciu podatności na zagrożenia zwiększającej poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług.

§ 3. 1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) w ramach tej sieci identyfikuje zagrożenia, ocenia prawdopodobieństwo ich wystąpienia,

zapewnia i stosuje środki minimalizujące skutki wystąpienia zagrożeń, w zakresie bezpieczeństwa i integralności sieci i usług, uwzględniając:

1) rekomendacje, o których mowa w art. 33 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);
2) unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług oraz wykorzystaniu najnowocześniejszych osiągnięć technicznych;
3) 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

Za zgodność pod względem prawnym, redakcyjnym i legislacyjnym
Iwona Szulc
Zastępca Dyrektora
Departamentu Prawnego
Ministerstwa Cyfryzacji
/-podpisano elektronicznie/

Uzasadnienie

Przedłożony projekt rozporządzenia w sprawie minimalnych środków technicznych i organizacyjnych dla przedsiębiorców telekomunikacyjnych stanowi wykonanie upoważnienia zawartego w art. 175d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460), zwanej dalej „PT". Wskazany przepis upoważnia ministra właściwego do spraw informatyzacji do określenia w drodze rozporządzenia minimalnych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, o których mowa w art. 175a i art. 175c ustawy, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Wydając rozporządzenie niezbędne jest z uwzględnienie wytycznych Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji w tym zakresie (ENISA, obecnie pod zmienioną nazwą: Europejska Agencja do spraw Cyberbezpieczeństwa).

Upoważnienie to ma charakter fakultatywny i rozporządzenie takie dotychczas nie zostało wydane, jednakże rozwój w telekomunikacji nowych technologii wrażliwych na naruszenia bezpieczeństwa (incydenty) wskazuje na potrzebę wskazania minimalnych środków technicznych i organizacyjnych zapewniającą bezpieczeństwo sieci, świadczonych usług oraz przetwarzania danych. Wprowadzone rozwiązania mają na celu zmniejszenie poziomu ryzyka oraz zagwarantowanie ciągłości działania. Należy przy tym zauważyć, że projektowane przepisy rozporządzenia powinny być neutralne technologicznie, a zatem nie mogą podawać konkretnych rozwiązań, a jedynie wskazywać na cel zastosowania środków technicznych. Należy także podkreślić związek pomiędzy środkami technicznymi i organizacyjnymi, polegający na tym, że każde rozwiązanie techniczne podlega procesowi zarządzania, a to jest związane ze środkami organizacyjnymi.

Artykuł 175 ust. 1 PT nakłada na przedsiębiorców telekomunikacyjnych obowiązek zapewnienia bezpieczeństwa i integralności sieci, usług i przekazu komunikatów za pomocą odpowiednich środków technicznych i organizacyjnych. Minister właściwy do spraw informatyzacji może w drodze rozporządzenia określić minimalne środki techniczne i organizacyjne (art. 175d PT).

Zarówno w interesie obywateli, jak i Państwa jest, aby przedsiębiorcy telekomunikacyjni mieli obowiązek stosowania konkretnych rozwiązań w celu zapewnienia bezpieczeństwa sieci i usług telekomunikacyjnych. Wraz z rozwojem technologii zwiększa się także liczba zagrożeń, które mogą wpłynąć na bezpieczeństwo i integralność sieci i usług telekomunikacyjnych, utrudniać życie obywatelom oraz niekorzystnie wpływać na sprawne funkcjonowanie Państwa.

W obecnej sytuacji przedsiębiorcy telekomunikacyjni sami decydują, jakie rodzaje środków technicznych i organizacyjnych chcą zastosować, aby zapewnić bezpieczeństwo sieci i usług telekomunikacyjnych. Brakuje jednolitych standardów prawnych, które działając w interesie obywateli, obligowałyby przedsiębiorców telekomunikacyjnych do stosowania konkretnych rodzajów rozwiązań w zakresie bezpieczeństwa. Artykuł 175 ust. 1 PT jest transpozycją artykułu 13a dyrektywy ramowej[2]. Państwa członkowskie mają informować się wspólnie oraz ENISA o istotnych incydentach bezpieczeństwa w telekomunikacji. Na podstawie tych informacji ENISA publikuje raporty o bezpieczeństwie w telekomunikacji.

Raport ENISA z 2018 r[3]. opiera się na 169 istotnych incydentach zgłoszonych do ENISA przez kraje członkowskie UE oraz EFTA. Spośród nich 51% miało wpływ na telefonię mobilną i Internet mobilny. Główną przyczyną (62% z ogółu zgłoszonych) incydentów bezpieczeństwa były awarie systemów, polegające najczęściej na awariach sprzętowych tudzież błędach oprogramowania. Awarie sprzętowe najczęściej dotyczyły przełączników sieciowych, ruterów, stacji bazowych sieci mobilnej, sterowników i systemów zasilania. Około 18% zgłoszonych incydentów było związanych z błędami ludzkimi. Dotyczyły średnio 1,2 mln połączeń.

W porównaniu z poprzednimi latami zwiększyła się ilość incydentów związana ze skutkami działalności natury – śniegu, burz, pożarów lasów (około 17% zgłoszonych incydentów). Podczas tego rodzaju incydentów, przez 96 godzin użytkownicy sieci nie mogli uzyskać do niej dostępu i stracili średnio 56,8 tys. użytkownikogodzin, co było najwyższym wynikiem spośród wszystkich incydentów. Ataki z wykorzystaniem szkodliwego oprogramowania stanowiły ok. 2% ze zgłoszonych incydentów. Spośród wszystkich incydentów 18% stanowiły awarie po stronie trzeciej. 1/3 incydentów miała wpływ na dostępność do numeru alarmowego 112.

Według raportu Urzędu Komunikacji Elektronicznej (UKE) w 2018 r. zgłoszono Prezesowi UKE 198 przypadków naruszeń bezpieczeństwa. Pięć z nich dotyczyło obszaru całego kraju, 4 obszaru kilku województw, a reszta dotyczyła obszaru gmin (157 przypadków obejmowało obszary od 1 do 10 gmin, 30 przypadków obejmował obszary powyżej 10 gmin). Najbardziej ucierpieli od naruszeń użytkownicy telefonii komórkowej i Internetu mobilnego (odpowiednio 525 tys. oraz 100 tys. użytkowników) W zdecydowanej ilości przypadków

---

[2] Dz. Urz. UE L 337/37 z 18.12.2009.

[3] ENISA, *Annual Report Telecom Security Incidents 2017*, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017, dostęp z dnia 19.09.2019 r.)

naruszenia dotyczyły dostępu do numerów alarmowych (190 przypadków), 22 przypadki dotyczyły integralności sieci, a 2 przypadki dotyczyły zagrożeń cyberbezpieczeństwa.

Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16 naruszeń, przerwa w zasilaniu - 6, a błąd ludzki - 5. Marginalne były przyczyny spowodowane klęską żywiołową i cyberatakiem.

Z powyższych danych wynika, że aby zwiększyć bezpieczeństwo w telekomunikacji przedsiębiorcy telekomunikacyjni powinni kłaść większy nacisk na bezpieczeństwo sprzętowe i oprogramowania, odpowiednie szkolenie pracowników co do najnowszych technologii, a także nad ochroną infrastruktury sieciowej przed warunkami atmosferycznymi. Mając na uwadze zjawisko konwergencji telekomunikacji i teleinformatyki w nadchodzącym okresie należy spodziewać się zwiększenia liczby naruszeń spowodowanych cyberatakami. Istotne jest też, aby przedsiębiorcy zwracali uwagę na dobór strony trzeciej (podwykonawców, usługodawców) nie tylko na i ich poziom techniczny oraz merytoryczny, ale także na sposób zarządzania bezpieczeństwem. Ze względu na interes społeczny ważne jest zapobieganie niedostępności numerów alarmowych. W Polsce najczęściej incydenty dotyczyły obszaru kilku gmin – toteż należy podjąć działania, aby obywatele tych obszarów nie byli dyskryminowani w dostępie do telekomunikacji. Projektowane rozporządzenie ma na celu wprowadzenie ogólnych standardów bezpieczeństwa telekomunikacyjnego na terenie całego kraju. Dzięki temu wszyscy obywatele będą mieli pewność, że wszyscy przedsiębiorcy telekomunikacyjni tak samo sprawnie i szybko reagują na incydenty, które uniemożliwiają korzystanie z usług telekomunikacyjnych.

Obecny stan prawny nakłada na przedsiębiorców telekomunikacyjnych obowiązek podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa oraz integralności sieci i usług. Brak za to regulacji zawierającej określenie minimalnych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 PT. Niniejsze rozporządzenie wypełnia tą lukę, jednak nie nakłada nowych obowiązków, a jedynie precyzując istniejące.

Przedsiębiorcy telekomunikacyjni będą obowiązani stosować projektowane środki w swojej działalności. Warto jednak wskazać, że mają one minimalny charakter i nie są nowymi przedsięwzięcia w branży – podobne regulacje istnieją w innych krajach. Wielu przedsiębiorców telekomunikacyjnych już obecnie stosuje środki, o których mowa w rozporządzeniu.

Przepisy § 2 rozporządzenia określają minimalne środki techniczne i organizacyjne oraz metody, które obejmą swoim zakresem ogólną działalność telekomunikacyjną.

Obowiązki zawarte w § 2 wynikają z wytycznych ENISA dotyczących minimalnych środków bezpieczeństwa[4], o których mowa w art. 13a Dyrektywy Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r.[5] i posiadają pełne odniesienie do wspomnianych wytycznych. W nowym Europejskim Kodeksie Łączności Elektronicznej istnieje bardzo podobna podstawa prawna (art. 40 i 41)[6].

Zarządzanie bezpieczeństwem zależne jest w szczególności od prawidłowego funkcjonowania dwóch procesów: procesu identyfikacji zasobów (zwanych też aktywami) oraz procesu zarządzania ryzykiem. Wprowadzenie konkretnych zabezpieczeń technicznych i organizacyjnych, w wyspecyfikowanych w wytycznych ENISA obszarach, wynika z postępowania z oszacowanym ryzykiem.

Aby ułatwić stosowanie przepisów § 2 rozporządzenia również u małych i średnich przedsiębiorców, odstąpiono od technicznego języka wytycznych i uproszczono niektóre wymogi.

Należy zaznaczyć, że ten sam cel zabezpieczenia w wielu przypadkach można osiągnąć zarówno środkami organizacyjnym, jak i technicznymi. Biorąc pod uwagę, że rozporządzenie skierowane jest do operatorów o różnej skali prowadzonej działalności, w rozporządzeniu wskazano cel zabezpieczenia. Środki do osiągnięcia celu zabezpieczenia pozostawione są do wyboru przez operatora.

W § 2 projektu punkt 1 wskazuje na obowiązek prowadzenia odpowiedniej dokumentacji dotyczącej bezpieczeństwa i integralności sieci. Musi ona obejmować opis wszystkich przedsięwzięć podjętych w celu realizacji pozostałych środków.

Punkt 2 wskazuje, że niezbędnym jest posiadanie wykazu infrastruktury telekomunikacyjnej i oprogramowania służących do świadczenia usług telekomunikacyjnych, obejmujący ich rodzaj i konfigurację. Posiadanie wykazu jest punktem wyjścia do oceny, czy sieć jest podatna oraz czy wykorzystywany w niej sprzęt spełnia wymogi bezpieczeństwa.

---

[4] ENISA, Technical Guideline on Minimum Security Measures, https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures, dostęp z dnia 17.09.2019.

[5] Dz. Urz. UE L 337, 18.12.2009, str. 37.

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona), (Dz. Urz. UE L 321 z 17.12.2018, str. 36)

Punkty 3-6 to opisowo określone przedsięwzięcia prowadzące do zarządzania ryzykiem w organizacji. Przedsiębiorca powinien identyfikować zagrożenia (przy czym za punkt wyjścia identyfikacji powinny służyć dokumenty ENISA w tym zakresie, np. ENISA Threat Landscape[7] – wydawane corocznie), oceniać prawdopodobieństwo oddziaływania tych zagrożeń na bezpieczeństwo oraz zapewniać i stosować środki minimalizujące skutki oddziaływania tych zagrożeń.

Punkty 7-10 regulują środki związane z dostępem do zasobów. Zgodnie z pkt 7, przedsiębiorca powinien ustanowić zasady i procedury dostępu do kluczowych zasobów, wraz z przypisaniem odpowiedzialności. Dostęp i odpowiedzialności powinny być zgodne z zakresem realizowanych zadań. Nie chodzi tu wyłączenie o dostęp fizyczny, a przede wszystkim o uprawnienia w rozumieniu systemów IT (privilege and access control). Punkt 8 uzupełnia powyższe, wskazując konieczność zabezpieczania dostępu do zasobów i monitorowanie tego dostępu, punkt 9 nakazuje ustanowić zasady dotyczące przetwarzania danych, a punkt 10 – zabezpieczyć te dane.

Punkt 11 wskazuje konieczność uwzględniania też tzw. bezpieczeństwa prawnego, rozszerzając obowiązek identyfikacji zagrożeń także w tym obszarze.

Punkt 12 dotyczy monitorowania i dokumentowania funkcjonowania sieci (element tzw. bezpieczeństwa operacyjnego), natomiast punkt 13 uzupełnia obowiązek ustawowy z art. 175a PT, dotyczący zgłaszania naruszeń. Kluczowe jest w tym wypadku posiadanie procedury regulującej zgłaszanie incydentów w organizacji.

Punkt 14 zawiera wytyczne dotyczące okresowej oceny bezpieczeństwa. Musi ona nastąpić:

1) raz na rok lub

2) po każdym naruszeniu bezpieczeństwa lub integralności sieci lub

3) po każdym wykryciu podatności.

Okresowe, coroczne sprawdzanie systemów wydaje się standardową, zalecaną praktyką. Nie musi to koniecznie być pełen audyt; nie jest też sugerowane, aby była to ocena zlecana na zewnątrz – może to zostać dokonane własnymi środkami przedsiębiorcy.

---

[7] Za ostatni rok: ENISA, ENISA Threat Landscape Report 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, dostęp z dnia 15.01.2020.

Konieczne jest sprawdzenie bezpieczeństwa po każdym istotnym incydencie oraz po pojawieniu się istotnej podatności – o ile logiczne jest, że nie należy wtedy sprawdzać całej sieci, to niezbędne jest zbadanie powiązań i ocena, czy konkretny incydent nie wpłynął na resztę infrastruktury i usług.

Oparcie regulacji prawnych na wytycznych ENISA jest z powodzeniem stosowane przez m. in. Grecję, która włączyła propozycje ENISA do swojego porządku prawnego jako część regulacji (wydanej przez właściwy organ ds. bezpieczeństwa komunikacji i prywatności)[8], Rumunię (regulacja włączająca propozycje ENISA została wydana przez organ właściwy ds. telekomunikacji – ANCOM)[9], Słowację (regulacja włączająca propozycje ENISA została wydana przez Urząd Regulacji Łączności Elektronicznej i Usług Pocztowych)[10], Holandię (regulacje wydane przez organ właściwy ds. telekomunikacji - Agentschap Telecom)[11].

Wskazać ponadto należy, że obecnie trwa wdrażanie pilotażowych instalacji 5G. Sieci najnowszej generacji w modelu non standalone będą współpracowały ze starszymi sieciami i innymi technologiami, jednak w docelowym modelu standalone nie będą wymagały tego wsparcia, co zwiększy ich wydajność i szybkość. Oznacza to, że już teraz należy przygotować odrębne środki bezpieczeństwa i integralności sieci 5G. Nie powoduje to różnego traktowania przedsiębiorców telekomunikacyjnych – wymogi są wyodrębnione ze względu na stosowaną technologię, a nie cechy identyfikujące przedsiębiorcę.

Główną cechą wyróżniającą sieć 5G w warstwie dostępowej jest tzw. New Radio czyli interfejs radiowy pozwalający na obsługiwanie danych w nowym podejściu (wysoki przepływ danych, niskie opóźnienia, połączenia wielu urządzeń końcowych), modeli komunikacji (ruch IP, ruch poza IP, short data bursts etc.) i różnych protokołów sesji (IPv4, IPv6, IPv4v6 etc.).

[8] Regulacja przez organ właściwy ds. bezpieczeństwa komunikacji i prywatności: http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013.pdf – za raportem ENISA dotyczącym implementacji art. 13a Dyrektywy 2009/140/WE: https://resilience.enisa.europa.eu/article-13/state-of-play-2015-public-report, dostęp z dnia 17.09.2019 r.

[9] Decyzja organu właściwego ds. telekomunikacji ANCOM - http://www.ancom.ro/en/uploads/forms_files/decizie_2013_512_en1381320558.pdf, dostęp z dnia 17.09.2019 r.

[10] Regulacja wydana przez Urząd Regulacji Łączności Elektronicznej i Usług Pocztowych https://www.teleoff.gov.sk/data/files/27461.pdf, dostęp z dnia 17.09.2019 r.

[11] Minimalne wymagania dla zachowania ciągłości działania: https://www.agentschaptelecom.nl/documenten/brochures/2016/november/1/minimale-eisen-continuiteitsplan-telecomaanbieders, dostęp z dnia 17.09.2019 r.

Minimalne wymagania dla planów bezpieczeństwa: https://www.agentschaptelecom.nl/documenten/brochures/2017/december/4/eisen-beveiligingsplan-telecomaanbieders, dostęp z dnia 17.09.2019 r.

Równie istotnymi cechami wyróżniającymi sieci 5G są, w warstwie szkieletowej, możliwość dzielenia sieci na warstwy (Network Slicing), możliwość świadczenia usług w punkcie dostępowym sieci (Mobile Edge Computing) oraz ułatwienie tworzenia nowych usług (Network Capability Exposure oraz Flexible Mobile Service Steering).

Wszystkie powyższe cechy powodują, że konieczne jest rozróżnienie środków technicznych w zależności od stosowanej technologii.

W Polsce nie ma zwyczaju definiowania generacji sieci komórkowych, stąd konieczne jest odwołanie się do specyfikacji – raportu technicznego ETSI TR 121 915 V.15.0.0. (2019-10), który zawiera niezbędne informacje dotyczące wstępnej fazy wdrażania sieci 5G. Rozporządzenie precyzuje zobowiązania z art. 175 ustawy – Prawo telekomunikacyjne poprzez wskazanie, że konieczne jest, aby przedsiębiorca telekomunikacyjny dostarczający sieci 5G , w zakresie bezpieczeństwa i integralności sieci i usług:

- identyfikował zagrożenia,

- oceniał prawdopodobieństwo oddziaływania tych zagrożeń,

- zapewniał środki minimalizujące skutki wystąpienia oddziaływania tych zagrożeń,

- stosujował środki minimalizujące skutki wystąpienia oddziaływania zagrożeń.

Są to elementy zarządzania ryzykiem w organizacji i są one niezbędne do poprawnego zabezpieczenia sieci i usług.

Dokonując zarządzania ryzykiem, przedsiębiorca powinien brać pod uwagę w swojej działalności:

1) treść rekomendacji, o których mowa w art. 33 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).

Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotyczą stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Nie oznaczają one automatycznie konieczności pozbycia się sprzętu z sieci – wskazują jedynie na możliwe zagrożenia wynikające ze stosowania określonych urządzeń. Rekomendacje mogą mieć również charakter pozytywny (wskazywać zalecany sprzęt) oraz wskazywać określony sposób korzystania (np. rodzaje systemów, w których zaleca się korzystać z określonego sprzętu lub oprogramowania).

2) unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług oraz wykorzystaniu najnowocześniejszych osiągnięć technicznych;

Konieczne jest rozważenie dywersyfikacji elementów sieci telekomunikacyjnej. Oczywistym jest, że w niektórych przypadkach będzie to niemożliwe bądź bardzo utrudnione – stąd wskazuje się na dążenie do unikania uzależnienia, a nie wskazuje się w procentowy sposób, ile urządzeń powinno być od różnych producentów.

3) podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych

Zamiast wskazywania konieczności redundancji poszczególnych elementów sieci, projekt rozporządzenia wskazuje na konieczność podwyższania odporności (resilience) sieci i usług. Projektodawca nie wskazuje w tym miejscu szczegółowych metod, gdyż można to osiągnąć na różne sposoby – np. redundancję sprzętu czy zapewnienie roamingu krajowego.

Przedsiębiorca telekomunikacyjny jest zobowiązany do prowadzenia dokumentacji ww. działań.

Podkreślić należy, że wprowadzenie redundantnej konfiguracji sieci nie naruszy reguł konkurencji. Legalność tego rozwiązania opiera się na art. 8 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, z późn. zm.), zwanej dalej „uokik”. Na podstawie tego przepisu przedsiębiorcy zawierają między sobą porozumienie. Warte zaznaczenia jest to, że treść art. 8 ust. 1 uokik jest analogiczna do treści art. 101 ust. 3 TFUE. Znalazło to potwierdzenie w wyroku SOKIKu z 2016 r.[12] Oznacza to, że indywidualne wyłączenie porozumienia spod zakazu ograniczenia konkurencji, będzie legalne zarówno z punktu widzenia polskiego jak i europejskiego prawa. Przedsiębiorcy zawierający porozumienie muszą spełnić jednocześnie cztery przesłanki z art. 8 ust. 1 uokik, to znaczy jednocześnie:

1) przyczyniają się do polepszenia produkcji, dystrybucji towarów lub do postępu technicznego lub gospodarczego;
2) zapewniają nabywcy lub użytkownikowi odpowiednią część wynikających z porozumień korzyści;

[12] Wyrok Sądu Okręgowego - Sądu Ochrony Konkurencji i Konsumentów z dnia 29 września 2016 r., sygn. akt: XVII AmA 100/11.

3) nie nakładają na zainteresowanych przedsiębiorców ograniczeń, które nie są niezbędne do osiągnięcia tych celów;
4) nie stwarzają tym przedsiębiorcom możliwości wyeliminowania konkurencji na rynku właściwym w zakresie znacznej części określonych towarów.

Trybunał Sprawiedliwości w ocenie pierwszej przesłanki z art. 101 ust. 3 TFUE[13] w pkt. 43 wyroku uznał że czynnik stabilizujący zatrudnienie wchodzi w zakres celów z art. 101 ust. 3 TFUE. W innych sprawach uwzględniono między innymi kwestie związane z solidarnością finansową, czy ochroną środowiska. Mając na uwadze powyższe, zgodnie z art. 175 ust. 1 PT przedsiębiorcy zawierający porozumienie, spełnią pierwszą przesłankę z art. 101 ust. 3 TFUE, a także art. 8 ust. 1 uokik przez zapewnienie większego poziomu bezpieczeństwa i zachowania integralności sieci, która wynikać będzie z zastosowania redundantnej konfiguracji.

Spełnienie drugiej przesłanki wynika bezpośrednio z pierwszej. Korzyści uzyskane przez użytkowników lub nabywców, zgodnie z jedną zasad z prawa antymonopolowego, tzw. regułą rozsądku, przeważają nad negatywnymi skutkami ograniczenia konkurencji. Sąd Apelacyjny w wyroku z 2016 r.[14] stwierdził, że chodzi tu o korzyści natury gospodarczej i społecznej, jak. np. wzrost produkcji, postęp techniczny, obniżki cen, utrzymanie poziomu zatrudnienia. Większe bezpieczeństwo sieci związane z istnieniem alternatywnej dostawy usługi, np. w wyniku awarii lub ataku na jednego dostawcę, pozwala zachować ciągłość działania usługi i ograniczyć negatywne skutki ekonomiczne i społeczne wynikające z braku ww. usługi, co ostatecznie niewątpliwie stanowi realizację przesłanki z art. 8 ust. 1. pkt 2 uokik.

Przesłanka trzecia odnosi się wprost do unijnej zasady proporcjonalności. Tym samym redundantna konfiguracja sieci objęta porozumieniem jest niezbędna, odpowiednia, i proporcjonalna sensu stricto. Proporcjonalność z art. 8 ust. 1 pkt 3 uokik jest osiągnięta, gdy spełnione zostają przesłanki z pkt. 1 oraz 2. Spełnienie powyższych przesłanek zostało udowodnione w poprzednich akapitach, w związku z tym spełniona zostaje także przesłanka z pkt 3.

Czwarta przesłanka zakłada, że dane porozumienie nie może dawać przedsiębiorstwom możliwości eliminowania konkurencji w stosunku do znacznej części danych

---

[13] Wyrok Trybunału Sprawiedliwości z dnia 25 października 1977 r., w sprawie nr: 26/76, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61976CJ0026&qid=1567676311457&from=PL

[14] Wyrok Sądu Apelacyjnego w Warszawie - V Wydział Cywilny z dnia 8 stycznia 2016 r., sygn. akt: VI ACa 1872/14.

produktów. Ograniczenie konkurencji wynikające z porozumienia odnośnie redundantnej konfiguracji sieci, dotyczyć będzie wąskiej kategorii produktów i nie wpłynie negatywnie na konkurencję przedsiębiorców na wszystkich pozostałych polach działalności. W związku z tym zostanie spełniona przesłanka z pkt 4.

Tym samym zawarcie przez przedsiębiorców porozumienia dotyczącego wprowadzenia redundantnej konfiguracji sieci na podstawie art. 8 ust. 1 uokik, przy spełnieniu powyższych warunków, będzie legalne.

Należy wskazać, że redundancja z powodzeniem jest stosowana m.in. w Finlandii[15], gdzie operatorzy telekomunikacyjni muszą zapewnić odporność swoich sieci lub usług, tak aby awaria któregokolwiek z komponentów nie zakłócała działania sieci lub usług albo nie miała znaczącego wpływu na ich działanie. W Finlandii komponenty sieci muszą być zabezpieczone w ten sposób, aby było możliwe automatyczne przejście z użytkowanego komponentu na komponent redundantny. Celem tego rozwiązania jest, by awaria komponentu nie zakłóciła działania usług lub sieci. W związku z tym, operator zapewnia dostępność odpowiedniego personelu, sprzętu i zasobów łącza transmisyjnego z wyprzedzeniem.

Rozporządzenie wejdzie w życie po upływie 6 miesięcy od daty ogłoszenia, co pozwoli dostosować się przedsiębiorcom do wdrożenia poszczególnych środków.

Zawarte w projekcie regulacje nie stanowią przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.), dlatego też projekt rozporządzenia nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawiania organom i instytucjom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt zostanie udostępniony w Biuletynie Informacji Publicznej. Ponadto zgodnie z § 52 ust. 1 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn.

---

[15] FICORIA, Regulation on resilience of communications networks and services and of synchronisation of communications networks, 17.12.2014, 54 B/2014 M (Regulation 54 on resilience of communications networks and services https://www.finlex.fi/data/normit/42160/Viestintavirasto54B2014M_EN.pdf, dostęp z dnia 17.09.2019 r.

zm.), projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Zawarte w projekcie regulacje będą miały wpływ na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2018 r. poz. 646, z późn. zm.).

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Marek Zagórski,** Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Jakub Dysarz, Naczelnik Wydziału, Departament Cyberbezpieczeństwa, jakub.dysarz@mc.gov.pl, tel. 22 245 58 38	**Data sporządzenia** 24.01.2020 **Źródło:** Upoważnienie ustawowe Art. 175d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460) **Nr w wykazie prac legislacyjnych Ministra Cyfryzacji:** 147

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Artykuł 175 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne nakłada na przedsiębiorców telekomunikacyjnych obowiązek zapewnienia bezpieczeństwa i integralności sieci, usług i przekazu komunikatów za pomocą odpowiednich środków technicznych i organizacyjnych. Minister właściwy do spraw informatyzacji może w drodze rozporządzenia określić minimalne środki techniczne i organizacyjne (art. 175d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne).

Rozporządzenie nie zostało dotychczas wydane, jednakże pojawienie się w telekomunikacji nowych technologii wrażliwych na naruszenia oraz incydenty wskazuje na potrzebę wskazania minimalnych środków technicznych i organizacyjnych zapewniającą bezpieczeństwo sieci, świadczonych usług oraz przetwarzania danych.

Zarówno w interesie obywateli, jak i Państwa jest, aby przedsiębiorcy telekomunikacyjni mieli obowiązek stosowania konkretnych rozwiązań w celu zapewnienia bezpieczeństwa sieci i usług telekomunikacyjnych. Wraz z rozwojem technologii zwiększa się także liczba zagrożeń, które mogą wpłynąć na bezpieczeństwo i integralność sieci i usług telekomunikacyjnych, utrudniać życie obywatelom oraz niekorzystnie wpływać na sprawne funkcjonowanie Państwa.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projekt rozporządzenia zawiera szereg środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, które, jeśli zostaną poprawnie wdrożone, wpłyną pozytywnie na poziom bezpieczeństwa i integralności sieci i usług telekomunikacyjnych.

Poza ww. środkami, projekt zawiera odrębne wymogi dotyczące bezpieczeństwa sieci 5G. Wymogi są wyodrębnione ze względu na stosowaną technologię, a nie cechy identyfikujące przedsiębiorcę.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Oparcie regulacji prawnych na wytycznych ENISA jest z powodzeniem stosowane przez m. in. Grecję, która włączyła propozycje ENISA do swojego porządku prawnego jako część regulacji (wydanej przez właściwy organ ds. bezpieczeństwa komunikacji i prywatności)[16], Rumunię (regulacja włączająca

[16] Regulacja przez organ właściwy ds. bezpieczeństwa komunikacji i prywatności: http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013.pdf – za raportem ENISA dotyczącym implementacji art. 13a Dyrektywy 2009/140/WE: https://resilience.enisa.europa.eu/article-13/state-of-play-2015-public-report, dostęp z dnia 17.09.2019 r.

propozycje ENISA została wydana przez organ właściwy ds. telekomunikacji – ANCOM)[17], Słowację (regulacja włączająca propozycje ENISA została wydana przez Urząd Regulacji Łączności Elektronicznej i Usług Pocztowych)[18], Holandię (regulacje wydane przez organ właściwy ds. telekomunikacji - Agentschap Telecom)[19].

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Przedsiębiorcy telekomunikacyjni	5360	Rejestr UKE	Realizacja wskazanych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom
Podmioty zainteresowane świadczeniem usług w zakresie sieci 5G	Nieznana	Nie dotyczy	Realizacja wskazanych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W Ministerstwie Cyfryzacji odbyły się dwie tury warsztatów z udziałem wybranych operatorów telekomunikacyjnych. Warsztaty dotyczyły wymogów bezpieczeństwa i integralności sieci 5G. Projekt był także prekonsultowany z Urzędem Komunikacji Elektronicznej w zakresie adekwatności proponowanych wymogów bezpieczeństwa.
Projekt rozporządzenia zostanie poddany uzgodnieniom międzyresortowym, opiniowaniu oraz konsultacjom publicznym.
Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt zostanie udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej MC oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki	0	0	0	0	0	0	0	0	0	0	0	0

[17] Decyzja organu właściwego ds. telekomunikacji ANCOM - http://www.ancom.ro/en/uploads/forms_files/decizie_2013_512_en1381320558.pdf, dostęp z dnia 17.09.2019 r.
[18] Regulacja wydana przez Urząd Regulacji Łączności Elektronicznej i Usług Pocztowych https://www.teleoff.gov.sk/data/files/27461.pdf, dostęp z dnia 17.09.2019 r.
[19] Minimalne wymagania dla zachowania ciągłości działania: https://www.agentschaptelecom.nl/documenten/brochures/2016/november/1/minimale-eisen-continuiteitsplan-telecomaanbieders, dostęp z dnia 17.09.2019 r. Minimalne wymagania dla planów bezpieczeństwa: https://www.agentschaptelecom.nl/documenten/brochures/2017/december/4/eisen-beveiligingsplan-telecomaanbieders, dostęp z dnia 17.09.2019 r.

(oddzielnie)												
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Nie dotyczy.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt rozporządzenia nie ma wpływu na wydatki sektora finansów publicznych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
	(dodaj/usuń)	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Konieczność zastosowania środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom wskazanych w projekcie może wymusić zmiany w organizacji oraz aktualizację istniejących rozwiązań technicznych.						
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe	Nie dotyczy.						
Niemierzalne	(dodaj/usuń)	Nie dotyczy						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, a także osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.						

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Komentarz: Projekt wskazuje prowadzenie dokumentacji, jako środek organizacyjny służący zapewnieniu bezpieczeństwa lub integralności sieci. Należy jednak wskazać, że istnienie niezbędnej dokumentacji w zakresie wykazu aktywów czy też procedur dotyczących zgłaszania naruszeń określonych zgodnie z art. 175a ustawy – Prawo telekomunikacyjne jest dobrą praktyką i bez niej trudno jest realizować zobowiązania ustawowe.	

9. Wpływ na rynek pracy

Nie dotyczy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Rozporządzenie wpłynie pozytywnie na poziom bezpieczeństwa telekomunikacji i informatyzacji, docelowo zmniejszając liczbę naruszeń bezpieczeństwa.	

11. Planowane wykonanie przepisów aktu prawnego

Przepisy wejdą w życie w terminie sześciu miesięcy od dnia ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Po dwóch latach obowiązywania przepisów Ministerstwo Cyfryzacji dokona analizy raportu dotyczącego liczby naruszeń i zawnioskuje do UKE o informację na temat kontroli przedsiębiorców telekomunikacyjnych w zakresie stosowania rozporządzenia.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak załączników.