KANCELARIA PREZESA RADY MINISTRÓW

DEPARTAMENT CYBERBEZPIECZEŃSTWA
Robert Kośla
DYREKTOR

Warszawa, dnia r.

DC.WSiC.700.1.1.2021(7)

Pan
Adam Abramowicz
Rzecznik Małych i Średnich
Przedsiębiorców
biuro@rzecznikmsp.gov.pl

Szanowny Panie Rzeczniku,

nawiązując do pisma z 26 września 2020 r. (WPL.631.2020.GG) w sprawie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa poniżej przedstawiam wyjaśnienia do zgłoszonych przez Państwa uwag.

1. W pierwszej kolejności chciałbym wyjaśnić, że przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o krajowym systemie cyberbezpieczeństwa poprzez ustawę wprowadzającą Prawo Komunikacji Elektronicznej. Ta ustawa będzie wdrażać art. 40 i 41 Europejskiego Kodeksu Łączności Elektronicznej. Zgodnie z art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty telekomunikacyjne do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.
2. Podkreślić należy, że przedsiębiorcy komunikacji elektronicznej będą wdrażać środki techniczne i organizacyjne adekwatne do oszacowanego ryzyka. Oczywistym jest fakt, że dużego przedsiębiorcę komunikacji elektronicznej będą dotyczyły innego rodzaju ryzyka niż małego przedsiębiorcę komunikacji elektronicznej. Dlatego też przepisy te zakładają wdrożenie środków proporcjonalnych do zagrożeń, z którymi może zmagać się przedsiębiorca komunikacji elektronicznej.
3. Do obowiązków każdego przedsiębiorcy komunikacji elektronicznej będzie należeć obsługa incydentu telekomunikacyjnego. Jest to konieczne, a także korzystne dla przedsiębiorcy, ponieważ jeżeli nie obsłuży incydentu telekomunikacyjnego, to poprzez takim brak działania przedsiębiorca może zagrozić funkcjonowaniu usługi komunikacji elektronicznej, na którą wpływa incydent telekomunikacyjny. Spowoduje to straty finansowe, a także utratę zaufania do przedsiębiorcy wśród jego klientów.
4. Obowiązek zgłaszania incydentów telekomunikacyjnych do zespołów CSIRT NASK, CSIRT GOV, CSIRT MON będzie dotyczył tych incydentów telekomunikacyjnych, które będą przekraczać progi ustalone w rozporządzeniu. Progi tych incydentów zostaną określone w rozporządzeniu ministra właściwego do spraw informatyzacji.
5. Przepisy dotyczące obowiązku sporządzania i posiadania planu działań w sytuacji szczególnego zagrożenia będą zawarte w Prawie Komunikacji Elektronicznej.
6. Ocena skutków regulacji została uzupełniona o ocenę wpływu projektowanych przepisów na małych i średnich przedsiębiorców. W szczególności wskazano, że:

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

a. Zmiany w ustawie w szczególności będą dotyczyć tych małych i średnich przedsiębiorców, którzy są operatorami usług kluczowych lub dostawcami usług cyfrowych:

   1) Operatorzy usług kluczowych będą musieli wypracować procedury kontaktu z sektorowymi zespołami CSIRT.

   2) Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się podmiotami prowadzącymi SOC na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji, SOC będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Oznaczać to będzie, że wprowadzone środki techniczne i organizacyjne będą mogły różnić się od dotychczas wprowadzonych, ponieważ to SOC będzie o nich decydował.

   3) Podmioty krajowego systemu cyberbezpieczeństwa (w tym operatorzy usług kluczowych i dostawcy usług cyfrowych) będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa.

b. Mali i średni przedsiębiorcy będą musieli wycofać dany sprzęt lub oprogramowanie dostawcy wysokiego ryzyka z użycia w ciągu 7 lat, jeżeli będą należeć do którejś z poniższych kategorii:
   1) Podmioty krajowego systemu cyberbezpieczeństwa
   2) przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia,
   3) operatorzy infrastruktury krytycznej,
   4) przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym

c. Obowiązek wycofania produktów, usług i procesów dostawcy wysokiego ryzyka nie będzie dotyczył mikro-, małych i średnich przedsiębiorców telekomunikacyjnych, ponieważ będzie on dotyczył wyłącznie przedsiębiorców telekomunikacyjnych sporządzających plany działań w sytuacji szczególnego zagrożenia, których w tej chwili jest około 100. Są to najwięksi przedsiębiorcy telekomunikacyjni w Polsce.

d. Ponadto, w wyniku wydania decyzji administracyjnej ws. polecenia administracyjnego, podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni (wszyscy), operatorzy infrastruktury krytycznej, przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym, dostawcy usług zaufania, których będzie dotyczyła ta decyzja m.in. zakazującej

korzystania z określonego oprogramowania, które zostało wskazane, jako stanowiące zagrożenie dla wystąpienia incydentu krytycznego. Jeżeli mali i średni przedsiębiorcy będą należeć do którejś z wymienionych grup, to będą musieli się zastosować do polecenia zabezpieczającego, jeżeli wobec nich zostało takie wydane.

Obecnie projekt ustawy został skierowany do Komitetu Rady Ministrów do Spraw Cyfryzacji, a także do Komitetu do Spraw Europejskich.

Informacje o dalszych pracach nad projektem będą publikowane na stronie Rządowego Procesu Legislacyjnego.

Odniesienie do załączonego pisma Związku Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM z 16 września 2020 r. zawarte zostało w tabeli załączonej do niniejszego pisma.

Z poważaniem

Robert Kośla

/podpisano kwalifikowanym podpisem elektronicznym/

	Stanowisko ZPMEiT Mediakom	Wyjaśnienie DC KPRM
1.	1. W pierwszej kolejności podnoszę, że niejasny jest stosunek projektowanych przepisów do zapisów projektu Prawa Komunikacji Elektronicznej (dalej PKE). Oba akty regulują tę samą materię, a część projektowanych przepisów jest tożsama: - art. 39 PKE i art. 20a ustawy o krajowym systemie cyberbezpieczeństwa, - i art.43 ust. 2 i 3 PKE i art. 20e ustawy o krajowym systemie cyberbezpieczeństwa - art. 44 ust. 1 PKE i art. 20f ustawy o krajowym systemie cyberbezpieczeństwa Nadto ustawa o krajowym systemie cyberbezpieczeństwa, równolegle do PKE reguluje obowiązek zgłaszania incydentów bezpieczeństwa, przy czym różny jest krąg podmiotów zobowiązanych i organ właściwy do przyjmowania zgłoszeń: - PKE nakłada obowiązek na wszystkich przedsiębiorców telekomunikacyjnych i nakazuje zgłaszać incydenty do UKE (art. 42), zaś - ustawa o krajowym systemie bezpieczeństwa nakłada obowiązki jedynie na tych przedsiębiorców, którzy mają obowiązek sporządzania planów działania w sytuacjach szczególnych zagrożeń i nakazuje zgłaszać incydenty do właściwego CSIRT (art. 20c). Biorąc pod uwagę powyższe, oraz treść otrzymanego z Ministerstwa Cyfryzacji pisma zawiadamiającego o konsultacjach, z którego wynika, że PKE ma zostać uzupełnione o przepisy regulujące obowiązki przedsiębiorców w zakresie zapewnienia bezpieczeństwa ciągłości świadczenia usług komunikacji elektronicznej oraz dostarczania sieci telekomunikacyjnej poprzez włączenie obowiązków zawartych w konsultowanym projekcie do	1. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o krajowym systemie cyberbezpieczeństwa poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Przedsiębiorcy komunikacji elektronicznej będą zgłaszać te incydenty telekomunikacyjne, które będą spełniać progi określone w rozporządzeniu.

	PKE, nie jest do końca jasne przyjęty sposób regulacji. Czy konsultowane przepisy mają znaleźć się w dwóch równoległych ustawach? Czy też mają one być wprowadzone do PKE i usunięte z konsultowanej ustawy? Mediakom postuluje, by kwestie bezpieczeństwa sieci i usług uregulowane zostały w jednym akcie prawnym, tak by maksymalnie uprościć przyjęte rozwiązania i zapewnić czytelność i możliwą łatwość stosowania przez przedsiębiorców komunikacji elektronicznej. Zbędne jest też powielanie tożsamych przepisów w dwóch niezależnych ustawach. Ponadto, wobec wyżej wskazanych rozbieżności pomiędzy projektowanymi art. 42 PKE i art. 20c ustawy o krajowym systemie cyberbezpieczeństwa Mediakom postuluje, by pozostać przy rozwiązaniu przyjętym w art. 20c - tak, by obowiązek zgłaszania incydentów obciążał wyłącznie tych przedsiębiorców telekomunikacyjnych, którzy są zobowiązani do sporządzania planów działania w sytuacjach szczególnych zagrożeń. Są to podmioty duże, osiągające ponad 10 mln przychodów, często posiadające rozbudowane sieci i dużą liczbę abonentów. To właśnie incydenty bezpieczeństwa dotykające tych podmiotów, z uwagi na skalę ich działalności, winny być raportowane. Natomiast mniejsi przedsiębiorcy, działający na mniejszą skalę, o znacznie mniejszym zasięgu sieci i liczbie abonentów nie powinni być objęci obowiązkiem raportowania incydentów bezpieczeństwa.	
2.	2. W związku z projektowaną treścią art. 4 ustawy o krajowym systemie cyberbezpieczeństwa, poprzez dodanie do niego pkt 2a i tym samym włączenie do krajowego systemu cyberbezpieczeństwa wszystkich przedsiębiorców komunikacji elektronicznej Mediakom postuluje, by ograniczyć grono	W sytuacji, gdy tak duża liczba różnych usług kluczowych dla bezpieczeństwa państwa i obywateli jest zależna od niezakłóconego świadczenia usług komunikacji elektronicznej niezbędne jest włączenie wszystkich przedsiębiorców komunikacji elektronicznej do jednolitego systemu cyberbezpieczeństwa.

	przedsiębiorców komunikacji elektronicznej będących częścią systemu cyberbezpieczeństwa do tych tylko, którzy zobowiązani są sporządzać plany działań w sytuacjach szczególnych zagrożeń, o którym mowa w art. 47 ust. 1 PKE. Jak wskazano powyżej - plany mają obowiązek sporządzać przedsiębiorcy o dużej skali działalności, świadczący własne usługi, z wykorzystaniem własnej sieci i osiągający przychody przekraczające 10 mln złotych. Mają oni realne znaczenie dla krajowego systemu cyberbezpieczeństwa, zaś incydenty bezpieczeństwa, które mogą ich dotknąć z zasady będą miały istotne znaczenie z uwagi na ilość abonentów i obszar, który incydent może dotknąć. Inaczej jest w przypadku mniejszych przedsiębiorców, których liczba jest bardzo znacząca, a jednocześnie znaczenie z uwagi na ilość obsługiwanych abonentów i obszar działania - niewielkie. Przedsiębiorcy ci nie mają realnego znaczenia dla krajowego systemu cyberbezpieczeństwa. Jak pokazała praktyka przedsiębiorcy osiągający przychody do 10 mln złotych nie mieli istotnego znaczenia z punktu widzenia lokalnych podmiotów odpowiedzialnych za zarządzanie kryzysowe - stąd zwolnienie ich z obowiązku tworzenia i uzgadniania z właściwymi podmiotami planów działania, o których mowa w art. 47 ust. 1 PKE. Jednocześnie wielość przedsiębiorców prowadzących działalność na mniejszą skalę jest tak duża - sięgająca aż 6.000 podmiotów, że sama obsługa zgłoszeń incydentów bezpieczeństwa będzie wymagała ogromnej pracy logistycznej. Wobec tego Mediakom proponuje, by dodawany do art. 4 pkt 2a projektowanej ustawy otrzymał brzmienie: „ 2 a) przedsiębiorców komunikacji elektronicznej sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy Prawo komunikacji elektronicznej"	Należy podkreślić, że zgodnie z art. 40 ust. 2 EKŁE wszyscy przedsiębiorcy komunikacji elektronicznej mają informować o *incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług.* Na gruncie krajowym nie jest możliwe zawężenie tego obowiązku wyłącznie do przedsiębiorców komunikacji elektronicznej sporządzających plany działań w sytuacji szczególnego zagrożenia. Podkreślić należy, że zgłaszane będą incydent telekomunikacyjne, które będą przekraczać progi ustalone w rozporządzeniu ministra właściwego do spraw informatyzacji.

3.	3. Odnosząc się do planowanej zmiany polegającej na dodaniu przepisów art. 66a, 66b i 66c Mediakom wskazuje, że nie popiera proponowanych zmian w zakresie w jakim uprawniają one do wydawania wiążących rozstrzygnięć skutkujących powstaniem zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług danego dostawcy oraz obowiązku wycofania ich z obrotu. Mediakom rozumie potrzebę kontroli bezpieczeństwa i jakości sprzętu, oprogramowania i usług dostawców, jednak w jego ocenie proponowana procedura może prowadzić de facto do wykluczenia z rynku dowolnych dostawców i będzie wiązać się z poważnymi kosztami dla przedsiębiorców komunikacji elektronicznej, którzy będą zmuszeni do wymiany być może znacznej części wykorzystywanych urządzeń. Jednocześnie okres wymiany tych urządzeń (5 lat od ogłoszenia komunikatu o ocenie) nie pokrywa się z okresem amortyzacji urządzeń, co dodatkowo wpływa na zwiększenie kosztów nowych urządzeń. Jeśli więc możliwość wydawania wiążących ocen miałaby pozostać, to należy postulować wydłużenie okresu czasu na wymianę urządzeń do 7-8 lat.	Przepisy art. 66a-66c zostały zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa zostanie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca, wobec którego będzie prowadzone postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. P Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność

		ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Ponadto zmieniony został termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych został dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.