OPINIA

Polskiej Izby Informatyki I Telekomunikacji [PIIT]

w sprawie planów działań przedsiębiorcy telekomunikacyjnego

w sytuacjach szczególnych zagrożeń

W odpowiedzi na pismo z dnia 24 września br. dot. prośby o opinię wz. założeń dla rozporządzenia, które **nie później niż do 28 sierpnia 2020 r.** miałoby zastąpić aktualne rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. **w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń**, wydane na podstawie art. 176a ustawy – Prawo telekomunikacyjne, przedstawiam wstępną opinię Polskiej Izby Informatyki i Telekomunikacji (PIIT).

Z formalnego punktu widzenia, konieczność zmiany rozporządzenia wynika przede wszystkim z pośredniej zmiany upoważnienia do wydania aktu wykonawczego z art. 176a ust. 5, tj. zmiany art. 176a ust. 2 pkt 4 oraz art. 92 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa (KSC), który przesądził o utracie mocy obowiązującej aktualnego rozporządzenia, w okresie 24 miesięcy od wejścia w życie tej ustawy. Zmiana ta polegała na zastąpieniu zwrotu *„zabezpieczenia infrastruktury telekomunikacyjnej w sytuacjach szczególnych zagrożeń oraz przed nieuprawnionym dostępem”* sformułowaniem *„technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”.* Zmiana polega, więc na wprowadzeniu nowego zakresu planów działań, o których mowa w art. 176a ust. 2, tj. konieczności uwzględnienia możliwości wystąpienia zdarzeń o charakterze incydentów cyberbezpieczeństwa. Takimi incydentami, zgodnie z brzmieniem definicji zawartych w art. 2 pkt 4 i 5 ustawy KSC, a więc zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwa, rozumianego, jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Biorąc pod uwagę fakt, że co do zasady przedsiębiorcy telekomunikacyjni zostali wyłączeni spod zakresu stosowania ustawy KSC w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, **ewentualna zmiana rozporządzenia w ww. zakresie nie powinna prowadzić do zbytniego rozszerzenia obowiązków przedsiębiorców telekomunikacyjnych w zakresie incydentów cyberbezpieczeństwa, a ograniczać się do określenia przez sporządzającego plan przedsiębiorcę środków odpowiednich dla dokonanej oceny aktualnej sytuacji faktycznej**. Natomiast w przypadku przedsiębiorców telekomunikacyjnych będących jednocześnie operatorami usług kluczowych, sygnalizujemy, że są oni zobowiązani są do sporządzania odrębnej dokumentacji na potrzeby wymogów ustawy KSC, a także obsługi incydentów. Tym samym nie powinni w tym zakresie podlegać dodatkowej, szczegółowej regulacji w zakresie planów działania w sytuacji szczególnych zagrożeń.

W zakresie **planów ochrony infrastruktury krytycznej oraz planów działania w sytuacjach szczególnych zagrożeń, trudno w aktualnym stanie prawnym i faktycznym odnieść się do korelacji** między nimi. Wynika to z faktu, że dokumenty te pozostają odrębnymi obowiązkami, są raportowane do innych podmiotów, a zakres w nich ujęty nie jest spójny. Tym samym **na obecnym etapie odnosimy się do stanu zakładającego istnienie odrębnych obowiązków w zakresie obu typów planów**. Niemniej jednak w przypadku ewentualnej decyzji i przedstawienia propozycji w zakresie ograniczenia obowiązków informacyjnych przedsiębiorców telekomunikacyjnych, deklarujemy zainteresowanie udziałem w takiej dyskusji i próbie przygotowania nowego podejścia do realizacji tych obowiązków.

W zakresie **dodatkowych zmian rozporządzenia, które mogą usprawnić opracowywanie planów działania**, zgłaszamy następujące propozycje:

- **umożliwienie zwolnienia operatora z obowiązku tworzenia planu w zakresie objętym posiadanym certyfikatem ISO 22301, ISO 27001** (w szczególności w zakresie świadczenia usług telekomunikacyjnych i teleinformatycznych).
- **urealnienie możliwości wykorzystania formy elektronicznej** - przewidziana obecnie możliwość przekazania planu do UKE w formie dokumentu elektronicznego, opatrzonego przez przedsiębiorcę kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, zapisanego w formacie .doc(x), .odt albo .pdf, z wyłączeniem elektronicznej kopii stanowiącej obraz pierwotnego dokumentu wymaga takiego dostosowania, aby faktycznie była możliwa. Obecnie brak jest możliwości skutecznego przekazania bardzo obszernych planów, których nie da się przesłać w wymagany obowiązującymi przepisami sposób - za pomocą takiego nośnika jak np. nagrana płyta CD lub pendrive.
- **skorelowanie planów działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń z planami ochrony infrastruktury krytycznej,** tak aby plany działań w sytuacjach szczególnych zagrożeń spełniały jednocześnie wymagania planów ochrony infrastruktury krytycznej, przygotowanych i wdrażanych zgodnie z art. 6 ust. 5 i 7 ustawy o zarządzaniu kryzysowym.
- **ograniczenie katalogu organów administracji publicznej, z którymi plan ma zostać uzgodniony, wyłącznie do podmiotów, z którymi uzgadnianie planu jest merytorycznie uzasadnione** biorąc pod uwagę kompetencje właściwych organów. Zgodnie z § 8 ust. 1 obowiązującego rozporządzenia z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, plan ogólny musi zostać uzgodniony łącznie z dziewięcioma podmiotami administracji publicznej, co czyni uzgodnienie planu ogólnego procesem bardzo czasochłonnym i biurokratycznie skomplikowanym. Wśród organów, z którymi plan ogólny ma zostać uzgodniony, są m.in. minister właściwy do spraw finansów publicznych oraz Minister Sprawiedliwości. Biorąc pod uwagę zakres kompetencji obu wymienionych ministrów brak jest jakiegokolwiek uzasadnienia merytorycznego do

utrzymywania obowiązku uzgadniania planu z Ministrem Finansów i Ministrem Sprawiedliwości, gdyż uzgadnianie planu ogólnego z tymi dwoma podmiotami nie wnosi wartości dodanej ani do uzgadnianego planu ani do systemu zarządzania kryzysowego podmiotów uzgadniających. W związku z powyższym przyszłe rozporządzenie w tym zakresie powinno przewidywać racjonalny i uzasadniony katalog organów, z którymi plan ma zostać uzgodniony, a w szczególności wśród tych podmiotów nie powinno znajdować się Ministerstwo Finansów i Ministerstwo Sprawiedliwości.

Jednocześnie z uwagi na bardzo wczesny etap prac oraz odległą perspektywę wydania nowego aktu wykonawczego, zastrzegamy możliwość uzupełnienia niniejszego stanowiska o dodatkowe zagadnienia na kolejnych etapach prac koncepcyjnych i legislacyjnych.