LEWIATAN

Warszawa, 13 czerwca 2018 r.
KL/208/85/1008/AM/2018

Pan
**Marek Kuchciński**
Marszałek Sejmu

Pan
**Paweł Pudłowski**
Przewodniczący
Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii

Pan
**Michał Jach**
Przewodniczący Komisji Obrony Narodowej

Szanowny Panie Marszałku,
Szanowni Panowie Przewodniczący,

W nawiązaniu do rozpoczynających się w Sejmie prac nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa (druk 2505), w załączeniu przekazuje uwagi Konfederacji Lewiatan do projektu.

Z poważaniem,

Henryka Bochniarz
Prezydent Konfederacji Lewiatan

Do wiadomości:
Departament Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
Pan Tomasz Zdzikot - Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Załącznik:
1. Stanowisko Konfederacji Lewiatan do rządowego projektu ustawy o krajowym systemie cyberbezpieczeństwa (druk 2505).



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

**Stanowisko Konfederacji Lewiatan do projektu ustawy o krajowym systemie cyberbezpieczeństwa (druk 2505)** (dalej: projekty ustawy)

Podniesienie poziomu krajowego cyberbezpieczeństwa bez wątpienia stanowi kluczowe wyzwanie, zarówno dla sektora publicznego, jak również dla prywatnych przedsiębiorców. Niestety jednak, proponowany model realizacji zadań państwa w obszarze cyberbezpieczeństwa może okazać się z jednej strony niewystarczająco efektywny, a z drugiej zbytnio ingerujący w sferę działalności podmiotów gospodarczych. Tym samym, nasze kluczowe wątpliwości dotyczą ustalenia:

- czy faktycznie projektowane rozwiązania przyczynią się **do podniesienia poziomu cyberbezpieczeństwa krajowego oraz**
- czy zakres przewidzianych rozwiązań nie wprowadza, zbytniego niekontrolowanego wpływu państwa na podmioty gospodarcze, rozszerzając uprawnienia władcze organów państwowych wobec podmiotów gospodarczych
- potencjalnego negatywnego wpływu na **konkurencyjność polskiej gospodarki**.

I. Biorąc to pod uwagę, przedstawiamy następujące uwagi o charakterze ogólnym:

1. **Brak precyzyjnych zasad funkcjonowania jednostek zależnych od organów państwowych** funkcjonujących również na rynku komercyjnym, w tym m.in. brak ograniczeń prowadzenia działalności komercyjnej przez jednostki wykonujące zadania CSIRT, w zakresie wynikającym z ustawy. W naszej ocenie podmiot pełniący funkcję CSIRT, powinien realizować wyłącznie zadania o charakterze publicznych i niekomercyjnym. Jego funkcjonowanie na rynku konkurencyjnym, budzi istotne wątpliwości, szczególnie w sytuacji gdy możliwość pozyskiwania (z mocy prawa) informacji od innych podmiotów stawia go w uprzywilejowanej pozycji rynkowej.
2. **Brak ograniczenia zakresu uprawnień nadzorczych organów nadzoru i kontroli** wyłącznie do obszaru związanego bezpośrednio ze świadczeniem usług kluczowych.
3. **Bardzo szerokie uprawnienia, CSIRT-ów w zakresie możliwości żądania od operatorów telekomunikacyjnych udostępnienia informacji dot. ich działalności** oraz przyjętych rozwiązań organizacyjno–technicznych. Wprowadzenie takich rozwiązań, w szczególności z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk, może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa.
4. **Brak publikacji kluczowych aktów wykonawczych**. Uwzględniając, że nowe obowiązki oraz ograniczenia prowadzenia działalności gospodarczej mogą być wprowadzane wyłącznie w drodze ustawowej, wątpliwości budzi fakt, że do konsultacji nie zostały skierowane projekty obligatoryjnych rozporządzeń, których postanowienia będą bardzo istotne dla całego systemu ochrony cyberprzestrzeni, a tym samym mają kluczowy wpływ na ocenę całości proponowanych rozwiązań. W naszej ocenie, **ustawa powinna być konsultowana i procedowana w pakiecie wraz ze wszystkimi**



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

(przynajmniej obligatoryjnymi) **aktami wykonawczymi**. Dodatkowo zwracamy uwagę, że trudno ustalić faktyczne i merytoryczne przesłanki uzasadniające decyzje o regulacji pewnych zagadnień na poziomie ustawowym, a część na poziomie aktów wykonawczych. Przykładowo, bardzo szczegółowo definiuje się wymagania funkcjonalne na system teleinformatyczny wspomagający obsługę incydentów, pozostawiając jednocześnie do regulacji w drodze rozporządzenia wydawanego przez ministra ds. informatyzacji istotne z punktu widzenia obrotu gospodarczego wymagania dla podmiotów świadczących usługi outsourcingu w zakresie cyberbezpieczeństwa. W tym kontekście, jako niespotykaną dotychczas praktykę odbieramy określenie w regulacji ustawowej (z zasady mało elastycznej i trudniejszej do zmiany) precyzyjnych wymagań dla systemu informatycznego i jego funkcjonalności (co wydaje się materią typowo wykonawczą), podczas gdy sam projekt ustawy nie określa w sposób jasny i precyzyjny podstawowego pojęcia, jakim ma być „incydent poważny".

5. **Brak jednego punktu zgłoszeń incydentów na poziomie krajowym**, do którego można byłoby zgłaszać incydenty, a do którego odpowiedzialności należałoby odpowiednie przekierowanie incydentu wg właściwości. Takie rozwiązanie wydaje się efektywniejsze, niż zaproponowany, dość skomplikowany model zgłaszania poszczególnych kategorii incydentów w Polsce. Warto w tym kontekście zauważyć, że liczba organów, do których przedsiębiorca powinien zgłaszać ewentualne incydenty, w ostatnim okresie, wraz ze stopniowym wprowadzaniem nowych rozwiązań legislacyjnych, znacząco wzrasta. Aktualnie obowiązki takie istnieją już w zakresie zgłoszeń do: UKE, GIODO, ministra ds. informatyzacji (odnośnie usług zaufania). Dodatkowo wprowadzony zostanie obowiązek wobec CSIRT NASK (odnośnie incydentów istotnych przy usługach cyfrowych), odpowiedni CSIRT (w zakresie incydentów poważnych przy usługach kluczowych). Liczne obowiązku sprawozdawcze, ograniczają funkcjonowanie przedsiębiorcom, a same w sobie nie przyczyniają się do zwiększenia poziomu cyberbezpieczeństwa użytkowników.
6. **Brak jednoznacznego i nie budzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego** – z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej strony projekt ustawy przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad przejmowania przez CSIRT incydentów do obsługi oraz przyznając CSIRT pewne uprawnienia „władcze" wobec operatora (np. wezwanie za pośrednictwem organu właściwego operatora do usunięcia podatności, żądanie informacji itd.). Tym samym, CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za podejmowane wobec operatora działania.

Uszczegóławiając powyższe, zwracamy uwagę, że zgodnie z projektowanym art. 12 ust. 1 pkt 6 operator ma zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT, w tym poinformować o usunięciu podatności, które doprowadziły lub mogły doprowadzić do poważnego incydentu.

Na wniosek operatora CSIRT może zapewnić wsparcie w obsłudze lub obsługę poważnych incydentów (art. **26** ust.2), przy czym odpowiednio – zgodnie z projektowanym art. **26** ust. 2 - zadaniem CSIRT jest realizacja zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynację obsługi poważnych incydentów.

Natomiast zgodnie z projektowanym art. **26** ust. 5, 6 i 7 do zadań CSIRT należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez wskazane w ustawie podmioty. Z tym uprawnieniem korelują



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

uprawnienia CSIRT wskazane w art. 32, zgodnie z którym CSIRTy mogą: „wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługa incydentów poważnych (...), a także dokonywać analiz (...)", „wystąpić do organu właściwego z wnioskiem o wezwanie operatora, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu" oraz „może wystąpić bezpośrednio do operatora o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu"

W praktyce może to oznaczać, że dla jednego incydentu, właściwe będą trzy ośrodki, co w praktyce znacznie utrudni, o ile nie uniemożliwi jego właściwą obsługę. Po drugie, istnieje znaczące ryzyko, że CSIRT może definiować względem operatora nieadekwatne wymagania, które mogą generować nadmierne obciążenia kosztowe, jednocześnie nie stanowiąc najbardziej efektywnego rozwiązania zaistniałego problemu.

II. Uwagi do poszczególnych artykułów projektu ustawy:

1. Zgodnie z Dyrektywą ustawa ma być przyjęta do 9 maja a stosowana od 10 maja włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada.

Ustawa ma vacatio legis tylko 14 dni (art. 88). Pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy.
Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce około 6-9 miesięcy, a na świecie nawet bliżej roku. Przy obecnym vacatio legis dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego zobowiązane wydaje się wątpliwym.

2. Art. 2 punkty 5-8 – definicje incydentów powinny umożliwiać dokładną ich klasyfikację.

Przy obecnie podanych definicjach, podmiot komercyjny dokonujący klasyfikacji będzie miał ogromny problem, aby ocenić, czy dany incydent skutkuje *'znaczną szkodą dla [..], zaufania do instytucji publicznych [...]'*.

3. Art. 5 ust. 1 oraz ust. 2 pkt 1

Sugerujemy, iż zawartość decyzji o uznaniu za operatora usługi kluczowej powinna doprecyzować **jakie usługi kluczowe** realizuje operator usługi kluczowej, które są objęte tymi przepisami.

W wykazie usług kluczowych powinny być sprecyzowane usługi kluczowe dla poszczególnych obszarów działalności w celu precyzyjnego określenia zakresu w jakim dostawcy usług mają wdrożyć wymagania ustawy.



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

4. Art 5 ust **7**

Podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprocedowania, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy.

Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że podmiot takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc).
Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na to nie dłuższy niż 1 rok (może być zależny od branży) lub określa zakres prac, które musi przeprowadzić i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie.

Proponujemy usunięcie Art. 5 ust. **7**.

5. Art. 6 i Art. 7 ust 1

Zmiany tych rozporządzeń będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na wiele lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać od nich nowych wydatków i znacznych nakładów pracy.
Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one oparte o ustawę, a nie o rozporządzanie.

6. Art. **6 ust. 1**

Należy dodatkowo zmienić treść tego ustępu nadając mu brzmienie: „ *Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa* – dodać – ***oraz operatorami usługi kluczowej*** *(...)".*

Opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorcy związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny.

7. Art. **8** ust.2 **e**

Użyte w przepisie pojęcie *trybu ciągłego* jest niewystarczająco precyzyjne. Prosimy o doprecyzowanie jakie elementy infrastruktury teleinformatycznej powinny być objęte ciągłym monitorowaniem. Proponujemy doprecyzowanie zapisu.



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

8. Art. 9 ust. 1 pkt 2

Ustęp ten może wnieść korzyści np. w sektorze bankowości. Jednakże w sektorze energii elektrycznej koszty zapewnienia dostępu do wiedzy mogą być wysokie, a korzyści niewielkie gdyż użytkownicy nie są wstanie przeciwdziałać atakom na infrastrukturę elektroenergetyczną.
Proponujemy następujące brzmienie art. 9 ust. 1 pkt 2:

> *Art. 9. 1. Operatorzy usług kluczowych są obowiązaniu do:*
> *... 2) zapewnienia użytkownikowi usługi kluczowej, o ile użytkownik ma wpływ na ciągłość świadczonej usługi kluczowej, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.*

Obowiązek prowadzenia działalności edukacyjnej powinien spoczywać przede wszystkim na CSIRT oraz przez organach państwa koordynujących kwestie cyberbezpieczeństwa na poziomie krajowym. Działalność operatorów usług kluczowych, w tym zakresie powinna mieć wyłącznie subsydiarny charakter. Jest to uzasadnione faktem, że wiedza o zagrożeniach cyberbezpieczeństwa powinna obejmować pełne spektrum zagrożeń i zabezpieczeń oraz dawać użytkownikowi całościowy obraz, a nie ograniczać się do pojedynczych usług. Uważamy, że to zadanie powinno być to realizowane przez wskazane w ustawie CSiRT'y lub MC, które dysponują wiedzą kompleksową na temat zagrożeń w cyberprzestrzeni i posiadają dane statystyczne.

Do prowadzenia takiej działalności predestynuje te podmioty również zakres informacji pozyskiwanych przez CSIRT-y oraz organy właściwe o incydentach, ale również o stosowanych zabezpieczeniach stosowanych przez operatorów, itd. Tego typu informacje, w formie dostosowanej do potrzeb edukacyjnych, zagregowanej i zanonimizowanej mogłyby być wykorzystywane właśnie w działalności edukacyjnej. Zwiększyłoby to istotnie proporcjonalność wykorzystania pozyskanych od podmiotów rynkowych danych.

9. Art. 11 ust. 1 pkt 4 oraz 18 ust. 1 pkt 4

Dostawca usługi kluczowej oraz **dostawca usługi cyfrowej** może nie być w stanie zebrać i przekazać wartościowych informacji w tak krótkim czasie jak 24 godziny. Proponujemy wydłużenie tego czasu do **48** godzin.

Proponujemy następujące brzmienie art. 11 ust. 1 pkt 4:

> *Art. 11. 1. Operatorzy usług kluczowych są obowiązani:*
> *... 4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu **48** godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;*

> *Art. 18. 1.*
> *... 4) zgłasza incydent istotny niezwłocznie, nie później niż w ciągu **48** godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;*
> Art. 12 ust. 2



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

10. Obowiązek zgłaszania incydentów poważnych (art. 12 ust. 1 pkt 6 pkt 7)

Zgodnie z projektem na operatorze spoczywa obowiązek zgłaszania „incydentu, który mógł mieć wpływ na usługi kluczowe", czyli potencjalnie każdego incydentu. W praktyce może to stanowić znaczące rozszerzenie spoczywającego na operatorze obowiązku notyfikacyjnego. W związku z tym rekomendujemy wykreślenie zapisu.

Ponadto sygnalizujemy, że zakresy obowiązków informacyjnych zdają się nakładać. Zgodnie z projektowanym pkt 4 lit. f należy wskazać m.in. przyczynę zaistnienia incydentu, a zgodnie z pkt. 7 mamy podać przyczynę i źródło incydentu, jeżeli są one znane w chwili zgłoszenia. W naszej ocenie należy pozostawić obowiązek określony w pkt. 7.

11. Przekazywanie przez operatorów usług kluczowych do właściwego CSIRT informacji o zagrożeniach, szacowaniach ryzyka, podatnościach, wykorzystywanych technologiach (art. 13)

Z uwagi na brak szczególnego uzasadnienia, brak określenia sposobu wykorzystywania danych przez CSIRT, a także fakultatywny charakter projektowanego art. 13 rekomendujemy usuniecie zapisu.

12. Art. **15** ust. 1

Organizacja certyfikowanego audytu jest dodatkowym kosztem dla operatorów. Wzorem audytu energetycznego sugerujemy wyznaczyć częstotliwość audytu raz na **4 lata.** Pozwoli to lepiej rozłożyć koszty oraz wysiłek jakie musi włożyć operator w przeprowadzenie audytu.

Proponujemy następujące brzmienie art. 15 ust. 1:

***15. 1. Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie co najmniej raz na cztery lata audytu bezpieczeństwa systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej „audytem".***

13. **Art. 15** ust 2

Proponujemy doprecyzować, że posiadanie przez operatora usług kluczowych aktualnego certyfikatu ISO/IEC 27001 (np. w zakresie cyberbezpieczeństwa) będącego wynikiem audytu systemu zarządzania bezpieczeństwem informacji zwalnia operatora usług kluczowych z obowiązku poddawania się ww. audytowi.

Ponadto brakuje korelacji między obowiązkiem przeprowadzenia audytu (w praktyce na koszt operatora) z obowiązkiem przekazania kopii sprawozdania z audytu organowi właściwemu, a obowiązkiem poddania się kontroli, o której mowa w rozdziale VIII. Skoro bowiem nakłada się na operatora obowiązek poddania się regularnemu audytowi to proponujemy w związku z tym ograniczenie uprawnień kontrolnych organu nadzorczego (audyt zastępuje kontrolę).



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

14. Art. 16 pkt 1 i 2

Art. 16 punkt 1

Okres 3 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu **6 miesięcy .**

Proponujemy następujące brzmienie art. 16 pkt 1:

*Art. 16. 1. Operatorzy usług kluczowych realizują obowiązki określone w:*
*1) art. 8 pkt 1 i 4, art. 9, art. 11 ust. 1–3, art. 12 i art. 14 ust. 1 – w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej*

Art. 16 punkt 2
Okres 6 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu **roku.**

Proponujemy następujące brzmienie art. 16 pkt 2:

*Art. 16. 2.*
*Operator usługi kluczowej realizuje obowiązki określone w:*
*2) art. 8 pkt 2 i 3 oraz pkt 5 i 6 i art. 10 ust. 1–3 – w terminie* ***roku*** *od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;*

15. Uprawnienia CSIRT w zakresie pozyskiwania od operatora informacji (art. 32)

Postulujemy doprecyzowanie, że obowiązek przekazania informacji CSIRT nie dotyczy informacji prawnie chronionych.
Projektowany art. 32 ust. 2 został określony w sposób zbyt ogólny i wymaga doprecyzowania poprzez wskazanie zamkniętego katalogu uprawnień. W swoim aktualnym brzmieniu umożliwiałby CSIRT wręcz nieograniczony zakres działań, w tym np. możliwość instalowania w sieci służącej świadczeniu publicznych usług telekomunikacyjnych i będącej własnością komercyjnego podmiotu, własnych urządzeń telekomunikacyjnych CSIRT, które pozostawałyby poza kontrolą właściciela tej sieci. Takie potencjalne działania skutkowałyby brakiem możliwości spełnienia przez operatora jego podstawowych obowiązków, np. w zakresie ochrony tajemnicy telekomunikacyjnej
Projektowany art. 32 ust. 3 w zakresie obowiązku usunięcia podatności w wyznaczonym przez właściwy organ terminie może oznaczać konieczność poniesienia wysokich kosztów oraz istotnej przerwy w świadczeniu podstawowej usługi. Dodatkowo może naruszać zasadę adekwatności zabezpieczeń w stosunku do ryzyk i w ten sposób ingerować w model biznesowy operatorów telekomunikacyjnych.
Podsumowując uprawnienia CSIRT określone w projektowanym art. 32 mogą skutkować naruszeniem regulacji związanych z ochroną tajemnicy telekomunikacyjnej oraz rozporządzenia RODO, a także duplikują


Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

istniejący mechanizm, który funkcjonuje dla służb ochrony państwa. Co więcej nie przewidziano żadnej niezależnej kontroli państwa nad tymi żądaniami, a w szczególności nie ma możliwości odwołania się od decyzji CSIRT, podczas gdy nawet dla działań ABW niezbędna jest zgoda sądu, a więc zapewnione są mechanizmy kontrolne przed nadużyciami uprawnień.

16. Organy właściwe (art. 41 pkt 1 pkt 8-11)

Sygnalizujemy, że w obszarze rynku telekomunikacyjnego może występować nakładanie się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE. Może to generować ryzyko nakładania się na siebie różnych, wykluczających się lub niespójnych obowiązków, a tym samym znacząco zwiększać ryzyko prowadzenia działalności gospodarczej.

17. Art. 42 ust. 3

**Uregulowania w ustawie zasad funkcjonowania jednostek podległych lub nadzorowanych przez organy państwowe (w ustawie „organy właściwe") funkcjonujących również na rynku komercyjnym.**

W takim wypadku podmiot realizujący zadania CSIRT powinien realizować wyłącznie zadania o charakterze publicznym i niekomercyjnym. Funkcjonowanie takiego podmiotu na rynku konkurencyjnym w sytuacji, gdy ma możliwość pozyskiwania (z mocy prawa) informacji od innych podmiotów stawia go w uprzywilejowanej pozycji rynkowej, co budzi uzasadnione obawy i wątpliwości. Obawy i wątpliwości są tym większe, że zgodnie z projektem ustawy organ właściwy może powierzyć realizację, w jego imieniu, zadań związanych z wykonywaniem nadzoru, w tym m.in. „prowadzenie kontroli operatorów usług kluczowych i dostawców usług cyfrowych" (art. 42 ust. 3) jednostkom podległym lub nadzorowanym przez ten organ, z zachowaniem wszystkich uprawnień przewidzianych w tym zakresie w ustawie.

18. Art. 46 ust 1 pkt 5

System informatyczny powinien zapewniać automatyczny (machine-2-machine) interfejs umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).

19. Art. 55 pkt 1 i pkt 6

Nie jest realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do przemieszczania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tę ustawę i wiele innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta dostępu czy inna metoda) powinien być wybrany przez



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

kontrolowany podmiot ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej.

Ponadto takie podejście jest sprzeczne z wymaganiami wynikającymi z ustawy o ochronie informacji niejawnych, a w przypadku takich podmiotów, jak przedsiębiorcy telekomunikacyjny zachodzi duże prawdopodobieństwo, że część obiektów, a na pewno elementów infrastruktury teleinformatycznej istotnej przy cyberbezpieczeństwie, podlega również pod rygory tej ustawy). Należy również pamiętać o kwestii przetwarzania danych osobowych (RODO) i kontroli dostępu.

Podmioty świadczące usługi kluczowe, to np. energetyka. Kto weźmie odpowiedzialność za nieprzeszkoloną stanowiskowo osobę poruszającą się po elektrowni czy petrochemii? Nieznajomość sygnałów czy zasad obowiązujących na obiekcie produkcyjnym może prowadzić nawet do śmierci osoby kontrolującej (wysokie napięcie, para wodna, chemikalia, wyziewy, etc).

Wnosimy o wykreślenie zapisu wskazującego na brak konieczności uzyskania przepustki.

**W projekcie należy wyraźnie zaznaczyć, że kontrola może dotyczyć wyłącznie pomieszczeń, dokumentów i systemów wykorzystywanych do świadczenia usługi kluczowej. Dlatego też** proponujemy wstęp do art. 55 ustawy uzupełnić, nadając mu następujące brzmienie:

> „Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami **w odniesieniu do pomieszczeń, dokumentów i systemów wykorzystywanych przez przedsiębiorcę do świadczenia usługi kluczowej** ma prawo do: (...)„

Dodatkowo w pkt 6 należy doprecyzować zakres działań związanych z „oględzinami urządzeń, nośników i systemów teleinformatycznych", w szczególności poprzez wskazanie, że takie „oględziny" nie mogą prowadzić do jakiejkolwiek ingerencji w działanie urządzeń, nośników i systemów (art. **55** pkt 6).

20. Art. 55 pkt 4

Dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.) a więc takie dane nie mogą być ujawnione, na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.

***Konfederacja Lewiatan, KL/208/85/1008/AM/2018***



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS