ZWIĄZEK PRACODAWCÓW TECHNOLOGII CYFROWYCH
LEWIATAN

Warszawa, 24 maja 2024 r.
KL/297/82/AM/2024

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik rządu ds. cyberbezpieczeństwa

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Premierze,
Szanowny Panie Ministrze,

W odpowiedzi na zaproszenie do udziału w konsultacjach projektu ustawy o zmianie ustawy krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (uksc) (wersja z dnia 24 kwietnia 2024 roku), Związek Pracodawców Technologii Cyfrowych Lewiatan, w załączeniu, przesyła stanowisko wobec projektu ustawy.

Z poważaniem

Jolanta Jaworska
Prezes
Związek Pracodawców Technologii Cyfrowych Lewiatan

Do wiadomości:
Pan **Łukasz Wojewoda**
Dyrektor Departamentu Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Załącznik: Stanowisko Związku Pracodawców Technologii Cyfrowych Lewiatan wobec projektu ustawy o zmianie ustawy krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (uksc) (wersja z dnia 24 kwietnia 2024 roku).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

ZWIĄZEK PRACODAWCÓW TECHNOLOGII CYFROWYCH LEWIATAN

Stanowisko Związku Pracodawców Technologii Cyfrowych Lewiatan wobec projektu ustawy o zmianie ustawy krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (uksc) (wersja z dnia 24 kwietnia 2024 roku).

Uwagi ogólne

1. Czas konsultacji i późniejszego wdrożenia

Stoimy na stanowisku, że projekt ustawy, który ma dotyczyć bezpośrednio ponad 38 tysięcy podmiotów, a pośrednio (dostawcy podmiotów kluczowych lub ważnych) kolejnych kilkudziesięciu tysięcy musi być bardzo solidnie przedyskutowany w szerokim gronie. Co więcej, w wielu krajach UE już dzisiaj rządy komunikują, że nie zdołają dotrzymać terminów przewidzianych w Dyrektywie, a oficjalna strona postępów wdrożenia wykazuje, że jedynym krajem, który ma proces za sobą jest Chorwacja. https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2555&qid=1715785064589

Dlatego też apelujemy, aby natychmiast rozpocząć kolejny etap konsultacji. Ze swojej strony deklarujemy gotowość do spotkania i przedstawienia w drodze dialogu przygotowane przez nas uwagi. Powinno to znakomicie skrócić czas związany z przygotowaniem kolejnych wersji.

2. Uksc a inne ustawy

Ustawa o krajowym systemie cyberbezpieczeństwa jest w sposób nierozerwalny połączona z wieloma innymi aktami prawnymi, które podlegają aktualnie nowelizacji. Wiele z nich nie zostało jeszcze formalnie opublikowanych, niektóre nie są przygotowywane w Ministerstwie Cyfryzacji – a to oznacza konieczność z jednej strony bardzo starannej koordynacji i synchronizacji pojęć, wymagań i procesów. Brak takiej analizy i odpowiednich zapisów będzie skutkował zwiększeniem poziomu prawnej niepewności, a w rezultacie finalnie nie przyczyni się do podniesienia cyberbezpieczeństwa Polski.
Część zauważonych problemów przekazujemy dalej w uwagach szczegółowych.
Wskazujemy na co najmniej następujące dokumenty, które właśnie podlegają zmianom:

a. Ustawa o informatyzacji – 9 maja 2024 https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-informatyzacji-dzialalnosci-podmiotow-realizujacych-zadania-publiczne
b. Rozporządzenie KRI – 10 maja 2024 https://www.gov.pl/web/premier/projekt-rozporzadzenia-rady-ministrow-w-sprawie-krajowych-ram-interoperacyjnosci-minimalnych-wymagan-dla-rejestrow-publicznych-

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

minimalnych-wymagan-dla-systemow-teleinformatycznych-oraz-wymiany-informacji-w-postaci-elektronicznej

c. Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa – 2 maja 2024 https://www.gov.pl/web/premier/projekt-ustawy-o-krajowym-systemie-certyfikacji-cyberbezpieczenstwa
d. Uchwała WIIP https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-zmieniajacej-uchwale-w-sprawie-inicjatywy-wspolna-infrastruktura-informatyczna-panstwa5
e. Projekt ustawy o zarządzaniu kryzysowym, infrastrukturze krytycznej i podmiotach krytycznych – w przygotowaniu
f. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (akty wdrażające DORA) https://legislacja.rcl.gov.pl/projekt/12384252/katalog/13053510#13053510
   Warto przy tym zaznaczyć, że do tego projektu organizacje społeczne przesłały uwagi liczące po co najmniej kilkanaście stron.

   ale także trzeba uwzględnić co najmniej

g. Ustawa o działaniach antyterrorystycznych, wprowadzającą stopnie alarmowe Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (sejm.gov.pl) oraz
   Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP
   Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (sejm.gov.pl)
   patrz także: motyw (88) Dyrektywy NIS2
h. Rozporządzenie European Health Data Spaces, które najprawdopodobniej zostanie opublikowane do czasu uchwalenia nowelizacji uksc, a którego znaczenie dla sektora ochrony zdrowia jest równe znaczeniu DORA dla sektora finansowego https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0140(COD)&l=en
i. Rozporządzenie AI Act, którego publikacja jest planowana w najbliższych dniach https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Warto zaznaczyć, że w projekcie nie widać także żadnych elementów związanych z wdrożeniem w Polsce Aktu w sprawie danych (Data Act), który będzie miał ogromne znaczenie dla cyberbezpieczeństwa podmiotów kluczowych i ważnych wykorzystujących dane nieosobowe, a które będzie egzekwowalny od 12 września 2025 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R2854

W szczególności chcemy tutaj zwrócić uwagę na współzależności pomiędzy Dyrektywami CER oraz NIS2, gdzie ta pierwsza odsyła zadania z cyberbezpieczeństwa do drugiej. Jednak należy zwrócić uwagę, że obszary ochrony w infrastrukturze krytycznej inne niż teleinformatyka są również w wielkim stopniu ucyfrowione. A to oznacza konieczność zgrania kompetencji i decyzyjności dla różnych regulatorów odpowiedzialnych za bezpieczeństwo.
Innym elementem jest oczywiście odesłanie transpozycji NIS2 do prawa dla określonego segmentu np. DORA czy EHDS, zwłaszcza że granice wcale nie są tak twarde. Przykładowo Zakład Ubezpieczeń Społecznych podlega DORA, jednak jako podmiot sektora finansów publicznych i realizujący zadania publiczne będzie miał nakładane dodatkowe wymagania. Każda sprzeczność, a nawet tylko niejasność przepisów będzie prowadziła do problemów.

3. **Oszacowanie kosztów wdrożenia w OSR**

Naszym zdaniem brakuje realnego oszacowania kosztów wdrożenia ustawy przez podmioty kluczowe i ważne. Wstępna ocena samej pracy papierowej związanej z przygotowaniem do realizacji zadań kierownika podmiotu kluczowego lub ważnego wymienionych w art. 8d (pomijając punkt 4) czyli szkolenia) będzie kosztowała średnio przynajmniej dziesięć tysięcy złotych. Podkreślamy, że jest to bardzo konserwatywne wyliczenie, ponieważ w podmiotach powyżej 250 pracowników i dodatkowo nadzorowanych innymi przepisami taki proces przygotowawczy będzie kosztował nawet kilkaset tysięcy złotych.
Jeśli nawet pominiemy podmioty sektora publicznego, które mają otrzymać dodatkowe wsparcie w wysokości ok. 1,5 mld złotych pochodzących z KPO to koszt dla pozostałych przedsiębiorstw będzie wynosił przynajmniej 100 milionów złotych. Chcemy dobitnie podkreślić, że nie są to kwoty wydane na podniesienie cyberbezpieczeństwa, ale na papierologię. Takie informacje i uczciwa kalkulacja powinna znaleźć się w OSR. W optymalnym przypadku razem z informacją w jaki sposób rząd zamierza ograniczyć wydatki na takie działania.

4. **Koncentracja na systemie sprawozdawczym cyberbezpieczeństwa. Brak zasadniczych elementów cyberbezpieczeństwa w treści ustawy.**

Wydaje się, że projekt ustawy zbyt koncentruje się na części formalnej i sprawozdawczej. Szczegółowo opisywane są procedury, a nawet zasady naliczania kary pieniężnej jakiej może podlegać kierownik podmiotu kluczowego lub ważnego w proporcji do wynagrodzenia „obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop”

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

(art. 73a), a jednak zasadniczym celem jest podniesienie poziomu cyberbezpieczeństwa, a nie „sprawozdawczości w cyberbezpieczeństwie".
Należy przy tym zauważyć, że zasady cyberbezpieczeństwa są podane w sposób bardzo ogólny w artykule 8, zaś bez jednoczesnej analizy aktów wykonawczych, o których mówi art. 8a trudno cokolwiek powiedzieć. Apelujemy o jak najszybsze przedstawienie projektów rozporządzeń, o których mówi ten artykuł, także w kontekście zmian innych aktów prawnych, o których mówiliśmy powyżej.
W szczególności chcemy zwrócić uwagę na brak w treści ustawy zagadnień zapisanych w motywie (89) Dyrektywy NIS2 takich jak:

- Zasada Zerowego Zaufania (Zero Trust)
- Segmentacja sieci
- Zarządzanie tożsamością i dostępem

Uważamy za właściwe, aby te zapisy znalazły się – podobnie jak zapisy dotyczące aktualizacji oprogramowania - w ustawie.

5. **Obecność outsourcingu informatycznego lub wykorzystania chmury obliczeniowej, w tym świadczonego z zagranicy**

Wydaje się, że przy projektowaniu ustawy przewidziano tylko jeden rodzaj przetwarzania w jednym rodzaju podmiotów. Zapisy są dopasowane do sytuacji, w której podmiot nadzorowany jest podmiotem działającym wyłącznie na terenie Polski i niebędącym częścią żadnej grupy przedsiębiorstw oraz przetwarzającym swoje dane wyłącznie w infrastrukturze własnej na terenie Polski.
Poniżej przedstawić chcemy – na przykładzie kilku scenariuszy związanych ze sprawowaniem nadzoru opisanych w art. 53a – 53d – jak najbardziej realne scenariusze:

- Polski podmiot kluczowy/ważny będący częścią grupy międzynarodowej przetwarza dane w infrastrukturze grupy poza Polską
- Polski podmiot kluczowy/ważny przetwarza u polskiego dostawcy chmury (centrum przetwarzania danych znajduje się w Polsce) współdzieląc zasoby tego dostawcy
- Polski podmiot kluczowy przetwarza u dostawcy chmury w CPD poza Polską
- Europejski podmiot kluczowy przetwarza u dostawcy chmury spoza Polski, ale w CPD znajdującym się na terenie Polski
- Polski podmiot korzysta z outsourcingu informatycznego świadczonego poza Polską przez podmiot ważny (w Polsce, zgodnie z uksc taki podmiot zakwalifikowany byłby jako podmiot kluczowy)
- Polski podmiot kluczowy sektora finansowego (podlegający DORA) wykorzystuje kluczowego zewnętrznego dostawcę ICT wyznaczonego przez Europejskie Urzędy Nadzoru (patrz art. 31-32 DORA)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Oczywiście w tym przypadku należy także rozważyć elementy związane ze sprawowaniem nadzoru zwłaszcza opisanymi w art. 53d. Czy urzędnik monitorujący uda się za granicę aby bez przepustki poruszać się po terenie podmiotu kluczowego i przeprowadzać oględziny urządzeń, nośników i systemów informacyjnych? Czy urzędnik monitorujący z innego kraju UE będzie mógł wkroczyć bez przepustki na teren CPD na terenie Polski i dokonywać oględzin? Jak takie oględziny związane z prewencyjną kontrolą podmiotu X będą wyglądały u dostawcy chmury obliczeniowej, gdzie przetwarzają także podmioty Y i Z? A może także podmiot U, który nie jest polskim podmiotem? Wreszcie jak wygląda odpowiedzialność w przypadku kiedy urzędnik monitorujący dokonując oględzin doprowadzi do incydentu bezpieczeństwa, zwłaszcza kiedy przetwarzanie będzie miało miejsce w infrastrukturze innego podmiotu, a incydent dotyczy podmiotu trzeciego, niebędącego przedmiotem kontroli?
Uważamy, że projekt uksc powinien być bardzo dokładnie przejrzany pod kątem różnych scenariuszy przetwarzania, tak aby oddawał rzeczywistość technologiczną, a także relacje nadzoru opisane w innych aktach prawnych powiązanych z Dyrektywą NIS 2 (Dyrektywa CER, DORA, EHDS, CRA).
Patrz także uwagi do art. 10, do art. 33 ust. 9 oraz art. 53d

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Uwagi szczegółowe:

6. Wykorzystanie jednolicie w całej ustawie pojęć produkt ICT, proces ICT i usługa ICT

Postulujemy wykorzystywać w całej ustawie jednolitą nomenklaturę z wykorzystaniem zdefiniowanych pojęć „produkt ICT", „proces ICT" i „usługa ICT" (art. 1 pkt 11h-11j). W tekście ustawy często używa się tych pojęć, niekiedy nawet nimi zastępuje pojęcia z aktualnej wersji ustawy, jednak pojawiają się ciągle równolegle określenia „sprzętu i oprogramowania" (przykład: art. 8, nawet sąsiadują ze sobą w pkt 4)

7. Definicja dostawcy chmury (art. 2 pkt 4e)

Uwaga 1: Dyrektywa NIS2 wprowadza definicję usług chmurowych (art. 6 p. 30), natomiast dostawca chmury (dostawca usług chmurowych) nie jest dalej definiowany. Wydaje się to właściwym podejściem.
Uwaga 2: Rekomendujemy określenie „dostawca chmury" lub „dostawca chmury obliczeniowej", ponieważ de facto zamawiający korzystają z predefiniowanych i prekonfigurowanych produktów, którymi samodzielnie zarządzają, używają i dostosowują przy minimalnym udziale dostawcy. Oferta chmurowa jako model jest podobna do oprogramowania z półki, w odróżnieniu od oferty outsourcingu, która jest bliższa oprogramowaniu tworzonemu na zamówienie, co wymaga bezpośredniego i dedykowanego zaangażowania usługodawcy. Widać to również w przypadku zamówień publicznych, w których dochodzi do dostawy produktów chmurowych.
Uwaga 3: Rekomendujemy dokonaniu ujednolicenia pojęć związanych z chmurą obliczeniową w uksc, ustawie o informatyzacji, Rozporządzeniu Krajowe Ramy Informatyzacji oraz uchwale WIIP, a także innych aktach prawnych takich jak ustawa o obszarach morskich Rzeczpospolitej (patrz art. 2 projektu uksc). Będzie to dotyczyło także kolejnych planowanych aktów prawnych oraz rekomendacji jak np. ustawa wdrażająca dyrektywę CER, nadchodzące wdrożenia Data Act i AI Act, czy oczekiwane zmiany w komunikacie chmurowym KNF.

8. Definicja dostawcy usługi ośrodka przetwarzania danych (art. 2 pkt 4g)

Uwaga 1: definicja w Dyrektywie NIS2 mówi o usłudze ośrodka przetwarzania danych, a nie o dostawcy. Proponujemy pozostawienie tego jak najbliżej wersji oryginalnej.
Uwaga 2: Proponujemy określenie „centrum przetwarzania danych", które przyjęło się już w nomenklaturze, np. ustawa dot. budowy Krajowego Centrum Przetwarzania Danych
Uwaga 3: Definicja w projekcie posługuje się pojęciem „scentralizowanego hostingu", które nigdzie nie jest zdefiniowane. Czy to oznacza, ze prawodawca świadomie ogranicza działanie uksc tylko do tych podmiotów, które świadczą usługę „scentralizowanego hostingu", a nie dotyczy to wszelkich innych form wykorzystywania centrów przetwarzania danych?

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

9. **Definicje dostawcy usług zarządzanych i dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa (art. 2 pkt 4h oraz 4i)**

Czy każde przedsiębiorstwo świadczące usługi supportu technicznego (także darmowe) staje się dostawcą usług zarządzanych, a jeśli w jakikolwiek sposób taka usługa dotyczy elementów związanych z cyberbezpieczeństwem to staje się dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa?
Jak działa ustawa w sytuacji kiedy taki support techniczny jest outsourcowany do podmiotu trzeciego? Czy to oznacza, że podmiot trzeci powinien być uświadomiony przez dostawcę produktu ICT, że staje się dostawcą usług zarządzanych?
Jak działa ustawa jeśli podmiot świadczący usługi supportu technicznego jest podmiotem zagranicznym? W przypadku szczególnym, np. wsparcia technicznego na najwyższym poziomie, takiego supportu mogą udzielać osoby spoza Unii Europejskiej.
Definicje te stają się szczególnie istotne w świetle art. 8h, jeśli dostawca produktu ICT lub usługi ICT dla podmiotu kluczowego/ważnego także jest podmiotem kluczowym/ważnym. W szczególności zapisy umów suportowych mogą wykluczać niektóre działania obu stron, które zostały zapisane w art. 8h

10. **Definicja incydentu, incydentu poważnego oraz potencjalnego zdarzenia dla cyberbezpieczeństwa (art. 2 odpowiednio pkt. 5, 7, 8 oraz 11e)**

Rekomendujemy pozostanie przy definicjach takich jak zapisane w Dyrektywie NIS2. Przykład: definicja „potencjalnego zdarzenia w cyberbezpieczeństwie" użyta w projekcie niewiele odbiega od definicji incydentu. Czy taki zabieg był celowy? Proponujemy powrót do definicji z Dyrektywy: „potencjalne zdarzenie dla cyberbezpieczeństwa" oznacza zdarzenie, które mogło naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, któremu udało się jednak zapobiec lub które jednak nie wystąpiło;

11. **Definicja podatności (art. 2 pkt 11)**

Proponowana definicja jest wierną kopią zapisu Dyrektywy NIS2. Mając jednak na uwadze definicję procesu ICT jaka jest przeniesiona do NIS2 z ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881 („proces ICT" oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;) rekomendujemy poszerzenie jej także o procesy ICT.
Przykładem takiego procesu może być nadzór nad procesem uczenia się modeli sztucznej inteligencji i w efekcie podatność wykorzystywanego systemu.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

12. Definicja podmiotu krytycznego (art. 2 pkt 11c)

Definicja powinna być tożsama/zgodna z definicją przyjętą w nieznanym nam projekcie ustawy o zarządzaniu kryzysowym, infrastrukturze krytycznej i podmiotach krytycznych (transpozycji dyrektywy CER)

13. Definicje przedsiębiorcy komunikacji elektronicznej i przedsiębiorcy telekomunikacyjnego (art. 2 pkt 11f i 11g)

Postulujemy tożsamość definicji z aktualnie procedowany Prawem Komunikacji Elektronicznej.

14. Definicja systemu informacyjnego (art. 2 pkt 14)

Rekomendujemy przygotowanie jednej i jednolitej definicji systemu informacyjnego i wykorzystanie jej we wszystkich ustawach (patrz uwaga nr 2). To oznacza oczywiście także m.in. nowelizację definicji systemu teleinformatycznego w ustawie o informatyzacji, z której wykorzystano definicję w aktualnym projekcie.

15. Uwzględnienie European Health Data Spaces (art. 8i)

Podobnie jak wymieniona w tym artykule DORA dla sektora finansowego należy uwzględnić European Health Data Spaces dla sektora ochrony zdrowia.

16. Uwzględnienie różnych modeli przetwarzania (art.10)

Obecne zapisy pasują wyłącznie do opisu infrastruktury własnej.
Istnieją co najmniej dwa możliwe rozwiązania dla opisu innych modeli przetwarzania.

- Opis wymagań dla poszczególnych modeli przetwarzania (outsourcing, hosting, kolokacja, chmura obliczeniowa, przetwarzanie w infrastrukturze innego podmiotu np. w grupie itd. itp. w tym modele, których jeszcze nie znamy)
- Zapis, że w przypadku przetwarzania poza infrastrukturą własną przetwarzanie może być wykonane tylko w infrastrukturze podmiotu, który także jest podmiotem kluczowym/ważnym

Brak takich zapisów będzie skutkował tworzeniem wielu bardzo rozbudowanych i często niezbyt sensownych wariantów zapytań do podmiotów, u których może być wykonywane przetwarzanie. Rekomendujemy zatem drugie, proste rozwiązanie. Propozycja:
Art. 10. Ust. 8. W przypadku systemu informacyjnego wykorzystywanego do świadczenia usługi i wykorzystującego produkty ICT, procesy ICT lub usługi ICT podmiotów trzecich wymagane jest aby były one podmiotami kluczowymi lub podmiotami ważnymi.

17. Przekazywanie tajemnic prawnie strzeżonych (art. 13 pkt 3)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Wydaje się, że prosty zapis w art. 13 pkt 3. jest jednak niewystarczający. Byłby wystarczający jeśli system S46 spełniał wymagania związane ze wszelkimi rodzajami tajemnic prawnie strzeżonych. Proponujemy następujący zapis:

> *3. Wszelkie informacje prawnie strzeżone przekazywane przez podmiot kluczowy i podmiot ważny są przekazywane zgodnie z obowiązującymi przepisami.*

18. **Przekazywanie rekomendacji (art. 33 ust. 4c oraz ust. 5)**

Postulujemy by informacje o wydaniu, zmianie lub – w szczególności! – odwołaniu rekomendacji były nie tylko publikowane na stronie podmiotowej w Biuletynie Informacji Publicznej, ale były wysyłane do wszystkich podmiotów kluczowych i ważnych. Należy rozważyć czy system S46 byłby właściwym narzędziem do takiej komunikacji.
Ust. 5 powinien być odpowiednio zmieniony (w tym przypadku: nie ulegałby zmianie)

19. **Zwracanie się o dokumentację do producenta produktów ICT, usług ICT lub procesów ICT (art. 33 ust.9)**

Zapis jest skuteczny wyłącznie w przypadku kiedy znany jest kontakt z producentem, odpowiednio produktów, usług lub procesów ICT, oraz ma on świadomość istnienia procedur zapisanych w art. 33 i art. 53c oraz sankcji zapisanych w art. 73. Kontakt taki będzie dodatkowo utrudniony jeśli korespondencja będzie odbywała się w języku innym niż polski.
Wydaje się konieczna taka modyfikacja ust. 9 aby uwzględniała ona możliwość skutecznego pozyskania dokumentacji od producenta jeśli nie ma on swojej siedziby, ani przedstawiciela w Polsce z zapewnieniem współpracy międzynarodowej.
Por. art. 67b ust. 8

20. **Współpraca z innymi organami państwa (art. 34)**

Postulujemy o usunięcie z powodu oczywistości opisywanego przypadku lub zmianę i uproszczenie tego artykułu do postaci:

> *Art. 34 [współpraca z innymi organami państwa]*
> *CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe współpracują z organami państwa przy realizacji ustawowych zadań tych organów.*

21. **Obowiązki dostawców usług zarządzanych w zakresie cyberbezpieczeństwa (art. 34)**

Postulujemy o wykreślenie w zapisach tego artykułu obowiązku nakładanego na dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, zwłaszcza, że definicja takich dostawców nie jest całkowicie jasna (patrz: uwaga 9 powyżej).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

22. Przewodniczenie zespołowi (art. 36 ust. 3)

Wydaje się, że należy zachować dotychczasowy zapis, który oddaje przewodnictwo Zepołu w ręce Dyrektora Rządowego Centrum Bezpieczeństwa, z zastrzeżeniem że dla obsługi incydentów krytycznych obejmujących wyłącznie ochronę teleinformatyczną może on przekazać w konkretnej sprawie przekazać kierownictwo w ręce Pełnomocnika.
Nowe brzmienie wyglądałoby następująco:

> *3. Dyrektor Rządowego Centrum BezpieczeństwaPełnomocnik Rządu do Spraw Cyberbezpieczeństwa przewodniczy pracom Zespołu. W przypadku incydentu krytycznego nie związanego z innymi obszarami ochrony może przekazać przewodnictwo Pełnomocnikowi.*

Uzasadnienie: Dyrektywa CER wprost odsyła bezpieczeństwo teleinformatyczne do Dyrektywy NIS2, stąd przeniesienie przewodniczenie zespołowi w ręce Pełnomocnika wygląda w pierwszym momencie na prawidłowe. Jednak mając na uwadze, że incydenty teleinformatyczne mogą być fragmentem większego ataku hybrydowego lub cyfrowy atak może dotyczyć innych obszarów ochrony (personalnej, technicznej, ciągłości działania itd.), które są obecnie także bardzo zdigitalizowane należy pozostać przy aktualnym zakresie odpowiedzialności. Podobnie w przypadku działań dezinformacyjnych, które mogą nie odpowiadać przecież definicji incydentu opisanego w uksc lub Dyrektywie NIS2.

23. Współpraca międzynarodowa CSIRT sektorowych (art. 44)

Brakuje wskazania potrzeby współpracy z podobnymi CSIRT sektorowymi w innych krajach. Takie zadanie – ogromnie ważne w konkretnym sektorze – powinno znaleźć się jako wprost zapisane w ustawie.
Korzystanie z okrężnej drogi przez Pojedynczy Punkt Kontatkowy może wydłużać proces komunikacji.

24. Zadania ministra właściwego ds. informatyzacji (art. 45 p. 9)

Wydaje się, że zapis tego punktu wymaga przeredagowania w zgodzie z zapisami projektu nowej ustawy o zarządzaniu kryzysowym, infrastrukturze krytycznej i podmiotach krytycznych. Nie powinno być żadnych wątpliwości co do rozdziału kompetencji. Patrz także uwaga dot. art. 36 ust. 3

25. Minimalne wymagania dla korzystania z systemu S46 (art. 46 ust. 6 i 7)

Postulujemy prostszy zapis i sprowadzenie dwóch punktów do jednego:
6) Podmioty kluczowe i podmioty ważne korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, przy wypełnieniu minimalnych wymagań technicznych i funkcjonalnych, w ciągu

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

3 miesięcy od opublikowania tych wymagań w Biuletynie Informacji Publicznej ministra właściwego ds. informatyzacji.

26. Sposób prowadzenia nadzoru (art. 53d)

Uważamy, że zapisy art. 53d nie przystają do reguł bezpieczeństwa i cyberbezpieczeństwa, wyglądają zaś jak zapisy uprawnień służby specjalnej, której zadaniem jest działanie w przypadku poważnego zagrożenia funkcjonowania państwa, a nie prowadzenia kontroli.
Dodatkowo – o czym wspominaliśmy wcześniej w uwadze poświęconej różnym modelom przetwarzania danych stosowanych przez podmioty kluczowe i ważne – taka kontrola będzie także stanowiła bezpośrednią ingerencję w przetwarzanie podmiotów i usług nie będących przedmiotem kontroli. Czy w takim przypadku organ właściwy delegujący urzędnika monitorującego bierze odpowiedzialność, w tym odpowiedzialność finansową, za wszelkie problemy (w tym incydenty w rozumieniu uksc), wynikające z działań tego urzędnika? Na przykład wynikające z udokumentowanej niefrasobliwości lub niewiedzy podczas „oględzin urządzeń, nośników oraz systemów informacyjnych”? Co oczywiście będzie potwierdzone protokołem, o którym mowa w art. 58.
Proponujemy dalszą dyskusję nad zapisem tego punktu, którego celem – jak nam się wydaje – ma być podnoszenie poziomu cyberbezpieczeństwa, a nie łapanka winnych niedociągnięć.

27. Stanowisko co do dostawcy wysokiego ryzyka (art. 67b ust. 9)

Wskazana została Izba Gospodarcza jako strona, która przedstawia stanowisko co do dostawcy. Członkostwo w samorządzie gospodarczym nie jest w Polsce obowiązkowe, choć oczywiście jest odpłatne, stąd potrzeba rozszerzenia katalogu podmiotów, które mogą przedstawiać takie stanowiska.
Postulujemy, abu podmiot składający takie stanowisko powinien ujawnić ministrowie właściwemu ds. informatyzacji wszelkie przychody jakie otrzymał od dostawcy w ciągu ostatnich trzech lat. Informacja ta stanowi tajemnicę handlową.
Postulujemy by warunek ujawnienia relacji pomiędzy dostawcą a podmiotem powinien pojawić się w zapisach ustawy.

28. Czas korzystania produktów, usług i procesów ICT od dostawców wysokiego ryzyka (art. 67c ust. 1 oraz ust. 5)

Postulujemy skrócenie czasu zapisanego w punkcie 2) do 5 lat.
Zapis taki realizuję potrzebę utrzymania tych produktów, usług lub procesów, które podlegają wymaganiom okresu trwałości wynikających z zasad postępowania przy zamówieniach publicznych. Utrzymywanie w systemach mających znaczenie dla cyberbezpieczeństwa sprzętu lub oprogramowania przez 7 lat samo w sobie nosi znamiona podnoszenia ryzyka.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

29. Polecenie zabezpieczające a stopnie alarmowe CRP

Wydaje się zasadne by w sytuacji wystąpienia incydentu krytycznego była również możliwość zmiany stopnia alarmowego CRP (ustawa o działaniach antyterrorystycznych, art. 15 ust. 2, art. 16 ust. 2 Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (sejm.gov.pl))
Patrz także uwagę dotyczącą niezbędnej nowelizacji ustawy o działaniach antyterrorystycznych.

30. Sposób powiadamiania w przypadku incydentu krytycznego skutkującego poleceniem zabezpieczającym (art. 67g ust. 4)

Jeśli wystąpi incydent krytyczny to proponowane w projekcie rozwiązanie polegające na publikowaniu informacji na stronie Biuletynu Informacji Publicznej należy uznać za dalece niewystarczające. W tym przypadku jednak należy użyć zarówno metody push (np. wysłanie wiadomości przez system S46, wysłanie SMSem wiadomości do właściwych osób o pojawieniu się polecenia zabezpieczającego, itd.), jak i metody pull (wprowadzenie polecenia na BIP).

31. Podział kompetencji (art. 67g ust. 7 i ust. 8 oraz art. 35)

Zgodnie z art. 35 ust. 1 Dyrektor Rządowego Centrum Bezpieczeństwa jest tylko informowany o incydencie krytycznym. O jego obecności w Zespole do spraw Incydentów Krytycznych nic nie mówi ust. 3. W zasadzie działanie od Dyrektora jest oczekiwane jeśli pojawi się wniosek o zwołanie Rządowego Zespołu Zarządzania Kryzysowego, co jest tylko opcjonalne (patrz art. 35 ust. 2 punkt 2).
Zapisy art. 67g ust. 7 i ust. 8 powinny być zatem zrewidowane pod kątem zapisu kompetencji właściwych organów.

32. Obowiązek określonego zachowania (art. 67g ust. 10)

Proponujemy zmianę w zapisie ust. 10
Jest: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:"
Propozycja: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, może być m.in.:"
Uzasadnienie: dla różnych poleceń zabezpieczających mogą być różne zakresy działań. Proponowany zapis pozwala na kształtowanie wymaganych zachowań wskazując jednocześnie na podstawową listę oczekiwanych zachowań.
Jednocześnie:
Postulujemy dodanie do listy nakazów obowiązku przygotowania odpowiednich kopii bezpieczeństwa (backupów) dla wszystkich podmiotów kluczowych i ważnych.
Postulujemy dodanie do listy nakazów dla podmiotów krytycznych przygotowanie do ewakuacji do chmury obliczeniowej, zgodnie z przygotowanym planem ochrony. Por. Narodowy Program Ochrony Infrastruktury Krytycznej, załącznik Nr 1.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

33. Sposób doręczenia polecenia zabezpieczającego (art. 67g ust. 16)

Postulujemy zrewidowanie tego zapisu tak aby wszystkie podmioty kluczowe i ważne były odpowiednio szybko powiadomione, zwłaszcza że ust. 14 mówi o natychmiastowej wykonalności. Por. uwagę dot. art. 67g ust. 4 powyżej.

34. Rodzaje krytycznej infrastruktury informatycznej (art. 72b ust. 2 punkt 6)

Wydaje się, że zapisy dotyczące infrastruktury krytycznej (także: informatycznej) powinny znaleźć się w aktach prawnych dotyczących IK, natomiast w uksc powinien znaleźć się odpowiedni odnośnik.

35. Krajowy Plan (art. 72b, 72f)

Czy Krajowy Plan, tak jak został zapisany w art. 72b jest dokumentem jawnym w całości? Mając na uwadze zapis art. 72f wydaje się, że tak, jednak czy wszystkie informacje opisane w ust. 2 powinny mieć taki charakter.

36. Nowelizacja ustawy o działaniach antyterrorystycznych

Wprowadzenie stopni alarmowych w polskim systemie prawnym jest przeniesieniem odpowiadających im stopni alarmowych NATO. Polski system dodatkowo wprowadził stopnie alarmowe dla cyberprzestrzeni (art. 15 ust. 2).
Proponowana zmiana związana jest z uwzględnieniem zapisu z kodeksu karnego (art. 269a). Ma również znaczenie dla podniesienia cyberbezpieczeństwa podmiotów kluczowych i ważnych, a także dotyczy dalszej synchronizacji z systemami NATO.
Jest:

> *Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub zagrożenie zaistnienia takiego przestępstwa.*

Propozycja

> *Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub sabotażu komputerowego, o którym mowa w art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny lub zagrożenie zaistnienia takich przestępstw.*

37. Sposób powiadamiania w przypadku incydentu krytycznego skutkującego poleceniem zabezpieczającym (art. 67g ust. 4)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Jeśli wystąpi incydent krytyczny to proponowane w projekcie rozwiązanie polegające na publikowaniu informacji na stronie Biuletynu Informacji Publicznej należy uznać za dalece niewystarczające. W tym przypadku jednak należy użyć zarówno metody push (np. wysłanie wiadomości przez system S46, wysłanie SMSem wiadomości do właściwych osób o pojawieniu się polecenia zabezpieczającego, itd.), jak i metody pull (wprowadzenie polecenia na BIP).

38. Podział kompetencji (art. 67g ust. 7 i ust. 8 oraz art. 35)

Zgodnie z art. 35 ust. 1 Dyrektor Rządowego Centrum Bezpieczeństwa jest tylko informowany o incydencie krytycznym. O jego obecności w Zespole do spraw Incydentów Krytycznych nic nie mówi ust. 3. W zasadzie działanie od Dyrektora jest oczekiwane jeśli pojawi się wniosek o zwołanie Rządowego Zespołu Zarządzania Kryzysowego, co jest tylko opcjonalne (patrz art. 35 ust. 2 punkt 2).
Zapisy art. 67g ust. 7 i ust. 8 powinny być zatem zrewidowane pod kątem zapisu kompetencji właściwych organów.

39. Obowiązek określonego zachowania (art. 67g ust. 10)

Proponujemy zmianę w zapisie ust. 10
Jest: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:"
Propozycja: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, może być m.in.:"
Uzasadnienie: dla różnych poleceń zabezpieczających mogą być różne zakresy działań. Proponowany zapis pozwala na kształtowanie wymaganych zachowań wskazując jednocześnie na podstawową listę oczekiwanych zachowań.
Jednocześnie:
Postulujemy dodanie do listy nakazów obowiązku przygotowania odpowiednich kopii bezpieczeństwa (backupów) dla wszystkich podmiotów kluczowych i ważnych.
Postulujemy dodanie do listy nakazów dla podmiotów krytycznych przygotowanie do ewakuacji do chmury obliczeniowej, zgodnie z przygotowanym planem ochrony. Por. Narodowy Program Ochrony Infrastruktury Krytycznej, załącznik Nr 1.

40. Sposób doręczenia polecenia zabezpieczającego (art. 67g ust. 16)

Postulujemy zrewidowanie tego zapisu tak aby wszystkie podmioty kluczowe i ważne były odpowiednio szybko powiadomione, zwłaszcza że ust. 14 mówi o natychmiastowej wykonalności. Por. uwagę dot. art. 67g ust. 4 powyżej.

41. Rodzaje krytycznej infrastruktury informatycznej (art. 72b ust. 2 punkt 6)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Wydaje się, że zapisy dotyczące infrastruktury krytycznej (także: informatycznej) powinny znaleźć się w aktach prawnych dotyczących IK, natomiast w uksc powinien znaleźć się odpowiedni odnośnik.

42. Krajowy Plan (art. 72b, 72f)

Czy Krajowy Plan, tak jak został zapisany w art. 72b jest dokumentem jawnym w całości? Mając na uwadze zapis art. 72f wydaje się, że tak, jednak czy wszystkie informacje opisane w ust. 2 powinny mieć taki charakter.

43. Nowelizacja ustawy o działaniach antyterrorystycznych

Wprowadzenie stopni alarmowych w polskim systemie prawnym jest przeniesieniem odpowiadających im stopni alarmowych NATO. Polski system dodatkowo wprowadził stopnie alarmowe dla cyberprzestrzeni (art. 15 ust. 2).
Proponowana zmiana związana jest z uwzględnieniem zapisu z kodeksu karnego (art. 269a). Ma również znaczenie dla podniesienia cyberbezpieczeństwa podmiotów kluczowych i ważnych, a także dotyczy dalszej synchronizacji z systemami NATO.
Jest:

> *Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub zagrożenie zaistnienia takiego przestępstwa.*

Propozycja

> *Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub sabotażu komputerowego, o którym mowa w art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny lub zagrożenie zaistnienia takich przestępstw.*

KL/297/82/AM/2024

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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