[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Dotyczy: konsultacji w sprawie wzorów dokumentów i wytycznych do stosowania ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: uKSC)

Załączniki:

- KSC_Wytyczne_do_Audytów
- KSC_Dok2_Dokumentacja_Normatywna
- KSC_Dok1_Plan_Działania
- KSC_Wymagania_i_Dowody (opracowane na podstawie wytycznych ENISA)
- Analiza art. 10 uKSC versus Załącznik nr 4 do uKSC
- Zestawienia różnicowe ISO 27001:2022 / uKSC i w drugą stronę

Szanowni Państwo,

W nawiązaniu do toczących się konsultacji dotyczących wzorów i szablonów dokumentów związanych ze stosowaniem uKSC, pozwalam sobie przedstawić niniejsze stanowisko. Czynię to z pełnym poczuciem odpowiedzialności, wynikającym z blisko dwudziestoletniego doświadczenia praktycznego w obszarze cyberbezpieczeństwa, w tym jako audytor wiodący systemów zarządzania bezpieczeństwem informacji i ciągłością działania. Do niniejszego pisma dołączam dokumentację opracowaną jako materiał pomocniczy, wyrażając tym samym wolę wniesienia merytorycznego wkładu w prace konsultacyjne.

1. Kwestia standaryzacji szablonów dokumentów audytowych

W toku lutowych konsultacji środowisko audytorów, prawników oraz przedstawicieli organizacji i izb branżowych podzieliło się w swych opiniach na dwa obozy. Zwolennicy pierwszego z nich opowiadali się za opracowaniem standardowych szablonów dokumentów, ze szczególnym uwzględnieniem formularza sprawozdania z audytu. Reprezentanci drugiego stanowiska wyrażali uzasadnioną obawę, że wprowadzenie urzędowego wzoru może przynieść więcej szkody niż pożytku z punktu widzenia celów, jakim ma służyć wdrożenie uKSC.

Moje stanowisko jest jednoznaczne: publikacja szablonu dokumentacji audytowej byłaby krokiem w złym kierunku. Przekonanie to opieram na konkretnych obserwacjach z praktyki zawodowej, które pozwalam sobie poniżej przedstawić.

- **Efekt normalizacji wzoru:** doświadczenia z poprzednią wersją uKSC jednoznacznie dowodzą, że publikacja przykładowego wzoru w praktyce szybko przekształca się w stosowanie go jako wymogu bezwzględnego. Jest to nadmierne uproszczenie, które w oczywisty sposób zwalnia audytorów – zarówno wewnętrznych, jak i zewnętrznych – z konieczności krytycznego, kontekstowego myślenia. W konsekwencji wiele audytów ograniczało się do mechanicznego wypełniania formularza, a materiał dowodowy był gromadzony nie po to, by stwierdzić zgodność lub jej brak, lecz po to, by uzupełnić rubryki w szablonie.

Wdrożenia nie przyniosły wówczas spodziewanych przez ustawodawcę efektów, mimo że intencja była tożsama z obecną.

- **Ryzyko zakłócenia relacji rynkowych:** jak wynika z tabeli mapowań opartych na wytycznych ENISA, w przestrzeni europejskiej funkcjonuje wiele aktów normatywnych z zakresu cyberbezpieczeństwa. Narzucenie jednego szablonu – nawet z zastrzeżeniem jego przykładowego charakteru – może zakłócić rynkową swobodę działalności i prowadzić do trudnych do rozwiązania kolizji ze standardami stosowanymi przez podmioty z kapitałem zagranicznym, szczególnie spoza Unii Europejskiej. Cała Europa ma obowiązek implementacji Dyrektywy NIS2, co oznacza, że poszczególne organizacje, zależnie od jurysdykcji i profilu działalności, stosują różne, lecz równorzędne podejścia do zarządzania cyberbezpieczeństwem. Zunifikowanie formy dokumentacji audytowej na poziomie krajowym może skutkować podwójnymi standardami i konfliktami organizacyjnymi, nie wzmacniając przy tym realnego poziomu cyberbezpieczeństwa.

- **Atrofia kompetencji audytorskich:** posiadanie gotowego formularza zwalnia audytora z czujności i samodzielnego myślenia. Przywołuję w tym miejscu wzorzec z obszaru ISO: nawet w środowisku jednostek akredytowanych nie istnieją ujednolicone szablony raportów audytowych. Każda firma certyfikująca stosuje własne wzory, które podlegają nadzorowi akredytującego, lecz w ramach indywidualnych reguł danej organizacji. Sam standard ISO 19011 – jako fundamentalny akt normatywny regulujący zasady przeprowadzania audytów systemów zarządzania i ich dokumentowania – nie narzuca żadnych gotowych formularzy, lecz definiuje zasady i wymagania merytoryczne. Uważam, że jest to wzorzec wart naśladowania.

- **Ryzyko pogłębienia deficytu świadomości:** zasadniczym problemem cyberbezpieczeństwa w naszym kraju pozostaje niewystarczający poziom świadomości społecznej w zakresie rzeczywistych środków technicznych i organizacyjnych skutecznie chroniących organizacje. Wprowadzenie szablonu nie tylko nie przyczyni się do jej podniesienia, ale może ten stan utrwalić. Dostarczając gotowe narzędzie zamiast rozwijać kompetencje, ryzykujemy powielenie błędu, który trafnie ujmuje metafora: zamiast wędki przekazujemy rybę. Jestem przekonany, że Ministerstwo Cyfryzacji powinno na wszystkich dostępnych polach kłaść nacisk na edukację społeczeństwa. Niniejsza dyskusja jest tego przykładem i z tego względu oceniam ją jako cenną.

Rekomendacja: *zamiast szablonów sugeruję opracowanie i opublikowanie na stronach Ministerstwa Cyfryzacji zestawu wytycznych do stosowania uKSC w formie mapy drogowej (roadmap) opisującej oczekiwane działania i ich skutki. Takie podejście poszerzy wiedzę osób odpowiedzialnych za systemy cyberbezpieczeństwa, nie zakłóci relacji rynkowych i będzie spójne z mapowaniami międzynarodowymi. Wytyczne powinny być zarówno na poziomie obowiązków jak również na poziomie dokumentacji czy informacji, które należy sprawdzić przy audycie. Całą dokumentację z prac moich i mojego zespołu przedkładam w załączeniu do dalszego procedowania przez specjalistów z Ministerstwa Cyfryzacji.*

2. Relacja między normą ISO 27001:2022 a ustawą o KSC

W załączeniu do niniejszego pisma przekazuję dwa zestawienia różnicowe pomiędzy normą ISO 27001:2022 a uKSC. Pozwalam sobie zaproponować następującą konkluzję, którą – jak sądzę – potwierdzą Państwo po zapoznaniu się z tymi materiałami.

ISO 27001 jest aktem normatywnym w wymiarze techniczno-zarządczym znacząco szerszym niż uKSC, jednak nie pokrywa wszystkich jej wymagań. Można zatem przyjąć, że podmioty certyfikowane przez jednostki akredytowane w zakresie ISO 27001 spełniają co do zasady wymagania ustawy, pod warunkiem uzupełnienia procesu nadzoru audytowego certyfikacji o dodatkowe zaświadczenie obejmujące wymagania uKSC, które nie znajdują swojego odpowiednika w normie. Sama certyfikacja ISO 27001 nie wypełnia w stu procentach obowiązków ustawowych.

Uważam, że tę kwestię warto doprecyzować w oficjalnych wytycznych, albowiem jej właściwe rozstrzygnięcie mogłoby istotnie usprawnić i odformalizować procesy weryfikacji zgodności podmiotów już certyfikowanych choćby w obowiązku przedkładania obowiązkowych audytów.

3. Rozbieżność między art. 10 uKSC a zakresem Załącznika nr 4 – potrzeba doprecyzowania

W toku analizy przepisów uKSC zidentyfikowałem rozbieżność, którą oceniam jako istotną i wymagającą pilnego doprecyzowania. Dotyczy ona podmiotów ważnych będących podmiotami publicznymi, które – stosownie do art. 8 ust. 3 uKSC – nie stosują art. 8 ust. 1, lecz budują SZBI w oparciu o wymagania Załącznika nr 4. Jednocześnie obowiązki dokumentacyjne określone w art. 10 stosują się do wszystkich podmiotów ważnych bez wyjątku.

Kwestia pierwsza – szacowanie ryzyka i plan postępowania z ryzykiem (art. 10 ust. 3 pkt 2 lit. c i d):

Przepisy art. 10 ust. 3 pkt 2 lit. c (szacowanie ryzyka dla obiektów infrastruktury) oraz lit. d (plan postępowania z ryzykiem) stanowią niezależne obowiązki dokumentacyjne stosujące się do wszystkich podmiotów ważnych. Tymczasem Załącznik nr 4 nie zawiera wymogu formalnego szacowania ryzyka ani opracowania planu postępowania z ryzykiem. Podmiot publiczny jest zatem zobowiązany do posiadania i utrzymywania dokumentacji szacowania ryzyka w rozumieniu art. 10, choć jego SZBI – oparty na Załączniku nr 4 – nie przewiduje stosowania żadnej formalnej metodyki oceny ryzyka. Brak tej dokumentacji stanowi niezgodność z art. 10 ust. 3 pkt 2 lit. c i d, niezależnie od stopnia wypełnienia wymagań Załącznika nr 4.

W ramach sekcji pytań i odpowiedzi (Q&A) proponuję wyjaśnienie tej kwestii poprzez wskazanie, że podmioty publiczne stosujące Załącznik nr 4 powinny opracować uproszczoną matrycę ryzyka dla infrastruktury, powiązaną ze środkami technicznymi i organizacyjnymi wdrożonymi stosownie do § I Załącznika nr 4. Takie podejście wypełni wymaganie art. 10 przy zachowaniu zasady proporcjonalności.

Kwestia druga – dokumentacja systemu zarządzania ciągłością działania (art. 10 ust. 3 pkt 3):

Artykuł 10 ust. 3 pkt 3 uKSC wymaga prowadzenia dokumentacji systemu zarządzania ciągłością działania. Zakres ten obejmuje co do zasady analizę wpływu na działalność (BIA), plan ciągłości działania (BCP) oraz plan odtwarzania po awarii (DRP). Tymczasem Załącznik nr 4 § I pkt 12 nakłada na podmioty publiczne wyłącznie obowiązek przygotowania i przetestowania procedur na wypadek awarii lub incydentu, nie wymagając wdrożenia pełnego systemu zarządzania ciągłością działania (BCMS).

Rozbieżność ta wymaga wyjaśnienia w oficjalnych wytycznych. Proponuję przyjąć interpretację proporcjonalną: dokumentacja systemu zarządzania ciągłością działania prowadzona przez podmiot publiczny może ograniczać się do procedur wymaganych przez

Załącznik nr 4 § I pkt 12, uzupełnionych o uproszczoną identyfikację procesów krytycznych oraz plan komunikacji kryzysowej. Rozwiązanie to pozwoli wypełnić obowiązek art. 10 ust. 3 pkt 3 bez nakładania na podmioty publiczne ciężarów wykraczających poza zakres Załącznika nr 4.

Szczegółową analizę relacji art. 10 versus Załącznik nr 4 przekazuję w osobnym załączniku.

4. Uwaga dotycząca kwalifikacji podmiotów telekomunikacyjnych jako dostawców usług DNS

Chciałbym zwrócić Państwa uwagę na zagadnienie dotyczące pkt 1.19 opublikowanego Q&A, traktującego o kwalifikacji małego przedsiębiorcy komunikacji elektronicznej świadczącego jednocześnie usługę dostępu do Internetu oraz usługę DNS.

W pełni podzielam stanowisko Unii Europejskiej oraz wyjaśnienia BEREC w zakresie, w jakim wskazują, że rekursywne serwery DNS udostępniane przez dostawcę usług internetowych wyłącznie własnym abonentom stanowią technicznie nieodłączny element usługi dostępu do Internetu i nie powinny być traktowane jako samodzielna usługa DNS. Serwer rekursywny jest bowiem konfiguracją pomocniczą, bez której usługa dostępu do sieci byłaby dla przeciętnego użytkownika niepraktyczna, lecz której działanie jest zamknięte w granicach infrastruktury danego operatora.

Inaczej rzecz się ma jednak w przypadku serwerów autorytatywnych DNS. Natura techniczna serwera autorytatywnego jest fundamentalnie odmienna: jest on źródłem wiedzy dla całego Internetu i – w odróżnieniu od serwera rekursywnego – nie może być ograniczony do określonego kręgu odbiorców bez ryzyka poważnych zakłóceń, takich jak zatruwanie pamięci DNS (DNS cache poisoning) lub fragmentaryzacja przestrzeni nazw. Rekordy przechowywane na takim serwerze (w tym rekordy A, MX, NS, CNAME) odpowiadają na zapytania serwerów rekursywnych i autorytatywnych z całego świata. Podmiot posiadający i w pełni kontrolujący – zarówno logicznie, jak i fizycznie – autorytatywny serwer DNS jest w istocie dostawcą usługi DNS w rozumieniu definicji uKSC, niezależnie od swojej wielkości jako przedsiębiorcy telekomunikacyjnego.

Na tej podstawie proponuję następujące brzmienie pkt 1.19 Q&A:

> **1.19. Czy mały przedsiębiorca komunikacji elektronicznej będący jednocześnie dostawcą usługi dostępu do Internetu oraz świadczący usługę DNS będzie podmiotem kluczowym czy podmiotem ważnym?**
>
> Co do zasady taki podmiot będzie podmiotem ważnym, **chyba że w swojej infrastrukturze, na własnej adresacji IP oraz pod pełną kontrolą – zarówno techniczną, jak i fizyczną – eksploatuje autorytatywny serwer DNS.** Dostawca usługi DNS jest podmiotem kluczowym niezależnie od wielkości podmiotu.
>
> Definicja wskazuje, że chodzi o podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych Internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych Internetu, z wyjątkiem głównych serwerów nazw. Wyjaśnienia BEREC wskazują, że rekursywne serwery DNS udostępniane przez dostawcę usług internetowych w ramach usługi dostępu do Internetu stanowią w praktyce element tej usługi – są instalowane automatycznie w momencie uruchomienia połączenia, a bez nich usługa dostępu do Internetu byłaby niepraktyczna dla przeciętnego użytkownika końcowego. **Natomiast serwer autorytatywny DNS z technicznego punktu widzenia odpowiada na zapytania serwerów z całego Internetu i nie jest elementem usługi dostępu do Internetu – jego eksploatacja stanowi odrębną, samodzielną usługę DNS.**

[redacted]

W konsekwencji: nie należy traktować małego dostawcy usługi dostępu do Internetu jako dostawcy usługi DNS, **jeżeli nie posiada on w swojej strukturze i adresacji rekursywnego serwera DNS dostępnego nieograniczonemu kręgowi odbiorców ani autorytatywnego serwera DNS.** Jeżeli natomiast podmiot ten eksploatuje autorytatywny serwer DNS w swojej infrastrukturze i sprawuje nad nim pełną kontrolę, staje się dostawcą usługi DNS, a tym samym podmiotem kluczowym niezależnie od swojej wielkości. Dostawca, który przenosi obsługę DNS autorytatywnego na zewnętrzny podmiot świadczący usługi DNS, nie nabywa statusu podmiotu kluczowego z tego tytułu. (por. BEREC Guidelines on the Implementation of the Open Internet Regulation)

Mam nadzieję, że powyższe uwagi okażą się przydatne w dalszych pracach konsultacyjnych. Jestem do dyspozycji w zakresie wszelkich pytań lub wyjaśnień dotyczących przesłanych materiałów oraz przedstawionych stanowisk.

Pozostaję z wyrazami szacunku,

[redacted]