Warszawa, 10 czerwca 2026 r.

Ministerstwo Cyfryzacji

konsultacje_cyber@cyfra.gov.pl

Dotyczy: konsultacji projektu zestawienia wymagań dokumentów normalizacyjnych

Szanowni Państwo,

Stowarzyszenie Women Go Cyber, w odpowiedzi na zaproszenie do konsultacji publicznych dotyczących zestawienia wymagań dokumentów normalizacyjnych wspierających realizację przez podmioty kluczowe i ważne obowiązków wynikających z UKSC, przekazuje poniższe uwagi i rekomendacje.

Uwagi ogólne

1. Zestawienie będące przedmiotem konsultacji koncentruje się na normach wspierających budowę systemu zarządzania bezpieczeństwem informacji. W naszej ocenie warto rozważyć szersze uwzględnienie dokumentów odnoszących się do wybranych obszarów operacyjnego cyberbezpieczeństwa (m.in. reagowanie na incydenty, Threat Intelligence, bezpieczeństwo środowisk chmurowych, bezpieczeństwo łańcucha dostaw oprogramowania, bezpieczeństwo systemów AI,).
2. Normy ujęte w zestawieniu zostały wskazane w konkretnych wydaniach (np. ISO/IEC 27001:2022), co spowoduje konieczność aktualizacji wykazu przy każdej zmianie edycji normy oraz ryzyko przejściowej niezgodności. Z tego względu rekomendujemy odwołanie się do „aktualnego wydania normy” lub dodanie klauzuli dopuszczającej stosowanie nowszych wersji standardów.
3. Ustawa definiuje podmioty kluczowe i podmioty ważne, w związku z tym zestawienie powinno również odzwierciedlać ten podział w zakresie oczekiwanego poziomu wdrożenia wymagań zgodnie z zasadą proporcjonalności. Nakładanie obowiązku pełnego wdrożenia rozbudowanych norm i frameworków na mniejsze organizacje może być niewspółmierne do skali działalności i poziomu ryzyka. Postulujemy, aby dla podmiotów ważnych o niższym

profilu ryzyka, przewidzieć katalog podstawowych wymagań, a pełne frameworki zarządzania ryzykiem pozostawić dla podmiotów kluczowych i infrastruktury krytycznej.

4. Postulujemy, aby Ministerstwo Cyfryzacji przygotowało wytyczne dotyczące stosowania zestawienia wzorowane na Q&A do UKSC oraz doprecyzowało zakres i sposób stosowania poszczególnych norm w kontekście wykazania zgodności z ustawą co pomoże uniknąć nadmiarowych lub nieproporcjonalnych wdrożeń.
5. Ministerstwo Cyfryzacji powinno jednoznacznie dopuścić korzystanie z bezpłatnych, powszechnie uznawanych frameworków oraz wytycznych, takich jak np. NIST CSF 2.0 - dokument ten został co prawda uwzględniony w zestawieniu, jednak brakuje wyraźnego rozróżnienia oraz wskazania, w jakim zakresie i dla których kategorii podmiotów jego stosowanie może zostać uznane za wystarczające dla wykazania zgodności z ustawą.

Uwagi szczegółowe

1. **Zarządzanie bezpieczeństwem łańcucha dostaw.**

   Rekomendujemy uzupełnienie zestawienia o wyspecjalizowane wytyczne dotyczące bezpieczeństwa łańcucha dostaw, takie jak NIST SP 800-161 czy normy z rodziny ISO/IEC 28000. W obecnym zestawieniu brakuje dostatecznej precyzji w zakresie oczekiwań wobec dostawców, co w praktyce może prowadzić do nadmiernych i wzajemnie powielających się działań weryfikacyjnych.

   Ponadto w obszarze bezpieczeństwa dostawców ICT i oprogramowania rekomendujemy uwzględnienie SLSA (Supply-chain Levels for Software Artifacts) oraz Software Bill of Materials (SBOM). Wymienione wyżej frameworki istotnie zwiększają przejrzystość łańcucha dostaw oprogramowania oraz wspierają szybką identyfikację podatnych komponentów wykorzystywanych przez organizacje.

2. **Bezpieczeństwo dla systemów sztucznej inteligencji.**

   Rekomendujemy włączenie do zestawienia normy ISO/IEC 23894, która zawiera wytyczne dotyczące zarządzania ryzykiem specyficznym dla systemów sztucznej inteligencji. Dodatkowo wskazujemy na zasadność uwzględnienia normy ISO/IEC 27090 po zakończeniu procesu jej opracowania i publikacji, ponieważ będzie ona odnosić się bezpośrednio do zagadnień cyberbezpieczeństwa systemów sztucznej inteligencji oraz specyficznych dla nich zagrożeń.

   Aktualnie, w obszarze sztucznej inteligencji zestawienie odwołuje się wyłącznie do normy ISO/IEC 42001, która koncentruje się na systemie zarządzania AI. W naszej ocenie, z punktu widzenia cyberbezpieczeństwa, jest to niewystarczające i wymaga uzupełnienia o standardy odnoszące się bezpośrednio do bezpieczeństwa systemów sztucznej inteligencji oraz specyficznych dla nich zagrożeń.

3. **Bezpieczeństwo środowisk chmurowych.**

Rekomendujemy uwzględnienie w zestawieniu norm ISO/IEC 27017, 27018 i CSA Cloud Controls Matrix (CCM), a także rozważenie uwzględnienia Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) jako krajowego zbioru dobrych praktyk.

W dobie rozwijającej się technologii i powszechnego korzystania z usług chmurowych dokumenty te wspierają realizację wymagań dotyczących zarządzania ryzykiem, bezpieczeństwa dostawców ICT, ochrony danych oraz bezpieczeństwa systemów funkcjonujących w modelach chmurowych.

4. **Zarządzanie podatnościami.**

   Rekomendujemy uwzględnić w zestawieniu NIST SP 800-40 – wytyczne dotyczące zarządzania podatnościami i aktualizacjami bezpieczeństwa, które są kluczowym elementem zarządzania ryzykiem cyberbezpieczeństwa.

5. **Threat Intelligence**

   Rekomendujemy rozważenie uwzględnienia uznanych wytycznych i frameworków wspierających budowę zdolności w zakresie Cyber Threat Intelligence (CTI), w szczególności NIST SP 800-150, MITRE ATT&CK oraz CTI-CMM. Dokumenty te stanowią powszechnie stosowane źródło dobrych praktyk w zakresie identyfikacji, analizy i wymiany informacji o zagrożeniach oraz wspierają budowę operacyjnych zdolności cyberbezpieczeństwa.

Mamy nadzieję, że przedstawione uwagi i rekomendacje okażą się pomocne w pracach nad przygotowaniem finalnej wersji zestawienia oraz dotyczących go wytycznych.

W naszej ocenie doprecyzowanie zakresu stosowania wskazanych dokumentów oraz uzupełnienie katalogu o wybrane standardy operacyjne znacząco zwiększy praktyczną użyteczność wykazu dla podmiotów objętych UKSC.

Z wyrazami szacunku

[redacted]

Prezeska Stowarzyszenia Women Go Cyber

W imieniu Stowarzyszenia Women Go Cyber uwagi i rekomendacje przygotowały ekspertki:

[redacted]