LEWIATAN

Warszawa, 27 czerwca 2018 r.
KL/232/103/AM/2018

Pan
Marek Zagórski
Minister Cyfryzacji

Pan
Tomasz Zdzikot
Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Szanowny Panie Ministrze,
Szanowny Panie Pełnomocniku,

W nawiązaniu do konsultacji publicznych projektów rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych oraz rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, w załączeniu przekazuję stanowisko Konfederacji Lewiatan wobec obu projektów.

Z poważaniem,

Henryka Bochniarz
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan Jacek Łosik - Kierujący Departamentem Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik:
Stanowisko Konfederacji Lewiatan wobec projektów rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych oraz rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

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 wobec projektów rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych oraz rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

I. Projekt rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

Uwaga ogólna: Konfederacja Lewiatan w swoich wcześniejszych stanowiskach wielokrotnie rekomendowała, aby w przypadkach przepisów określając wymogi lub standardy – tam gdzie jest to możliwe – stosować odwołania do najlepszych międzynarodowych praktyk, w tym wymagań norm ISO, między innymi ISO27001. Dlatego też przyjmujemy z zadowoleniem fakt, iż w przedmiotowym rozporządzeniu zastosowania takie podejście.

Uwaga dot. § 3: zgodnie z uzasadnieniem do rozporządzenia:

„W § 3 wskazany został minimalny zakres dokumentacji normatywnej, która musi być prowadzona przez operatora usługi kluczowej. Zakres tej dokumentacji mieści się w ramach dokumentacji, którą musi prowadzić operator infrastruktury krytycznej w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 oraz z 2018 r. poz. 1566).

Oznacza to, że operator usługi kluczowej, który jest jednocześnie operatorem infrastruktury krytycznej, nie musi tworzyć odrębnej dokumentacji na podstawie projektowanego rozporządzenia", **- jednakże warto byłoby jednoznacznie wskazać również w treści samego rozporządzenia (a nie tylko w uzasadnieniu) kwestie zwolnienia takiego operatora infrastruktury krytycznej z obowiązku tworzenia odrębnej dokumentacji.**

Uwaga dot. § 5 ust. 1 pkt 2: niezrozumiałe jest, czemu ma służyć określanie w dokumentacji operacyjnej *„wzoru zapisów dokumentujących wykonanie procedury"*. Nie kwestionujemy w żadnym razie zasadności dokumentowania wykonania procedury, ale uważamy, że określenie sposobu, w jaki ów cel będzie w danym systemie osiągany powinien pozostawać do decyzji podmiotu. W zależności od procedury może to być formuła o ustalonej treści, którą administrator będzie wpisywał do dziennika systemu, ale może to być również zapis w innym systemie, a także log systemowy. Przepisywanie tych ostatnich informacji do dokumentacji operacyjnej wydaje się być zbędnym i nadmiarowym formalizmem.

II. Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

Uwaga ogólna: Konfederacja w swoich wcześniejszych stanowiskach wielokrotnie rekomendowała, aby w przypadkach przepisów określając wymogi lub standardy – tam gdzie jest to możliwe –

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

stosować odwołania do najlepszych międzynarodowych praktyk, w tym wymagań norm ISO, między innymi ISO27001. Dlatego też przyjmujemy z zadowoleniem fakt, iż w przedmiotowym rozporządzeniu zastosowano takie podejście.

Uwaga dot. § 2 ust. 1 pkt. 3: wymaganie upubliczniania w języku polskim i angielskim deklaracji polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez Internet Engineering Task Force (IETF), w kontekście utrzymywania dokumentacji SZBI ISO 27001, a w ramach niej Deklaracji Stosowania SZBI (SoA -Statement of Applicability) oraz posiadania aktualnych certyfikatów ISO 27001 i 22301 uważamy za nadmiarowe i zbędne. Zgodnie z uzasadnieniem do rozporządzenia powinno zostać to uznane za dobrą praktykę, a nie wymóg wynikający z przepisów prawa. Proponujemy więc usunięcie tego zapisu.

Uwaga dot. § 3 ust. 1 pkt 5 i 6: projekt określa wymagania dotyczące zabezpieczeń technicznych pomieszczeń, których spełnienie może oznaczać poniesienie dodatkowych kosztów, a co więcej ich sformułowanie jest nieprecyzyjne. Problematyczna wydaje się kwestia braku ich doprecyzowania, bowiem w praktyce powstają pytania szczegółowe np. w zakresie „zewnętrznych drzwi wejściowych do pomieszczeń" i kwestii tego, czy poprzez zewnętrzne drzwi wejściowe do pomieszczeń należy rozumieć tylko sytuacje, kiedy pomieszczenie w którym wydzielona cześć struktury zajmująca się cyberbezpieczeństwem u danego przedsiębiorcy ma bezpośredni dostęp z zewnątrz, czy też dotyczy wszystkich przypadków.

Konfederacja Lewiatan, KL/232/103/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