LEWIATAN

Warszawa, 23 stycznia 2020 r.
KL/25/10/AM/2020

Pan
Marek Zagórski
Minister Cyfryzacji

Szanowny Panie Ministrze,

W nawiązaniu do prowadzonych przez Ministerstwo Cyfryzacji konsultacji założeń dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie (pismo resortu cyfryzacji z dnia 19 grudnia 2019 r.), przekazuję w załączeniu stanowisko Konfederacji Lewiatan.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan Robert Kośla - Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik:
Stanowisko Konfederacji Lewiatan do założeń dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie.

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 założeń dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie

Konfederacja Lewiatan z zadowoleniem przyjmuje fakt przeprowadzania przez Ministerstwo Cyfryzacji konsultacji w sprawie wdrożenia rozporządzenia UE 2019/881 ("Cybersecurity Act", dalej „rozporządzenie). Konfederacja Lewiatan popiera cel Ministerstwa Cyfryzacji, polegający na określeniu nowego modelu certyfikacji bezpieczeństwa cybernetycznego w Polsce w ramach rozporządzenia. Pozwoli to nie tylko na poprawę i harmonizację poziomu ochrony urządzeń, infrastruktury IT i usług internetowych przed zagrożeniami cybernetycznymi, ale także wzmocni poziom zaufania obywateli, organizacji publicznych i prywatnych do tych technologii.

I. Proponowany model ogólny

Ministerstwo Cyfryzacji zaleca mieszany model certyfikacji, w którym sektor publiczny i prywatny będą współpracować w celu zapewnienia przyjęcia i łatwego dostępu do certyfikatów. Konfederacja aprobuje to podejście, tym bardziej, że uznaje ono korzyści płynące z certyfikatów bezpieczeństwa również dla małych i średnich przedsiębiorstw.

II. Organy certyfikacyjne

Konfederacja wspiera analizę Ministerstwa Cyfryzacji dotyczącą jednostek certyfikujących. Uważamy, że posiadanie jednej akredytowanej jednostki certyfikującej może zwiększyć długość i koszt procesu certyfikacji, zniechęcając tym samym firmy do ubiegania się o certyfikaty bezpieczeństwa cybernetycznego. Zamiast tego, model, który jest otwarty dla wielu jednostek certyfikujących, oferowałby lepszy dostęp do certyfikacji poprzez dopuszczenie różnych ofert, które byłyby dostosowane do firm każdej wielkości. Podczas gdy polskie prawo zezwala obecnie na działalność publicznych lub prywatnych jednostek certyfikacyjnych, uważamy, że należy preferować model prywatny. Stworzy to konkurencyjny krajobraz i zachęci do innowacji pomiędzy jednostkami certyfikującymi w sposób efektywny kosztowo, z wyłączną korzyścią dla firm ubiegających się o certyfikację. Zauważyliśmy, że konsultacje nie dotyczą obecnie akredytacji jednostek certyfikujących zgodnie z rozporządzeniem (WE) nr 765/2008. Ponieważ akredytacja może mieć wpływ na dostępność certyfikatów na polskim rynku, zalecamy Ministerstwu Cyfryzacji podanie dodatkowych szczegółów na ten temat.

W odniesieniu do krajowego organu ds. certyfikacji cyberbezpieczeństwa (art. 58 rozporządzenia) w pełni zgadzamy się, że powołanie jednego organu będzie skuteczniejsze w nadzorowaniu i monitorowaniu właściwego wdrażania ustawy o bezpieczeństwie cybernetycznym. Ponadto, głos jednego organu zapewniłby jasność stanowiska Polski w dyskusjach z Europejską Agencją

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

Bezpieczeństwa Sieci i Informacji (ENISA), jak również z innymi unijnymi odpowiednikami w ramach Europejskiej Grupy ds. Certyfikacji Bezpieczeństwa Cyberprzestrzeni (ECCG).

III. Obowiązkowa certyfikacja

Konfederacja popiera strategię Ministerstwa Cyfryzacji, zgodnie z którą konieczne jest stworzenie odpowiedniego zapotrzebowania na certyfikaty. Szerokie przyjęcie certyfikatów jest jedynym środkiem gwarantującym ich sukces i osiągnięcie celów bezpieczeństwa Ministerstwa. W tym kontekście pochwalamy gotowość Ministerstwa Cyfryzacji do zachęcania do korzystania z certyfikatów bezpieczeństwa. Obawiamy się jednak, że w praktyce takie zachęty mogą prowadzić do stworzenia systemu certyfikacji, który jest obowiązkowy, a który w większości przypadków ma być dobrowolny zgodnie z wymogami rozporządzenia. Narzucenie określonych systemów certyfikacji w zamówieniach publicznych lub w ramach polityki sektorowej miałoby trwały wpływ na konkurencyjność naszych członków i ich możliwości rozwoju biznesowego. Jesteśmy równie zaniepokojeni, że plany w zakresie systemu bezpieczeństwa i obowiązkowej certyfikacji, będą miały negatywny wpływ na ciągłość funkcjonowania biznesu. Np. zaimplementowana infrastruktura zostanie poddana w wątpliwość lub lista certyfikowanych systemów będzie ograniczona, co utrudni rozwój przedsiębiorstwa. Sugerujemy, by usługi i infrastruktura chmurowa nie podlegały, z uwagi na swą specyfikę, obowiązkowej certyfikacji, z uwagi na to, że podlegają one wymogom obowiązujących międzynarodowych standardów w zakresie certyfikacji, takim jak seria ISO 27 i SOC 2.

System certyfikacji byłby postrzegany jako bariera dostępu do rynku, która będzie szkodliwa zarówno dla lokalnych przedsiębiorców, jak i dla firm zagranicznych inwestujących w Polsce.

Konfederacja uważa również, że określenie, czy certyfikacja powinna być obowiązkowa, powinno opierać się na dogłębnej analizie ryzyka związanego z wykorzystaniem produktów, usług ICT lub procesów ICT, a nie na rodzaju świadczonych usług i wielkości operatorów usług kluczowych. Podejście "uniwersalne" oparte wyłącznie na usługach i wielkości operatorów usług kluczowych nie uwzględniałoby realiów ryzyka i nakładałoby na przedsiębiorstwa znaczne obciążenia związane z certyfikacją. Kontrole narzucone przez proces certyfikacji w tym kontekście nie byłyby współmierne do ryzyka i wpłynęłyby na rentowność świadczonych usług, zmniejszyłyby liczbę usługodawców i w rezultacie doprowadziłyby do wzrostu cen.

Konfederacja twierdzi, że w przypadku niewłaściwego wykorzystania, certyfikacja może również potencjalnie zagrażać innowacjom technologicznym. O ile rozporządzenie ma uzasadniony cel, jakim jest uniknięcie fragmentaryzacji krajobrazu certyfikacji w zakresie bezpieczeństwa cybernetycznego, o tyle nie powinniśmy podważać wysiłków podejmowanych przez firmy, które zainwestowały w certyfikację odpowiadające wymogom międzynarodowych standardów bezpieczeństwa, takim jak ISO/IEC 27001 i PCI DSS. Dlatego też uważamy, że istniejące normy międzynarodowe powinny być

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

w pełni wykorzystane przed stworzeniem jakiegokolwiek nowego systemu, a wszelkie uzupełnienia lub zmiany norm międzynarodowych muszą być zharmonizowane zarówno na poziomie europejskim, jak i międzynarodowym. Jeżeli nie można wykorzystać takich standardów w sposób wyżej wskazany, należy ustanowić wzajemne uznawanie („mutual recognition") między istniejącymi systemami bezpieczeństwa a standardami międzynarodowymi.

Programy certyfikacji cyberbezpieczeństwa nie powinny mieć na celu powielania istniejącego systemu, lecz tworzenie wartości dodanej poprzez uniezależnienie z czasem systemu lokalnego od systemów i inicjatyw międzynarodowych.

IV. Nadzór i kontrola

Rozporządzenie nakłada na państwa członkowskie obowiązek ustanowienia przepisów dotyczących kar mających zastosowanie w przypadku naruszenia unijnych systemów certyfikacji w zakresie bezpieczeństwa cybernetycznego (art. 64). Rozumiemy, że niewłaściwe wykorzystanie certyfikatu powinno podlegać sankcjom, o których mowa w konsultacjach, jednak Konfederacja podkreśla, że kary powinny pozostać "proporcjonalne", a ponadto skuteczne i odstraszające. W przeciwnym razie nieproporcjonalne sankcje najprawdopodobniej zniechęcą małe i średnie przedsiębiorstwa do przeprowadzania oceny zgodności na zasadzie dobrowolności. Przyniesie to efekt przeciwny do zamierzonego, tj. stworzenia popytu na certyfikację i "osiągnięcia jak największego nasycenia rynku certyfikatami".

Konfederacja Lewiatan, KL/25/10/AM/2020

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