POLSKIE TOWARZYSTWO INFORMATYCZNE
IZBA RZECZOZNAWCÓW

Izba Rzeczoznawców PTI, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: +48 22 887 31 47, +48 22 838 47 05, e-mail: ir@pti.org.pl, www.pti.org.pl/ir

Warszawa, dn. 31.12.2021 r.

Departament Regulacji Cyfrowych
Kancelaria Prezesa Rady Ministrów
ul. Królewska 27; 00-060 Warszawa

Szanowni Państwo

Dziękujemy za skierowane do Polskiego Towarzystwa Informatycznego zapytanie dotyczące **projektu rozporządzenia Rady Ministrów w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa (RD472)**.

Poniżej przedstawiamy stanowisko **Polskiego Towarzystwa Informatycznego** do przedstawionego Projektu.

Z uwagi na bardzo krótki czas przeznaczony na przygotowanie opinii, który jednocześnie przypada na okres świąteczno-noworoczny przekazujemy niniejsze, bardzo syntetyczne i nie wyczerpujące tematu uwagi i spostrzeżenia. Jednocześnie deklarujemy dalszą współpracę przy redakcji zarówno niniejszego Rozporządzenia jak i innych regulacji prawnych z obszaru szeroko rozumianej teleinformatyki, w tym cyberbezpieczeństwa.

Po przeprowadzeniu, w ramach wewnętrznych konsultacji, analizy zapisów Załącznika do Rozporządzenia Rady Ministrów (Projekt z 27 grudnia 2021 r.) uważamy, że przy opracowywaniu wymagań co do osób realizujących zadania z zakresu cyberbezpieczeństwa popełniono w założeniach błąd metodyczny. Wykorzystywanie jedynie certyfikatów jako podstawy oceny kwalifikacji jest nieporozumieniem i niezrozumieniem złożoności kwestii związanych z cyberbezpieczeństwem. Rozwiązanie powstało jako tzw. silver bullet solution (nie ma dobrego polskiego odpowiednika – vide

https://dictionary.cambridge.org/pl/dictionary/english/silver-bullet)

Przy tworzeniu wymagań dla poszczególnych grup osób należy odwołać się przede wszystkim do doświadczeń i najlepszych praktyk światowych w zakresie kwalifikacji i kompetencji osób w IT. Proponujmy powołać się np. na "The global skills and competency framework for the digital world" (https://sfia-online.org/en).

Model, tak jak w przytoczonym przykładzie, powinien uwzględniać uwzględnia nie tyle certyfikaty (które można traktować jako uzupełnienie), ale przede wszystkim poziomy odpowiedzialności (jest ich 7) ujętych w aspekcie pięciu atrybutów:

- autonomii (samodzielności),
- wpływu (oddziaływania) na organizację i współpracowników,
- złożoności realizowanych działań,
- umiejętności biznesowych (nie tylko technicznych),
- wiedzy

odniesionych do określonych czynników behawioralnych (zachowań).

Oznaczałoby to konieczność stworzenia modeli wymagań (są określone ramy w SFIA) oraz ich utrzymywanie. Wtedy też należałoby odnieść się do innych czynników umożliwiających

(vide COBIT) pozwalających na uzyskanie skuteczności podejmowanych działań, a nie jedynie posiadania pliku certyfikatów.

Warto uwzględnić również e-CF (E-COMPETENCE FRAMEWORK), która jest również polską normą „okładkową" (https://www.pkn.pl/informacje/2020/01/nowa-norma-europejska-dotyczaca-e-kompetencji) PN-EN 16234-1.

W Rozporządzeniu nie mówi się o wymogach formalnych dotyczących wykształcenia osób realizujących poszczególne grupy zadań.

W Rozporządzeniu nie są sprecyzowane sposoby weryfikacji (poza faktem posiadania certyfikatów) posiadania specjalistycznej wiedzy oraz doświadczenia zawodowego w zakresie cyberbezpieczeństwa.

Stwierdzenie z Uzasadnienia, że ***„...do grup o najwyższych kwotach zostały przyporządkowane*** *najważniejsze zadania z zakresu cyberbezpieczeństwa, takie jak: ocena bezpieczeństwa systemów IT – w tym testy penetracyjne i audyty bezpieczeństwa, analizowanie szkodliwego oprogramowania, czy też* ***kierowanie jednostką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa***" jest nie do końca słuszne. O sile zespołu cyberbezpieczeństwa decydują w dużej mierze eksperci i kierownicy średniego szczebla.

W obecnym kształcie Rozporządzenia uzyskanie efektu podanego w Uzasadnieniu: "... *zwiększające zarobki pracowników administracji publicznej, zajmujących się cyberbezpieczeństwem, do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym*" jest mało realne z uwagi na niejasność kryteriów oceny kwalifikacji oraz całkowitą uznaniowość wysokości świadczeń, których minimum jest jednolite dla wszystkich.

Rozporządzenie nie precyzuje sposobu weryfikacji/potwierdzenia wiedzy specjalistycznej osób realizujących szczegółowe zadania z zakresu cyberbezpieczeństwa. Z jednej strony dziesiątki certyfikatów (pozycja 1 to 42 szt.) bez podania w jakiej konfiguracji miałyby być rozpatrywane – łącznie czy wystarczy 1, 3, 8 lub którykolwiek? Z drugiej ustawa przewiduje możliwość przeprowadzenia bliżej nie zdefiniowanego, subiektywnego „sprawdzianu". Z punktu widzenia procedury certyfikacyjnej to jest nierówne, niemierzalne i nieprecyzyjne.

Deklarujemy udział Polskiego Towarzystwa Informatycznego, w opracowaniu właściwych, adekwatnych do aktualnej sytuacji rynkowej, zapisów dotyczących zadań z zakresu cyberbezpieczeństwa oraz doświadczenia zawodowego oraz (!) posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa osób realizujących w administracji państwowej zadania z zakresu cyberbezpieczeństwa.

Polskie Towarzystwo Informatyczne to najstarsza polska organizacja z branży IT; organizacja zrzeszająca ponad 1000 informatyków pracujących w administracji publicznej, środowiskach akademickich i biznesowych w całej Polsce. W ramach działalności statutowej Polskie Towarzystwo Informatyczne wypowiada się w imieniu skupionego wokół niego środowiska w najistotniejszych kwestiach związanych z informatyzacją, bierze aktywny udział w procesach legislacyjnych, prowadzi działalność certyfikacyjną oraz rzeczoznawczą. Działa również na rzecz zwiększenia ogólnych umiejętności cyfrowych w społeczeństwie.

Z poważaniem

Elektronicznie podpisany przez Tomasz Szatkowski
Data: 2021.12.31 13:55:26 +01'00'

Tomasz Szatkowski

Dyrektor Izby Rzeczoznawców

Polskie Towarzystwo Informatyczne