OPINIA
Polskiej Izby Informatyki i Telekomunikacji [PIIT] w sprawie założeń dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie

W odpowiedzi na zaproszenie do udziału w konsultacjach dot. Modelu systemu certyfikacji cyberbezpieczeństwa w Polsce - założenia dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie, PIIT poniżej przedstawia swoją opinię z prośbą o jej uwzględnienie w dalszych pracach Ministerstwa.

W pierwszej kolejności potwierdzić należy znaczenie certyfikacji cyberbezpieczeństwa dla ogólnego poziomu zaufania dla usług, produktów i procesów ICT, zarówno w ujęciu krajowym, unijnym, jak i globalnym. Polska, jako uczestnik kreującego się obecnie europejskiego modelu certyfikacji powinna być aktywnym uczestnikiem dyskusji na poziomie UE, co jest szczególnie istotne na etapie opracowywania pierwszego unijnego kroczącego programu prac, którego publikację przewidziano do 28 czerwca 2020 r. Tym samym, uruchomione w Ministerstwie Cyfryzacji prace Zespołu ds. Certyfikacji uważamy za istotne i deklarujemy udział w jego dalszych pracach.

Odnosząc się natomiast bezpośrednio do przedstawionych założeń, należy wskazać, że pozostają one na znaczącym poziomie ogólności. Tym samym, uważamy, że debata nad ich doprecyzowaniem powinna być kontynuowana w ramach prac wzmiankowanego Zespołu ds. Cyberbezpieczeństwa. Efektem prac powinno być przedstawienie finalnego modelu certyfikacji w Polsce oraz korespondujących z nim założeń projektu ustawy dostosowującej w niezbędnym zakresie przepisy krajowe do potrzeby wykonywania postanowień *Cybersecurity act* („CSA").

1. Model certyfikacji

Na poparcie zasługuje ogólny postulat, aby przyjęty został model mieszany, w którym zakładana jest współpraca sektora publicznego i prywatnego. Dalszych prac wymaga jednak określenie ram tej współpracy, również w kontekście możliwego do zidentyfikowania katalogu schematów certyfikacji europejskiej, które zgodnie z przepisami CSA, mogą być z jednej strony dobrowolne lub obligatoryjne (po ich wprowadzeniu w przepisach prawa), a z drugiej w zależności od certyfikowanej materii mogą zostać zastrzeżone do wyłącznej właściwości jednostek publicznych lub otwarte także dla jednostek prywatnych. W tym kontekście kluczowe będzie proporcjonalne i wynikające z oceny ryzyk określenie, jaki status będzie posiadał dany schemat pomocowy, tak, aby nie dochodziło do sytuacji, w której znaczna większość procesów certyfikacyjnych musiałaby być prowadzana wyłącznie przez jednostki publiczne. Faktyczne ramy „mieszanego" modelu, bazującego na współpracy różnych podmiotów będą więc ściśle skorelowane ze zidentyfikowanymi do certyfikacji usługami, produktami i procesami ICT oraz przypisanemu im znaczeniu.

Koszty certyfikacji

W zakresie kosztów certyfikacji wskazano, że laboratoria powinny działać na zasadach rynkowych, a ceny powinny być kształtowane przez rynek. Zasadniczo należy poprzeć taki wniosek, przy czym kluczowe będzie monitorowanie tego tworzącego się dopiero rynku. W przypadku funkcjonowania na rynku większej ilości podmiotów faktycznie istnieje szansa na kształtowanie cen w oparciu o mechanizmy konkurencyjne. Natomiast w przypadku w którym funkcjonowałby naturalny monopol

publicznej jednostki certyfikującej dla niektórych schematów certyfikacji, kwestia proporcjonalnego określania cen będzie kluczowa z punktu widzenia podmiotów zobowiązanych do poddawania jej swoich produktów, usług i procesów. Podobnie będzie w przypadku jednostek prywatnych, szczególnie w odniesieniu do schematów obowiązkowych oraz pierwszego okresu, w którym struktura rynku jednostek certyfikujących dopiero będzie budowana.

Tym samym, w naszej ocenie krajowy organ ds. certyfikacji cyberbezpieczeństwa powinien w ramach swojej działalności monitorować rozwój sytuacji na rynku certyfikacji, w tym w zakresie cen, w celu ograniczenia ryzyka zbyt wysokich kosztów certyfikacji dla podmiotów obowiązanych do jej prowadzenia.

Wnioskujemy ponadto o uznanie międzynarodowych standardów opartych o światowe normy takie jak np. Common Criteria (norma ISO 15408), tak aby nie było konieczności wykonywania powtórzonych badań. Może to w znaczony sposób skrócić i usprawnić wnioskowane działania w Polsce .

2. Podmioty w systemie certyfikacji

Jak już wskazaliśmy, popieramy model bazujący na współistnieniu jednostek certyfikujących publicznych i prywatnych, przy założeniu jednak racjonalnego podziału zadań i braku tendencji do zbytniej ekspansji działalności jednostek publicznych. Potencjał do organizacji jednostek certyfikujących przez rynek prywatny powinien być wykorzystany w możliwie szerokim stopniu, przede wszystkim, aby zapewnić podmiotom obowiązanym do dokonania certyfikacji możliwość jej przeprowadzenia w możliwie krótkich terminach i w cenach wynikających z gry rynkowej. Zbytnia koncentracja zadań w jednostkach publicznych może skutkować zbyt długim (i negatywnie wpływającym na innowacyjność) czasem koniecznym do uzyskania certyfikacji. Byłoby to szczególnie uciążliwe w przypadku wskazania w danym schemacie certyfikacji warunków dla utrzymania certyfikacji np. dla przypadków aktualizacji oprogramowania w pierwotnie certyfikowanym produkcie.

Z drugiej strony, z perspektywy administracji publicznej, budowa silnych kompetencji certyfikacyjnych wśród podmiotów prywatnych w Polsce, powinna być również postrzegana, jako potencjał do budowy nowego rynku w sektorze technologii informacyjnych i komunikacyjnych. Taki rynek, w zależności także od rozwoju sytuacji w innych krajach członkowskich UE, mógłby adresować potrzeby nie tylko przedsiębiorstw krajowych, ale potencjalnie także z innych krajów naszego regionu. W tym kontekście, warte rozważenia są proaktywne działania służące wsparciu budowy nowej krajowej specjalizacji w zakresie certyfikacji cyberbezpieczeństwa, w tym poprzez tworzenie odpowiedniego otoczenia prawnego, jak i możliwości uzyskania wsparcia na rozwój działalności certyfikacyjnej.

Popieramy propozycję, aby struktura krajowego organu ds. certyfikacji cyberbezpieczeństwa została zorganizowana przy ministrze właściwym ds. informatyzacji.

3. Certyfikacja obowiązkowa

W pierwszej kolejności, kluczowe wydaje się rozstrzygnięcie kwestii niezaadresowanej w opublikowanych założeniach systemu certyfikacji tj. ustalenia czy działalność krajowych jednostek certyfikujących będzie bazowała wyłącznie na schematach unijnych, czy planowane jest także przyjmowanie także schematów krajowych w obszarach nieobjętych certyfikacją unijną. W naszej ocenie w pierwszej kolejności należy bazować na certyfikacji harmonizowanej na poziomie unijnym, a w przypadku identyfikacji nowych istotnych obszarów, w ramach współpracy na poziomie unijnym

określać nowe zakresy podlegające certyfikacji. W tym ujęciu ewentualne przygotowanie schematów krajowych obligatoryjnych do stosowania powinno być ograniczone i dopuszczalne jedynie w przypadku identyfikacji potrzeb specyficznych dla uwarunkowań polskich.

W zakresie ustalania, które schematy certyfikacji powinny zostać uznane za obowiązkowe kluczowe powinny być czynniki merytoryczne, ocena ryzyka oraz proporcjonalność, a nie jedynie cel w postaci osiągnięcia wysokiego nasycenia rynku certyfikatami. Jako obligatoryjne na poziomie krajowym powinny być jednocześnie przyjmowane jedynie te schematy certyfikacji, które za takie uznane zostały w innych krajach unijnych.

Zakres i katalog usług, produktów i procesów ICT, które mogłyby zostać objęte schematami certyfikacji, w szczególności obligatoryjnej powinien zostać ustalony w toku dalszych prac roboczych z uwzględnieniem wszystkimi zainteresowanych stron, a w szczególności przedstawicieli sektorów, które mogłyby zostać objęte nowymi obowiązkami.

Ważnym jest określenie grup sprzętu oraz poziomu certyfikacji, który powinien zostać zaimplementowany. Które z urządzeń lub systemów winny być poddane temu procesowi np. w certyfikacji opartej o Comman Crieria jaki poziom EAL.

Jednocześnie PIIT pragnie się podzielić kilkoma wątpliwościami na kanwie opiniowanego dokumentu, które nasunęły się w trakcie przygotowywania naszej opinii:

- Czy system certyfikacji będzie podlegał unijnym wymaganiom w zakresie akredytacji i nadzoru, określonym w rozporządzeniu PE nr 765/2008 i stąd jednostka certyfikująca powinna posiadać akredytację PCA lub innego ciała - odpowiednika w państwie członkowskim, co w konsekwencji daje uznawalność takiego certyfikatu w całej UE? Jeżeli nie, to jaka będzie wzajemna uznawalność certyfikacji wydanych w poszczególnych państwach? Czy to jest określone w odrębnych przepisach;
- Według opinii naszych ekspertów nie należy spodziewać się wielkiej podaży usług certyfikacyjnych, które są bardzo specyficzne i wymagają sporych nakładów na przygotowanie odpowiedniej infrastruktury badawczej. Firmy komercyjne, jeżeli mają (lub inwestują) w takie laboratoria, to przeważnie wykorzystują je dla swoich potrzeb i nie bardzo mogą być obiektywnym audytorem dla przeprowadzenia badań rozwiązań konkurencyjnych;
- Może warto zastanowić się nad możliwością wykorzystania przez jednostki certyfikujące potencjału uczelni technicznych lub nawet doposażyć ich laboratoria i zlecać część badań uczelniom, które mogłyby odpłatnie świadczyć usługi (wybrane, specyficzne badania) na rzecz kilku podmiotów certyfikujących (zarówno publicznych, jak i prywatnych).