Warszawa, dnia 19 grudnia 2019 r.

MINISTERSTWO CYFRYZACJI

Departament Cyberbezpieczeństwa

Założenia dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie[1]

Niniejsza notatka zawiera główne założenia dotyczące wdrażania CSA w Polsce. Zapraszam do zgłaszania uwag i propozycji do niniejszych założeń w terminie **do 24 stycznia 2020 r. na adres konsultacje_cyber@mc.gov.pl.**

Proponowany model ogólny

Model rekomendowany dla Polski to model mieszany. Zakłada współpracę sektora publicznego i prywatnego w celu zapewnienia łatwej dostępności certyfikacji oraz jej promocji wśród przedsiębiorców. Nie będzie naruszał innych przepisów o certyfikacji, w tym bezpieczeństwa.

Konieczne jest określenie modelu certyfikacji cyberbezpieczeństwa w Polsce – przede wszystkim sposobu tworzenia **programów certyfikacji.**

Podmioty w systemie certyfikacji

Laboratoria powinny działać na zasadach rynkowych. Ponieważ **koszt oceny** jest trudny do oszacowania i zależny od wielu czynników, powinien być kształtowany przez rynek. Regulacja w tym zakresie powinna być minimalna.

Zgodnie z CSA możliwe jest utworzenie jednej lub wielu **jednostek certyfikujących.** Mogą być one publiczne lub prywatne. Polskie prawo zna oba modele[2]. Przy jednej jednostce certyfikującej państwo ma większą kontrolę nad tym kto jest certyfikowany; model ten jest jednak niewydolny, kiedy dużo podmiotów jest zainteresowanych uzyskaniem certyfikatu.

Publiczne jednostki certyfikujące można przyporządkować do jednostek, w których obecnie funkcjonują zespoły CSIRT – wymaga to dalszych uzgodnień z tymi jednostkami. Pozwoliłoby to na zachowanie spójności systemu z krajowym systemem cyberbezpieczeństwa. Oznacza to także konieczność ustalenia odgórnie kosztów uzyskania certyfikatu.

W przypadku **prywatnych jednostek certyfikujących** można określić sposoby ich funkcjonowania w oparciu o model stosowany dla wyrobów przeznaczonych na potrzeby

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE L 151 z 7.6.2019, str. 15 (dalej: CSA)

[2] Np. ustawa o ochronie informacji niejawnych zakłada jedną jednostkę certyfikującą – tj. Szefa ABW.

obronności i bezpieczeństwa państwa. Koszty certyfikacji powinny być ustalane przez jednostkę na zasadach rynkowych.

CSA dopuszcza istnienie wielu **krajowych organów ds. certyfikacji cyberbezpieczeństwa** (organu nadzoru), ale celem zachowania spójności działań i jednolitego nadzoru sugerowane jest ustanowienie jednego organu nadzoru. Proponowanym krajowym organem jest Minister Cyfryzacji. Do jego obowiązków należałoby m.in. monitorowanie przestrzegania ustawy, monitorowanie wykonywania obowiązków wytwórców lub dostawców w zakresie samooceny, rozpatrywanie skarg.

Certyfikacja obowiązkowa

Jeśli chcemy osiągnąć jak największe nasycenie rynku certyfikatami, **należy stworzyć na nie odpowiedni popyt**. Można to zrobić np. poprzez utworzenie odpowiedniego systemu zachęt w ustawie o informatyzacji lub prawie zamówień publicznych.

Administracja powinna opierać się na bezpiecznych rozwiązaniach, co jest mocnym argumentem za zachęcaniem do używania certyfikowanego sprzętu i oprogramowania. Można to też osiągnąć poprzez **nałożenie obowiązku certyfikacji** na wybrany sprzęt (domyślnie certyfikacja jest dobrowolna). Przy określeniu podmiotów obowiązanych do obowiązkowej certyfikacji należy odnieść się do rodzaju świadczonych usług oraz wielkość samych operatorów. **Dla większości operatorów, szczególnie mniejszych, powinna wystarczyć deklaracja zgodności**. Będzie to tańsze rozwiązanie. Do rozważenia jest obowiązek nadania certyfikatu o wyższym stopniu w przypadku operatorów infrastruktury krytycznej o bardzo wysokim znaczeniu (rurociągi, energetyka, obsługa organów centralnych administracji publicznej, łączność).

Nadzór i kontrola

Należy też określić **zasady nadzoru i kontroli**, w tym produktów i usług, co do których zachodzi podejrzenie, że zostały niewłaściwie oznaczone certyfikatem. Podejrzenie może też wynikać z uzyskania informacji z innego kraju UE (KE planuje utworzenie systemu na wzór systemu RAPEX dla znaków CE). Należy pamiętać, że mimo iż będzie tylko jeden organ nadzoru, to może być wielu właścicieli programów certyfikacji, którzy będą mieli własne uprawnienia, niewynikające z ustawy.

Polecany model kontroli powinien zostać opracowany w oparciu o kryteria zawarte w Prawie Przedsiębiorców (w stosunku do prywatnych jednostek certyfikujących) i ustawie o kontroli w administracji rządowej[3] (w stosunku do publicznych jednostek certyfikujących). Powinny być określone sankcje jakie mogą stosować organy kontroli w przypadku niezastosowania się do zaleceń przez podmiot kontrolowany – np. cofnięcie certyfikatu.

[3] Dz. U. 2011 Nr 185, poz. 1092

Pismo jest zgodne z wymaganiami WCAG 2.0 dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych, określonymi w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 poz. 2247)

Konieczne będzie też uregulowanie kwestii kar. Powinny one regulować wszystkie kwestie związane z nieodpowiednim użytkowaniem certyfikatu.

Zgłaszanie **deklaracji zgodności** będzie oparte na ogólnych zasadach unijnych. Nie są planowane odrębne rozwiązania krajowe.

Ministerstwo Cyfryzacji jest zaangażowane w prace Międzyresortowego Zespołu ds. Reformy Systemów Oceny Zgodności i Nadzoru Rynku. Prace nad wprowadzeniem CSA w Polsce będą zgrywane z reformą systemu oceny zgodności.