Warszawa, dnia 09 listopada 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.143.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 20 października 2017 r. Posła na Sejm RP Pana Pawła Pudłowskiego w sprawie *wiedzy rządu na temat rodzajów oprogramowań, z jakich korzystają instytucje publiczne oraz przedsiębiorstwa zarządzające infrastrukturą krytyczną* (interpelacja nr 16279)

Szanowny Panie Marszałku,

prawo polskie nie przewiduje żadnej formy rejestru dotyczącego wykorzystywanego oprogramowania w instytucjach państwowych. Ministerstwo Cyfryzacji nie ma narzędzi prawnych pozwalających na sprawdzanie, jakie oprogramowanie jest stosowane w poszczególnych podmiotach publicznych. Zgodnie z obowiązującym prawem nadzór nad bezpieczeństwem teleinformatycznym administracji państwowej oraz bezpieczeństwem operatorów infrastruktury krytycznej sprawuje Agencja Bezpieczeństwa Wewnętrznego.

Stosowanie środków zabezpieczeń w systemach teleinformatycznych związane jest z przeprowadzeniem dla takiego systemu szacowania ryzyka w zakresie bezpieczeństwa informacji. Zastosowanie środka zabezpieczenia (m.in. oprogramowania antywirusowego) wynika z przyjętego sposobu postępowania z ryzykiem, w tym z uwzględnienia ryzyka zastosowania samego środka zabezpieczającego.

Operatorzy infrastruktury krytycznej w Polsce to w większości przedsiębiorcy działający w formie spółek prawa handlowego. Ponieważ przedsiębiorcy nie są elementem sektora finansów publicznych w rozumieniu ustawy *o finansach publicznych*[1], posiadają prawo do swobodnego kształtowania swojej sytuacji prawnej poprzez zawieranie umów z wybranymi przez siebie podmiotami. Ministerstwo Cyfryzacji nie dysponuje narzędziami ani środkami prawnymi mogącymi zakazać zawierania umów na konkretne usługi czy produkty przez przedsiębiorców działających na polskim rynku

[1] Ustawa z dnia 27 sierpnia 2009 r. *o finansach publicznych* (Dz. U. z 2016 r. poz. 1870).

Operatorzy infrastruktury krytycznej należący do sektora finansów publicznych podlegają ustawie - *Prawo zamówień publicznych*[2]. Z jej zapisów wynika, że wykluczenia podmiotowe wykonawców mogą wystąpić m. in. w przypadku gdy przepis prawa wymaga od wykonawcy posiadania określonego zezwolenia, co nie ma miejsca w przypadku sprzedaży oprogramowania antywirusowego[3]. Kierownik zamawiającego może odstąpić od stosowania ustawy, w tym skierować zapytanie ofertowe do wybranych przez siebie wykonawców, między innymi w przypadku zamówień:

1) którym nadano klauzulę zgodnie z przepisami o ochronie informacji niejawnych lub
2) jeżeli wymaga tego istotny interes bezpieczeństwa państwa, lub
3) jeżeli wymaga tego ochrona bezpieczeństwa publicznego, lub
4) którym muszą towarzyszyć, na podstawie odrębnych przepisów, szczególne środk bezpieczeństwa

– w zakresie, w jakim ochrona istotnych interesów dotyczących bezpieczeństwa państwa określonych w w/w pkt. nie może zostać zagwarantowana w inny sposób niż udzielenie zamówienia bez zastosowania ustawy.

Decyzja o odstąpieniu od stosowania ustawy *prawo zamówień publicznych* pozostaje wyłączną kompetencją kierownika zamawiającego, który w konkretnym przypadku ponosi odpowiedzialność zarówno za zastosowanie, jak i niezastosowanie ustawy.

W dn. 31 października br. został udostępniony do konsultacji projekt ustawy o krajowym systemie cyberbezpieczeństwa. Celem projektu ustawy jest ustanowienie krajowego systemu cyberbezpieczeństwa, którego zadaniem będzie zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług. Efektem będzie podniesienie odporności kluczowych usług świadczonych z wykorzystaniem technologii informacyjnych na ataki pochodzące z cyberprzestrzeni. System będzie obejmować operatorów usług kluczowych – wśród których mogą się znaleźć również operatorzy infrastruktury krytycznej – dostawców usług cyfrowych, zespoły CSIRT poziomu krajowego, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa.

[2] ustawa z dnia 29 stycznia 2004 r. - *Prawo zamówień publicznych* (Dz. U. z 2017 r. poz. 1579).
[3] W świetle obowiązującego prawa sprzedaż oprogramowania antywirusowego nie podlega koncesjonowaniu, tak jak na przykład działalność w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym.

Ustawa wdraża procedurę identyfikacji operatorów usług kluczowych przewidzianą dyrektywą NIS[4].

Projekt ustawy formułuje obowiązki w zakresie bezpieczeństwa teleinformatycznego dla operatorów usług kluczowych. Będą oni zobowiązani do wdrożenia i stosowania środków technicznych i organizacyjnych, aby zapewnić bezpieczeństwo systemów informacyjnych służących do świadczenia usług kluczowych. Będą również zobligowani do szacowania ryzyka związanego cyberbezpieczeństwem oraz przekazywania CSIRT poziomu krajowego informacji o zaistniałych incydentach (lub podejrzeniu wystąpienia incydentu) wraz z ich obsługą we współpracy ze wspomnianym CSIRT. Operatorzy usług kluczowych będą mogli realizować obowiązki z zakresu cyberbezpieczeństwa samodzielnie bądź poprzez delegowanie ich realizacji na podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Ustawa określa szczegółowo obowiązki w zakresie monitorowania, kontrolowania, audytów i testowania wdrożonych zabezpieczeń.

Jeśli chodzi o *soft law*, Rządowe Centrum Bezpieczeństwa opublikowało załącznik do Narodowego Programu Ochrony Infrastruktury Krytycznej, który zawiera dobre praktyki i rekomendacje dotyczące zapewnienia sprawnego funkcjonowania infrastruktury krytycznej. Wspomniany dokument dotyczy również bezpieczeństwa teleinformatycznego.

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*.