Warszawa, dnia 14 listopada 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.145.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 25 października 2017 r. Posła na Sejm RP Pana Adama Andruszkiewicza w sprawie *programu antywirusowego Kaspersky Lab w polskiej administracji* (interpelacja nr 16520)

Szanowny Panie Marszałku,

prawo polskie nie przewiduje żadnej formy rejestru na temat wykorzystywanego oprogramowania w instytucjach państwowych. Ministerstwo Cyfryzacji nie ma narzędzi prawnych pozwalających na sprawdzanie, jakie oprogramowanie jest stosowane w poszczególnych podmiotach publicznych.

Zgodnie z ustawą *o informatyzacji*[1] podmioty publiczne mają obowiązek zapewnienia m.in. sprawnej i bezpiecznej wymiany informacji w postaci elektronicznej między podmiotami publicznymi. Szczegółowe wymogi w tym zakresie precyzuje rozporządzenie o Krajowych Ramach Interoperacyjności[2], które określa m.in. wymóg zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Odpowiedni dobór oprogramowania antywirusowego zależy zatem od decyzji poszczególnych podmiotów.

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.

[1] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (t.j.: Dz. U. z 2017 r. poz. 570).

[2] Zgodnie z § 20 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 (t.j.: Dz. U. z 2016 r. poz. 113) dalej „KRI"

Zakup oprogramowania przez administrację publiczną jest regulowany przez ustawę - *Prawo zamówień publicznych*[3]. Zgodnie z tymi przepisami, 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 jej zastosowanie, jak i niezastosowanie.

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 podmioty będące administracją publiczną – dostawców usług cyfrowych, zespoły CSIRT poziomu krajowego, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa.

Zgodnie z projektem ustawy, podmioty publiczne są obowiązane identyfikować i klasyfikować incydent, dokumentować jego obsługę, zgłaszać incydenty poważne niezwłocznie do właściwego CSIRT, zapewnić obsługę incydentu zwykłego, podejmować działania naprawcze, w tym usuwać skutki incydentu oraz zapewnić użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Z wyrazami szacunku,
Anna Streżyńska

[3] ustawa z dnia 29 stycznia 2004 r. - *Prawo zamówień publicznych* (Dz. U. z 2017 r. poz. 1579).

Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów