Warszawa, dnia 26 lutego 2018 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

BM-WOP.072.12.2018

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z 6 lutego 2018 r. Posła na Sejm RP Pana Tomasza Kostusia w sprawie *stosowania programu antywirusowego Kaspersky przez jednostki administracji publicznej* (interpelacja nr 18991)

Szanowny Panie Marszałku,

zgodnie z ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne[1] obowiązkiem organów administracji publicznej jest wykorzystanie systemów spełniających minimalne wymagania dla systemów teleinformatycznych (szczegółowe wymogi w tym zakresie precyzuje rozporządzenie o Krajowych Ramach Interoperacyjności[2]). 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. Odpowiedzialność za zakupione oprogramowanie leży w gestii poszczególnych podmiotów. Niemniej ważne od samego zakupu – w tym przypadku oprogramowania antywirusowego – jest sposób korzystania z niego i odpowiednia konfiguracja dostosowana do przyjętej polityki bezpieczeństwa informacji w danej instytucji, poprzez między innymi wybór takiego trybu działania oprogramowania, który minimalizuje ryzyko wycieku danych.

[1] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 t.j.)
[2] Rozporządzenie 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 2012 r. poz. 526)

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)

W odniesieniu do oprogramowania antywirusowego Kaspersky Lab Ministerstwo Obrony Narodowej RP, odnosząc się do stanowiska Stanów Zjednoczonych i Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii, zarekomendowało zaprzestanie używania ww. oprogramowania[3].

Ministerstwo Cyfryzacji nie dokonuje rekomendacji co do stosowania konkretnego oprogramowania antywirusowego, ani nie dysponuje środkami prawnymi, które umożliwiłyby wprowadzenie zakazu stosowania jakiegoś oprogramowania. Wprowadzenie takiego zakazu bez podstawy prawnej godziłoby w zasady uczciwej konkurencji i mogłoby naruszać unijne zasady konkurencji. Jak wskazano powyżej, dobór oprogramowania zależy od decyzji podmiotu.

Niemniej jednak Ministerstwo Cyfryzacji prowadzi działania na rzecz podwyższenia poziomu cyberbezpieczeństwa w Polsce oraz uregulowania podstaw prawnych dla takich działań, jak rekomendacje dotyczące oprogramowania. Ministerstwo skierowało pod obrady właściwych komitetów Rady Ministrów projekt ustawy o krajowym systemie cyberbezpieczeństwa, który ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym 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. System będzie obejmować również administrację publiczną.

Zgodnie z projektem ustawy, podmioty publiczne będą 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.

W celu zwiększenia cyberbezpieczeństwa Polski zostały wdrożone rozwiązania, które m. in. promują dobre praktyki, dostarczają informacji na temat zagrożeń, monitorują nowe regulacje i inicjatywy. Potwierdza to działalność takich instytucji jak NASK, będący państwowym instytutem badawczym nadzorowanym przez Ministerstwo Cyfryzacji. Działalność operacyjną w zakresie cyberbezpieczeństwa NASK realizuje w ramach pionu NC Cyber (Narodowego Centrum Cyberbezpieczeństwa).

[3] pismo z 5 grudnia 2017 r., nr 104/158/17 skierowane do Rady Ministrów

NC Cyber to centrum wczesnego ostrzegania i szybkiego reagowania. Centrum funkcjonuje w trybie 24/7 przez 365 dni w roku. W strukturze NC Cyber działa Zespół CERT Polska odpowiedzialny za reagowanie na zgłoszone incydenty. Zespół ten odpowiada również za rejestrowanie i obsługę zdarzeń naruszających bezpieczeństwo sieci. CERT Polska analizuje zagrożenia i monitoruje stan cyberbezpieczeństwa.

W strukturze Agencji Bezpieczeństwa Wewnętrznego funkcjonuje natomiast Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Jednym z jego podstawowych zadań jest zapewnianie i rozwijanie zdolności jednostek administracji rządowej do ochrony przed zagrożeniami płynącymi z cyberprzestrzeni.

Z wyrazami szacunku,
z up. Marek Zagórski
Sekretarz Stanu
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów

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)