Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.81.2024
Warszawa, 05 sierpnia 2024 r.

**Szanowny Pan**
**Szymon Hołownia**
**Marszałek Sejmu RP**

Dot. pisma z 11 lipca br. Posła na Sejm RP Pana Pawła Papke w sprawie wsparcia finansowego dla samorządów w związku z wymianą systemów operacyjnych Windows 10 Pro (interpelacja nr 3666)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

**Ad 1) Czy w planach Ministerstwa jest stworzenie programu wsparcia finansowego samorządów w tych wydatkach? Jeśli tak, proszę o przedstawienie planów wraz z terminami realizacji i wejścia ich w życie.**

Przede wszystkim należy wyjaśnić, że okres wsparcia dla systemu operacyjnego Windows 10 został określony przez producenta na 10 lat. System Windows 11 jest dostępny na rynku od 2021 roku i nowe komputery wprowadzane od tego czasu do sprzedaży spełniają wymagania sprzętowe tego systemu. Także znaczna część działających obecnie komputerów wyprodukowanych w latach wcześniejszych spełnia wymagania systemu Windows 11. Z kolei samo uaktualnienie z systemu Windows 10 Pro do systemu Windows 11 Pro jest bezpłatne.

Jednocześnie warto wskazać, że dostępnych jest też wiele w pełni bezpłatnych, otwartoźródłowych (open source) dystrybucji systemów operacyjnych. Migracja do otwartoźródłowych systemów może wiązać się z początkowym czasem wdrożenia dla administratorów i użytkowników (z uwagi na ich przyzwyczajenia), lecz ostatecznie rozwiązania open source są znacznie tańsze w utrzymaniu i cechują się wysoką odpornością na złośliwe oprogramowanie.

Należy podkreślić, że Ministerstwo Cyfryzacji dostrzega zasadność wspierania samorządów w zakresie cyberbezpieczeństwa i realizuje działania w tym zakresie. W celu zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych Ministerstwo Cyfryzacji uruchomiło program Cyberbezpieczny Samorząd. Łącznie na wsparcie JST w bieżącej edycji programu przeznaczonych zostanie ok. 1,5 mld zł, z czego część tych środków będzie mogła być wykorzystana przez JST na zakup oprogramowania i sprzętu związanego z zapewnianiem cyberbezpieczeństwa.

**Ad 2) Czy w planach ministerstwa jest wprowadzenie dodatkowych zabezpieczeń chroniących dane wrażliwe mieszkańców, zabezpieczeń chroniących wycieki danych osobowych, chroniące przed cyberatakami, zakażeniem wirusem lub złośliwym oprogramowaniem?**

Ministerstwo Cyfryzacji prowadzi wiele kompleksowych działań mających na celu podniesienie poziomu cyberbezpieczeństwa w Polsce. W kontekście samorządu terytorialnego szczególnie istotny jest wyżej opisany program Cyberbezpieczny Samorząd, jak również inne planowane inicjatywy obliczone na wsparcie JST w zakresie cyberbezpieczeństwa, np. utworzenie wojewódzkich zespołów specjalistów

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

cyberbezpieczeństwa, czy utworzenie Lokalnych Centrów Cyberbezpieczeństwa na poziomie samorządu terytorialnego.

Oprócz tego wiele działań jest realizowanych i przygotowanych na poziomie krajowym, w tym przykładowo między innymi:

- procedowana projekty aktów prawnych: nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, ustawa o krajowym systemie certyfikacji w cyberbezpieczeństwie;
- przygotowanie nowej Strategii Cyberbezpieczeństwa RP na lata 2025-2029;
- rozwój potencjału i zdolności instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym (np. w zakresie rozpoznawania zagrożeń w cyberprzestrzeni, ochrona przed atakami typu DDoS, rozwój systemu S46);
- zapewnienie bezpiecznych środków łączności na potrzeby administracji rządowej i podmiotów krajowego systemu cyberbezpieczeństwa;
- podnoszenie poziomu wiedzy, kompetencji i umiejętności zarówno specjalistów ds. cyberbezpieczeństwa, jak i całego społeczeństwa;
- utworzenie Funduszu Cyberbezpieczeństwa, którego środki przeznacza się na wyrównanie poziomu wynagrodzeń w sektorze prywatnym i publicznym, co pozwala ustabilizować fluktuację zatrudnienia specjalistów ds. cyberbezpieczeństwa w administracji publicznej;
- podnoszenie poziomu cyberbezpieczeństwa państwowych systemów i rejestrów oraz cyfrowych usług publicznych.

Wyżej opisane działania przyczyniają się do zwiększania poziomu odporności polskiej cyberprzestrzeni, a przez także do lepszego zabezpieczenia danych wrażliwych mieszkańców i wzmacniania ochrony systemów administracji publicznej przed złośliwym oprogramowaniem i działaniami różnego typu grup cyberprzestępczych. Szczegółowe dane na temat realizowanych inicjatyw dostępne są w Sprawozdaniu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok, opublikowanym na stronie Ministerstwa Cyfryzacji[1].

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

**Do wiadomości:**
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[1] https://www.gov.pl/attachment/d3f61dae-8635-4de7-84b7-5369894a865b

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa