Warszawa, 18 kwietnia 2014 r.

RZECZPOSPOLITA POLSKA
MINISTERSTWO
ADMINISTRACJI I CYFRYZACJI

PODSEKRETARZ STANU
Roman Dmowski

BM-WP.072.138.2014

Pan
Bogdan Borusewicz
Marszałek Senatu RP

Szanowny Panie Marszałku,

w odpowiedzi na pismo z dnia 5 marca 2014 r. (sygn. SPRM-4813-99-(1)/14), przekazujące tekst oświadczenia złożonego przez Senatora RP Macieja Klimę podczas 49. posiedzenia Senatu RP w dniu 20 lutego 2014 r. w sprawie *korzystania z systemu Windows XP w instytucjach rządowych oraz publicznych po 8 kwietnia 2014 r.*, przedstawiam odpowiedzi na poszczególne pytania.

Ile systemów operacyjnych Windows XP oraz programów zależnych jest wykorzystywanych w administracji rządowej oraz instytucjach podległych rządowi Rzeczpospolitej Polskiej, w ujęciu procentowym lub liczbowym?

Jakie koszty wprowadzenia nowych systemów operacyjnych, zastępujących dotychczasowe Windows XP, w zakresie infrastruktury informatycznej w administracji rządowej i instytucjach podległych rządowi należy ponieść w latach 2014-2015 i czy te środki zostały uwzględnione w budżecie rządu lub budżetach resortów na 2014 r.?

Ministerstwo Administracji i Cyfryzacji nie dysponuje konkretnymi danymi liczbowymi, które umożliwiałyby udzielenie odpowiedzi w przedmiotowej sprawie. Każda jednostka organizacyjna administracji państwowej prowadzi samodzielną politykę w zakresie nabywania niezbędnych do prowadzonej działalności składników majątkowych, w tym oprogramowania komputerowego. Istniejące przepisy nie wymagają także, aby jednostki te przekazywały w tym zakresie dane lub sprawozdania.

Jakie jest oficjalne stanowisko instytucji rządowych odpowiedzialnych za bezpieczeństwo związane z zagrożeniami w cyberprzestrzeni, jeśli chodzi o korzystanie z systemów operacyjnych Windows XP i programów zależnych po 8 kwietnia 2014 r.?

Jakie działania podjął lub ewentualnie zamierza podjąć rząd Rzeczpospolitej Polskiej w związku z realnym zagrożeniem wynikającym z zapowiadanych przez Microsoft zmian dotyczących aktualizacji systemu Windows XP?

Odpowiedzi na powyższe pytania leżą poza zakresem kompetencji Ministerstwa Administracji i Cyfryzacji.

Jakie instytucje ponoszą odpowiedzialność za nadzorowanie bezpieczeństwa w zakresie cyberprzestrzeni w administracji rządowej oraz instytucjach podległych rządowi?

Odpowiedzialność za bezpieczeństwo i ochronę cyberprzestrzeni Polski jest rozproszona. Nie istnieje jeden podmiot koordynujący działania w tym zakresie. W związku z tym, poszczególne instytucje odpowiadają za wybrane obszary związane z ochroną cyberprzestrzeni. Te obszary to: ochrona cyberbezpieczeństwa administracji państwowej, ochrona użytkowników prywatnych i sfera obrony narodowej. Dodatkowo w każdym z wymienionych obszarów bezpieczeństwo informatyczne może obejmować jawne i niejawne systemy teleinformatyczne. Przekazane poniżej informacje dotyczą bezpieczeństwa cyberprzestrzeni administracji państwowej i użytkowników prywatnych oraz jawnych systemów teleinformatycznych w niej użytkowanych oraz ogólne informacje na temat zakresu właściwości poszczególnych instytucji wobec niejawnej sfery systemów teleinformatycznych.

Zgodnie ze strukturą rządu Ministerstwo Administracji i Cyfryzacji jest głównym resortem zajmującym się informatyzacją państwa. Ustawa *o działach administracji rządowej* (t.j.: Dz. U. z 2013 r. poz. 743, z późn. zm.) nakłada na ministra właściwego ds. informatyzacji m.in. zadania w zakresie informatyzacji administracji publicznej, systemów i sieci teleinformatycznych administracji publicznej, technologii i technik informacyjnych, standardów informatycznych, rozwoju społeczeństwa informacyjnego oraz realizacji zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji. Przyjęta przez Radę Ministrów w dniu 25 czerwca 2013 r. „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" (dalej „Polityka") wskazuje ponadto na ministra ds. informatyzacji jako podmiot koordynujący jej realizację, z zastrzeżeniem, że organem nadzorującym wdrożenie „Polityki" jest Rada Ministrów. Celem omawianego dokumentu jest wzmocnienie wzajemnego zaufania i bezpieczeństwa wśród podmiotów działających w cyberprzestrzeni i określenie ról, które powinny one odgrywać. Polityka wskazuje także na zadania operacyjne do wykonania. I tak rolą ministra właściwego ds. informatyzacji jest określenie, we współpracy z zaangażowanymi instytucjami, jednolitej metodyki przeprowadzania analiz ryzyka bezpieczeństwa cyberprzestrzeni w urzędach administracji rządowej. Dodatkowo wskazane w „Polityce" urzędy administracji rządowej mają przekazać ministrowi właściwemu ds. informatyzacji sprawozdania podsumowujące wyniki szacowania ryzyka zgodne z wzorcem przygotowanym w ramach metodyki. MAC przekazało w dniu 13 lutego br. projekt wymienionej metodyki wraz z prośbą o sporządzenie sprawozdania z oceny ryzyka w danej instytucji do dnia 31 marca br. Polityka przewiduje również przeprowadzenie

kampanii medialnej na temat sposobów przeciwdziałania i zwalczania zagrożeń w cyberprzestrzeni. Informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach „Polityki" będą prezentowane na stronach internetowych MAC oraz na stronie Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Wymieniony Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL to działający od 2008 r. w ramach Agencji Bezpieczeństwa Wewnętrznego zespół, którego celem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę systemów i sieci teleinformatycznych, których ewentualne zniszczenie mogłoby stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego lub środowiska, powodować poważne straty materialne lub zakłócić funkcjonowanie państwa. W 2012 r. w ramach działań CERT.GOV.PL powołano zespoły dyżurujące, pełniące funkcję całodobowego punktu kontaktowego dla administratorów systemów i sieci teleinformatycznych. CERT.GOV.PL zarządza głównie incydentami cybernetycznymi w sektorze publicznym, a jego działania obejmują koordynację procesu reagowania na incydenty, rozwiązywanie i analizowanie zdarzeń, koordynacja reagowania na luki w zabezpieczeniach. CERT.GOV.PL publikuje raporty o stanie bezpieczeństwa cyberprzestrzeni RP w kolejnych latach (raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r. dostępny jest pod adresem http://www.cert.gov.pl/cer/publikacje/raporty-o-staniebezpi). CERT.GOV.PL działa więc zarówno w obszarze bezpieczeństwa IT jawnych i niejawnych systemów wykorzystywanych w administracji rządowej. Sama Agencja Bezpieczeństwa Wewnętrznego jest natomiast odpowiedzialna zgodnie z ustawą z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. Nr 182, poz. 228) za realizację zadań w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych.

Należy w tym miejscu wskazać, że w Polsce nie istnieje jeden „zespół reagowania na incydenty komputerowe", lecz szereg CERT-ów, zajmujących się kwestią szeroko rozumianego bezpieczeństwa teleinformatycznego, oprócz wspomnianego CERT.GOV.PL funkcjonuje także resortowe Centrum Zarządzania Bezpieczeństwem Usług i Sieci Teleinformatycznych Ministerstwa Obrony Narodowej zajmujące się zapobieganiem incydentom mogących wpłynąć na obronność RP, a także zespoły utworzone przez „środowisko telekomunikacyjne", m.in. CERT OPL, PIONIERCERT oraz CERT POLSKA – funkcjonujący w ramach Naukowej i Akademickiej Sieci Komputerowej (będącej instytutem badawczym, jak i operatorem sieci transmisji danych). Od początku istnienia rdzeniem działalności zespołu CERT POLSKA jest obsługa incydentów bezpieczeństwa komputerowego i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. CERT POLSKA od 1996 r. przygotowuje i udostępnia roczne statystyki dotyczące incydentów bezpieczeństwa teleinformatycznego w polskich zasobach internetowych, także cywilnych, które zostały zgłoszone do zespołu. W 2013 r. opublikowany został raport za 2012 r. CERT Polska „Analiza incydentów naruszających bezpieczeństwo teleinformatyczne" (dostępny pod adresem http://www.cert.pl/raporty).

Ważnym elementem otoczenia cyberbezpieczeństwa w Polsce, działającym w sferze publicznych sieci telekomunikacyjnych, jest Urząd Komunikacji Elektronicznej, który jest krajowym organem regulacyjnym w dziedzinie telekomunikacji. Zgodnie z art . 175a pkt 1 ustawy z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (t.j.: Dz. U. z 2014 r., poz. 243)

przedsiębiorcy telekomunikacyjni mają obowiązek niezwłocznie powiadomić Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które mają istotny wpływ na działanie sieci lub usług oraz podjętych w tym celu środkach zapobiegawczych. Podobnie dostawca publicznie dostępnych usług telekomunikacyjnych powiadamia Generalnego Inspektora Ochrony Danych Osobowych o naruszeniu danych osobowych, niezwłocznie, nie później niż w ciągu trzech dni od daty naruszenia. Informacje znajdują się na stronie internetowej UKE pod adresem: http://www.uke.gov.pl/informowanie-o-naruszeniach-bezpieczenstwa-lub-integralnosci-sieci-12238.

Przedmiotem działalności Rządowego Centrum Bezpieczeństwa jest jawna i niejawna sfera funkcjonowania systemów teleinformatycznych. Zgodnie z ustawą z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (t.j.: Dz. U. z 2013 r. poz. 1166, z późn. zm.) infrastruktura krytyczna obejmuje systemy teleinformatyczne niezbędne do minimalnego funkcjonowania gospodarki i państwa. Przygotowany na podstawie art. 5b ust. 7 pkt. 1 „Narodowy Program Ochrony Infrastruktury Krytycznej" (dalej „Program") określa ministrów i kierowników urzędów centralnych odpowiedzialnych za funkcjonowanie systemów krytycznych. Wyznacza także szczegółowe kryteria, które pozwolą zidentyfikować obiekty, instalacje, urządzenia i usługi zawarte w systemach infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli. W tym zakresie Minister Administracji i Cyfryzacji jest odpowiedzialny za następujące systemy infrastruktury krytycznej: systemy łączności, systemy sieci teleinformatycznych, systemy zapewniające ciągłość działania administracji publicznej. Zgodnie z „Programem" odpowiedzialność za dany system infrastruktury krytycznej (dalej IK) wiąże się m.in. z dokonywaniem oceny ryzyka zakłócenia funkcjonowania systemu IK, wywołanego zniszczeniem lub zakłóceniem funkcjonowania IK, organizacją i obsługą systemowego forum ochrony IK i udziałem w mechanizmie ochrony IK, dokonywaniem okresowych analiz i ocen skuteczności ochrony infrastruktury krytycznej we właściwym systemie, inspirowaniem wdrażania nowoczesnych technik ochrony IK w systemie.

Podsumowując należy również podkreślić, że w przypadku jawnych systemów teleinformatycznych, które są głównie przedmiotem działalności MAC, zadania i uprawnienia ośrodka właściwego w sprawach bezpieczeństwa IT jawnych systemów wykorzystywanych w sferze publicznej nie mają podstaw w przepisach ustawowych. Możliwości w zakresie egzekwowania wdrożenia wymagań, zaleceń i rekomendacji wynikają jedynie z „Polityki ochrony cyberprzestrzeni RP", która nie jest dokumentem rangi ustawowej. Należy przy tym wskazać, że na poziomie Unii Europejskiej przedmiotem prac jest wniosek dotyczący dyrektywy w sprawie zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci teleinformatycznych i przetwarzanych w nich informacji („Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", COM(2013)48). Projekt dyrektywy został przedstawiony łącznie ze wspólnym komunikatem Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa w sprawie (dalej: „Strategia"). Proponowana dyrektywa jest kluczowym elementem europejskiej strategii bezpieczeństwa cybernetycznego, zatytułowanej: „Otwarta, bezpieczna i chroniona cyberprzestrzeń" i nakłada obowiązek zapewnienia bezpiecznego i wiarygodnego środowiska cyfrowego w całej UE na państwa członkowskie, podmioty dostarczające kluczowe usługi świadczone drogą elektroniczną (np. platformy handlu elektronicznego i portale społecznościowe), operatorów infrastruktury krytycznej, takich jak: przedsiębiorstwa

z sektora energetycznego, sektora transportu, sektora bankowego i opieki zdrowotnej. Projekt dyrektywy przewiduje przyjęcie następujących środków:

a) zobowiązanie państw członkowskich do przyjęcia strategii w dziedzinie bezpieczeństwa sieci i informacji oraz wyznaczenia właściwych krajowych organów, dysponujących odpowiednimi środkami finansowymi i zasobami ludzkimi, by odpowiednio postępować i reagować w przypadku wystąpienia incydentów i zagrożeń w dziedzinie bezpieczeństwa sieci;
b) ustanowienie mechanizmu współpracy między państwami członkowskimi a Komisją, aby przekazywać za pośrednictwem bezpiecznej infrastruktury wczesne ostrzeżenia dotyczące zagrożeń i incydentów, współpracować i organizować regularne wzajemne weryfikacje;
c) zobowiązanie operatorów infrastruktury krytycznej w niektórych sektorach (usług finansowych, transportu, energii i opieki zdrowotnej), oraz organów administracji publicznej do stosowania właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez te podmioty sieci i systemy teleinformatyczne oraz do przyjęcia praktyk w zakresie postępowania w przypadku wystąpienia zagrożeń i zgłaszania incydentów mających znaczny wpływ na bezpieczeństwo świadczonych przez nie usług podstawowych.

Ministerstwo Administracji i Cyfryzacji uczestniczy w wypracowaniu ostatecznego kształtu rozwiązań przewidzianych w dyrektywie poprzez przygotowanie stanowisk Rządu, instrukcji wyjazdowych i innych dokumentów, przekazywanych elektronicznie delegatom na posiedzenia organów, na których są dyskutowane we współpracy ze wszystkimi zainteresowanymi instytucjami. Projekt dyrektywy przewiduje obecnie konieczność wyznaczenia organu odpowiedzialnego za realizację zadań z zakresu cyberbezpieczeństwa oraz wyposażenie go w uprawnienia władcze, co będzie wymagało odpowiedniej implementacji do prawa polskiego w drodze ustawy.

Z poważaniem,

PODSEKRETARZ STANU
w Ministerstwie Administracji i Cyfryzacji

Roman Dmowski

Do wiadomości:
Departament Spraw Parlamentarnych
Kancelarii Prezesa Rady Ministrów