Warszawa, dnia 02 sierpnia 2017 r.

**RZECZPOSPOLITA POLSKA**
MINISTER CYFRYZACJI

***Anna Streżyńska***

BM-WOP.072.99.2017

**Pan**
**Marek Kuchciński**
**Marszałek Sejmu RP**

Dot. przesłanej przy piśmie z dnia 14 lipca 2017 r. (sygn. DSP.INT.4810.404. 2017) interpelacji Posła na Sejm RP Pani Joanny Muchy w sprawie *ataków cybernetycznych* (interpelacja nr 13879)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane w interpelacji pytania.

1. **Jaka była skala ataku wirusa Petya w Polsce? Ile firm i instytucji zostało zaatakowanych?**

W Polsce zidentyfikowano jedenaście firm komercyjnych dotkniętych atakiem Petya. W większości są to firmy zajmujące się działalnością logistyczną i handlową. Narodowe Centrum Cyberbezpieczeństwa[1] (NC Cyber) nie odnotowało informacji o zgłoszeniach dotyczących administracji publicznej, instytucji finansowych i infrastruktury krytycznej państwa.

Po zidentyfikowaniu ataku natychmiast poinformowano o nim instytucje i firmy współpracujące z NC Cyber – z prośbą o szczególną czujność i wszelkie informacje, a także zgłoszenia ewentualnych przypadków infekcji. W informacjach dla opinii publicznej NC Cyber radziło, aby aktualizować systemy, robić backupy i nie korzystać z niezaufanych sieci (w tym Wi-fi). Działający w NC Cyber zespół CERT Polska już w dzień następujący po ataku, tj. 28 czerwca 2017 r., opublikował analizę ataku wraz z rekomendacjami w zakresie reagowania na zagrożenie.

[1] Działające w strukturze organizacyjnej Państwowego Instytutu Badawczego NASK.

2. **Jakie instytucje nadzorują przestrzeganie Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne?**

Ustawa *o informatyzacji działalności podmiotów realizujących zadania publiczne*[2] określa organy właściwe dla kontroli przestrzegania przepisów ustawy, w zależności od zasięgu projektów informatycznych:

- realizację ponadsektorowych projektów kontroluje Prezes Rady Ministrów;
- realizację projektów sektorowych kontrolują ministrowie odpowiedzialni za dany dział administracji;
- działania systemów teleinformatycznych (pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych) kontrolują odpowiednio:
    - w jednostkach samorządu terytorialnego i ich związkach oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych – właściwy wojewoda;
    - w podmiotach publicznych podległych lub nadzorowanych przez organy administracji rządowej – organ administracji rządowej nadzorujący dany podmiot publiczny;
    - w pozostałych przypadkach – minister właściwy do spraw informatyzacji.

3. **Czy zapisy Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne są wystarczające wobec powtarzających się w br. ataków cybernetycznych?**

Wobec ciągłego wzrostu znaczenia cyberbezpieczeństwa na świecie, a więc także w Polsce, należy uznać za konieczne stworzenie systemu prawnego umożliwiającego odpowiednią reakcję na ewentualne zagrożenia cyberbezpieczeństwa. Na potrzebę tę odpowiada projekt ustawy o krajowym systemie cyberbezpieczeństwa, implementujący dyrektywę NIS[3]. Wymaganym przez Dyrektywę terminem przyjęcia tej ustawy jest dzień 9 maja 2018 r. Przekazanie projektu ustawy do konsultacji publicznych i uzgodnień międzyresortowych planowane jest na koniec sierpnia. Następnie projekt zostanie przekazany do rozpatrzenia przez Komitet Rady Ministrów ds. Cyfryzacji.

Ustawa ureguluje kwestie związane z operatorami usług kluczowych (czyli, zgodnie z przepisami Dyrektywy, podmiotów które świadczą usługę o kluczowym znaczeniu dla

[2] Art. 25 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r. poz. 570 z późn. zm.)

[3] 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 (Dz. U. UE L 194 z 19 lipca 2016 r., str. 1).

utrzymania krytycznej działalności społecznej lub gospodarczej - świadczenie tej usługi zależy od systemów informatycznych, a ewentualny incydent miałby istotny skutek zakłócający dla jej zapewnienia) oraz ich obowiązkami. Wprowadzi regulacje dotyczące CSIRT (zespołów reagowania na incydenty komputerowe). Ustanowi także kontrolę państwa nad przestrzeganiem przepisów ustawy.

Projektowana ustawa pozwoli zachować kontrolę nad sytuacją w przypadku powtórzenia się ataków na systemy teleinformatyczne. Należy mieć na względzie, że metody ataków na systemy teleinformatyczne są ciągle udoskonalane. Z tego powodu trudno jest mówić o pełnym zabezpieczeniu państwa przed nimi. Ustawa o krajowym systemie cyberbezpieczeństwa pozwoli jednak skuteczniej im zapobiegać, a także lepiej radzić sobie z ich ewentualnymi skutkami (zachowanie ciągłości usług kluczowych).

4. **Czy ministerstwa: Cyfryzacji, Spraw Wewnętrznych i Administracji, Obrony Narodowej współpracują w celu obrony naszego kraju przed kolejnymi atakami cyberprzestępców?**

Ministerstwo Cyfryzacji pozostaje w stałym kontakcie z Ministerstwem Spraw Wewnętrznych i Administracji oraz Ministerstwem Obrony Narodowej. MC, MSWiA i MON współpracują na poziomie strategicznym, czego wyrazem jest działalność międzyresortowych zespołów ds. Krajowych Ram Polityki Cyberbezpieczeństwa na lata 2017-2022, współpraca nad planem działań do wspomnianych Krajowych Ram oraz wspólne prace nad projektem ustawy o krajowym systemie cyberbezpieczeństwa. Również na poziomie operacyjnym współdziałają ze sobą zespoły reagowania na incydenty komputerowe będące we właściwości poszczególnych resortów oraz inne jednostki (czego wyrazem są m.in. ćwiczenia NASK, Policji i prokuratury CyberPOL 2017).
W odpowiedzi na ww. pytanie zarówno MSWiA, jak i MON potwierdziły fakt współpracy w zakresie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej z wieloma podmiotami krajowymi i międzynarodowymi.

Z wyrazami szacunku,
Anna Streżyńska
Minister Cyfryzacji
*/podpisano elektronicznie/*

**Do wiadomości:**
Kancelaria Prezesa Rady Ministrów