Warszawa, dnia 02 października 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.125.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 12 września 2017 r. Posła na Sejm RP Pana Jarosława Gonciarza w *sprawie cyberbezpieczeństwa i globalnych ataków ransomware* (interpelacja nr 15302)

Szanowny Panie Marszałku,

w Polsce funkcję strategii cyberbezpieczeństwa w rozumieniu dyrektywy NIS[1] pełnią Krajowe Ramy Polityki Cyberbezpieczeństwa RP - jednak obowiązki związane z cyberbezpieczeństwem w administracji publicznej regulują także akty prawne. Wszystkie instytucje rządowe podlegają regulacjom ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne* [2], zgodnie z którą są obowiązane m.in. posiadać system zarządzania bezpieczeństwem informacji. Rozporządzenie *o krajowych ramach interoperacyjności*[3] reguluje konieczne działania wchodzące w skład takiego systemu - w tym zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegające m.in.: na minimalizowaniu ryzyka utraty informacji w wyniku awarii i ochronie przed błędami, utratą czy nieuprawnioną modyfikacją. Należy założyć, że instytucje państwowe spełniające minimalnie wymogi określone w rozporządzeniu, mają zadowalający poziom bezpieczeństwa. Warto w tym miejscu zaznaczyć, że Ministerstwo Cyfryzacji nie jest uprawnione do ingerowania w działania poszczególnych instytucji rządowych w zakresie bezpieczeństwa informacji.

MC oraz instytut badawczy NASK w ramach inicjatywy Narodowego Centrum Cyberbezpieczeństwa[4] budują natomiast system partnerski w zakresie współpracy z kluczowymi podmiotami. NC Cyber to centrum wczesnego ostrzegania i szybkiego reagowania, a w razie ewentualnych ataków – koordynowania działań i wymiany informacji.

---

[1] 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.
[2] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r., poz. 570 z późn. zm.).
[3] § 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* (Dz. U. z 2016 r., poz. 113 t.j.).
[4] znajdującego się w strukturze NASK - dalej jako NC Cyber

Centrum funkcjonuje w trybie 24/7 przez 365 dni w roku. Szybka wymiana informacji między kluczowymi podmiotami ma szansę zapewnić skuteczne reagowanie na pojawiające się zagrożenia. NC Cyber współpracuje więc z przedsiębiorstwami telekomunikacyjnymi (Orange, Polkomtel, T-Mobile), branżą energetyczną (Energa, PSE, Gaz System, PERN), Związkiem Banków Polskich oraz bankami (Bank Zachodni WBK S.A., Credit-Agricole Bank Polska S.A., Bank Handlowy w Warszawie S.A., mBank S.A., Bank Millennium S.A., PKO BP S.A. oraz Raiffeisen Bank Polska S.A.) oraz innymi podmiotami m.in. z sektora transportowego czy chemicznego. W strukturze NC Cyber działa Zespół CERT Polska odpowiedzialny za reagowanie na incydenty. Zespół ten odpowiada również za rejestrowanie i obsługę zdarzeń naruszających bezpieczeństwo sieci, wykrywanie i analizę zagrożeń wymierzonych w szczególności w polskich internautów lub zagrażających domenie „.pl" oraz dynamiczne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla polskich internautów. CERT Polska analizuje zagrożenia i monitoruje stan bezpieczeństwa polskiego Internetu. Za bezpieczeństwo infrastruktury krytycznej przez atakami o charakterze terrorystycznym oraz ochronę systemów administracji rządowej odpowiada CERT.GOV.PL funkcjonujący w strukturze Agencji Bezpieczeństwa Wewnętrznego.

W Polsce zidentyfikowano jedenaście firm komercyjnych dotkniętych atakiem Petya. W większości są to firmy zajmujące się działalnością logistyczną i handlową. 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 za 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., analizę ataku wraz z rekomendacjami w zakresie reagowania na zagrożenie.

Jeśli chodzi o straty, to możliwe są jedynie szacunki. Wiele strat jest niepieniężnych (utrata zaufania do przedsiębiorstwa, wyciek danych osobowych, zmniejszenie poziomu bezpieczeństwa) lub po prostu trudna do oszacowania (uniemożliwienie dostępu do określonej usługi bądź obniżenie poziomu jakości jej świadczenia). Ministerstwo nie posiada dokładnych informacji na ten temat.

Ministerstwo Cyfryzacji posiada natomiast wiedzę o ogólnej liczbie incydentów zgłoszonych do CERT Polska - w 2016 r. CERT Polska obsłużył 7275 zgłoszeń, na podstawie których zidentyfikowano 1926 incydentów, zaś w 2015 r. zidentyfikowano 1456 incydentów. W 2016 r. CERT Polska przetworzył automatycznie przy pomocy platformy n6 200 mln zgłoszeń dotyczących komputerów z Polski, co stanowiło podobną liczbę jak w poprzednim roku.

Warto zaznaczyć, że nie wszystkie incydenty zgłaszane były do CERT Polska. Informacje o atakach w infrastrukturze administracji publicznej posiada CERT.GOV.PL.

Ponadto informuję, że planowane jest utworzenie Rządowego Klastra Cyberbezpieczeństwa - rodzaju rządowego intranetu, którego celem będzie zapewnienie bezpiecznego, efektywnego dostępu do zasobów Internetu przez instytucje rządowe, przy jednoczesnym zapewnieniu bezpieczeństwa użytkowników. Powstać ma również Zintegrowany System Bieżącego Zarządzania Bezpieczeństwem Cyberprzestrzeni RP (koordynatorem systemu będzie NC Cyber), który dostarczy informacji o bieżącym stanie cyberbezpieczeństwa w Polsce. Ponadto, realizowany jest projekt Systemu Łączności Systemu Kierowania Bezpieczeństwem Narodowym (SŁ SKBN), który służy do sprawnej wymiany informacji, wzmocnienia spójności i efektywności działań na wszystkich poziomach administracji publicznej.

W ramach implementacji dyrektywy NIS powstaje projekt ustawy o krajowym systemie cyberbezpieczeństwa. Planowane jest objęcie regulacją ustawową także podmiotów administracji publicznej, co ujednolici wymogi bezpieczeństwa i usprawni współpracę z zespołami reagowania na incydenty komputerowe w skali kraju.

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów