Warszawa, dnia 25 lipca 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.96.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 12 lipca 2017 r. Posła na Sejm RP Pana Adama Andruszkiewicza w sprawie *cyberbezpieczeństwa i ochrony zasobów informacyjnych w Ministerstwie Cyfryzacji* (interpelacja nr 13984)

Szanowny Panie Marszałku,

Ministerstwo Cyfryzacji zdaje sobie sprawę z istniejących zagrożeń wynikających z korzystania z systemów teleinformatycznych. Stan cyberbezpieczeństwa i ochrony zasobów informacyjnych w Ministerstwie należy uznać za optymalny. Stosowane są zabezpieczenia zarówno systemów, jak i sieci oraz urządzeń klienckich. Pracownicy ministerstwa są na bieżąco informowani o aktualnych zagrożeniach i sposobach ich zapobiegania.

W urzędzie funkcjonują również stosowne pragmatyki postępowania, mające na celu ochronę przed atakami a oprogramowanie wykorzystywane przez pracowników jest na bieżąco aktualizowane. W lipcu 2016 r. wycofano z eksploatacji przestarzałe komputery z systemem Windows XP, a na większości z używanych komputerach zainstalowano najnowszy system operacyjny tj. Windows 10. Do końca 2017 r. planuje się wdrożenie wirtualnych stacji roboczych, które pozwolą jeszcze lepiej zabezpieczyć środowisko pracy. Wówczas, w przypadku ewentualnego skutecznego ataku, będzie można znacząco szybciej i łatwiej przywrócić je do działania. Poza podjętymi działaniami mającymi na celu ochronę przed incydentami, służby informatyczne resortu podjęły działania mające na celu zachowanie ciągłości pracy Ministerstwa.

W związku z ostatnią kampanią ransomware dokonano także przeglądu obecnie stosowanych zabezpieczeń. Istniejące zabezpieczenia uznano wówczas za wystarczające (są one aktualizowane w ramach prac bieżących). Jednocześnie informuję, że żadne firmy zewnętrzne nie są zaangażowane w bezpieczeństwo Ministerstwa. Cyberbezpieczeństwem MC zajmują się bezpośrednio własne służby informatyczne, które stosują wielostopniowe

zabezpieczenia mające na celu niwelowanie zagrożeń wynikających z podatności sprzętu/oprogramowania pojedynczego dostawcy.

W przypadku ataków typu malware (także w kontekście najnowszej kampanii ransomware „Petya"), największe znaczenie ma jednak praca ludzi. Przepływająca poczta jest monitorowana celem wychwytywania wszelkich anomalii, użytkownicy są informowani i wyczulani, sprawdzana jest aktualność oprogramowania i wersja systemów dołączanego sprzętu. Ministerstwo posiada również infrastrukturę, która chroni zasoby: podwójną linię firewalli i oprogramowanie antywirusowe (planowane jest poszerzenie całości o firewalle klienckie). Ostatnią linią są bezpośrednie kontakty z instytucjami takimi jak CERT.gov.pl, które informują nas (oraz odwrotnie) o potencjalnych zagrożeniach. Ponieważ nie ma jednej, skutecznej ochrony przed ransomware najważniejsza jest dywersyfikacja narzędzi służących ochronie.

Poza działaniami w sferze IT, Ministerstwo buduje komplementarny system zarządzania bezpieczeństwem informacji (SZBI), zgodny z normą PN/ISO 27001. Pierwszym krokiem procesu budowy SZBI było opracowanie i wdrożenie w lipcu 2016 r. „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Ministerstwie Cyfryzacji", „Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych w Ministerstwie Cyfryzacji", a także dokumentu „Zasady Przetwarzania Danych Osobowych w Ministerstwie Cyfryzacji". Dokumentacja kompleksowo obejmuje swoim zasięgiem wszystkie systemy informatyczne Ministerstwa.

Stworzono także dokumentację, która określa i reguluje kwestie środków ochrony osobistej/fizycznej (w tym dostęp do pomieszczeń MC) czy korzystania ze sprzętu teleinformatycznego (w postaci regulaminu). Obowiązuje też Polityka Bezpieczeństwa Teleinformatycznego oraz Instrukcja postępowania w zakresie obsługi teleinformatycznej incydentów bezpieczeństwa systemów. Dodatkowo powołano „Zespół Reagowania na Incydenty Komputerowe w Ministerstwie Cyfryzacji". Ponadto w 2013 r., przeprowadzono audyt pn. „Zarządzanie bezpieczeństwem systemów teleinformatycznych w MAC". W jego następstwie w roku 2014, w ramach testów bezpieczeństwa Systemu Rejestrów Państwowych (SRP), wykonano globalne testy penetracyjne SRP. W roku 2015 przeprowadzono natomiast testy penetracyjne systemów informatycznych.

Obecnie w Ministerstwie Cyfryzacji w Departamencie Zarządzania Danymi powstaje Zespół do spraw zarządzania bezpieczeństwem informacji. Do jego zadań będzie należeć m.in. przeprowadzenie inwentaryzacji zasobów informacyjnych oraz zasobów systemów teleinformatycznych MC i przypisanie do tych zasobów „właścicieli zasobu", wypracowanie dokumentacji niezbędnej do zarządzania ryzykiem dla zasobów oraz przeprowadzenie

szacowania ryzyka zasobów oraz opracowanie nowej kompleksowej polityki bezpieczeństwa dla MC oraz szczegółowych polityk systemu zarządzania bezpieczeństwem informacji.

Warto również zaznaczyć, że podstawą prowadzenia polityki państwa w przedmiotowym zakresie są Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022[1], uwzględniające m.in. udoskonalanie struktury krajowego systemu cyberbezpieczeństwa. Ministerstwo podejmuje także konkretne działania zmierzające do wypełnienia celów przewidzianych w Krajowych Ramach, tj. implementuje dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148[2] w drodze ustawy, której celem będzie stworzenie krajowego systemu cyberbezpieczeństwa.

Przy Ministrze Cyfryzacji zainicjowano Forum Cyberbezpieczeństwa. Jest to forma współpracy sektora prywatnego z publicznym. Forum docelowo ma pracować w ramach czterech grup roboczych: legislacyjnej, edukacyjnej, automatyki przemysłowej oraz rozwoju Narodowego Centrum Cyberbezpieczeństwa[3].

Ponadto, planowane jest utworzenie Rządowego Klastra Cyberbezpieczeństwa (RKB), w 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, wzmocnieniu spójności i efektywności działań na wszystkich poziomach administracji publicznej.

Poza wspomnianymi wyżej Krajowymi Ramami, które pełnią w Polsce funkcję strategii cyberbezpieczeństwa w rozumieniu dyrektywy NIS, obowiązki związane z cyberbezpieczeństwem w administracji publicznej regulują poszczególne akty prawne. Wszystkie instytucje rządowe podlegają regulacjom ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*[4]. Zgodnie z zapisami tej ustawy są one obowiązane posiadać system zarządzania bezpieczeństwa informacji. Ponadto, kwestie te

[1] Uchwała Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. *w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*.

[2] 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 UE* (Dz. Urz. UE nr L 194/1). Dalej „NIS"

[3] Znajdujące się w strukturze Państwowego Instytutu Badawczego NASK – dalej jako NC Cyber.

[4] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2014 r., poz. 1114 z późn. zm.)

reguluje także rozporządzenie *o Krajowych Ramach Interoperacyjności*[5]. Z przepisów powyższych dokumentów wynikają dla podmiotów publicznych konkretne obowiązki. Obejmują m.in. posiadanie systemu zarządzania bezpieczeństwem informacji, zaś przepisy rozporządzenia precyzują działania wchodzące w skład takiego systemu. W tym zakresie Ministerstwo nie jest uprawnione do ingerowania w działania poszczególnych instytucji rządowych.

W ramach implementacji dyrektywy NIS powstaje projekt ustawy o krajowym systemie cyberbezpieczeństwa. Planowane jest objęcie regulacją ustawową także kategorii operatorów usług kluczowych będących podmiotami administracji publicznej

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów

[5] 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* (t.j.: Dz. U. z 2016 r., poz. 113).