Warszawa, dnia 21 listopada 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.151.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 2 listopada 2017 r. Posła na Sejm RP Pana Arkadiusza Marchewki w sprawie *zabezpieczenia środków finansowych na realizację Krajowych Ram Polityki Cyberbezpieczeństwa RP* (interpelacja nr 16665)

Szanowny Panie Marszałku,

w następstwie uzgodnień Rady Ministrów, Ministerstwo Cyfryzacji wystąpiło z wnioskiem do Ministra Finansów o dokonanie zmian w projekcie budżetu na rok 2018 poprzez zmianę przeznaczenie wydatków w części 29 – obrona narodowa. Ministerstwo Cyfryzacji wnioskowało o kwotę 76.130 tys. zł z przeznaczeniem na utworzenie przedmiotowej rezerwy. Obecnie trwają uzgodnienia pomiędzy resortem cyfryzacji a Ministerstwem Obrony Narodowej dot. zagospodarowania w/w kwoty w ramach rezerwy na wydatki na realizację części zadań określonych w Planie Działań do Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022"[1].

Ministerstwo Cyfryzacji planuje wykorzystać wskazane wyżej środki na realizację części zadań określonych w Planie Działań, w szczególności na następujące cele:

1) opracowanie metodyki testów penetracyjnych oraz utworzenie repozytorium audytów i testów – jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń są okresowe audyty systemów teleinformatycznych. Na podstawie norm i dobrych praktyk oraz uwzględniając specyfiki poszczególnych sektorów, opracowane zostaną spójne metodyki audytów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów w różnych podmiotach. Kolejnym środkiem oceny bezpieczeństwa są testy penetracyjne, które pozwalają na

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

rzeczywistą ocenę odporności systemu na zagrożenia. Ich wyniki stanowią podstawę weryfikacji przyjętych założeń w zakresie ustanowionych zabezpieczeń;

2) wydatki związane z prowadzeniem repozytorium audytów i testów systemów teleinformatycznych – celem utworzenia repozytorium audytów i testów jest gromadzenie najlepszych praktyk zawierających światowe rekomendacje z obszaru bezpiecznej konfiguracji urządzeń i oprogramowania w celu osiągniecia minimalnego, rekomendowanego poziomu bezpieczeństwa;

3) ekspertyzy związane z rozbudową zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa oraz ekspertyzy w zakresie wymagań bezpieczeństwa dla sektorów usług kluczowych w związku z wdrażaniem nowych regulacji prawnych – celem ekspertyz z tego zakresu będzie określenie w jaki sposób należy dokonać odtworzenia i rozbudowy kompetencji w obszarze budowy zdolności do kompleksowego wytwarzania urządzeń i oprogramowania wykorzystywanych we wszystkich gałęziach przemysłu a także określenie wymogów bezpieczeństwa teleinformatycznego w określonych sektorach gospodarki w związku z planowanymi regulacjami dotyczącymi cyberbezpieczeństwa (min. transpozycja dyrektywy NIS);

4) budowę centralnej części systemu zarządzania bieżącym bezpieczeństwem cyberprzestrzeni RP – system ten umożliwi zgłaszanie informacji o zagrożeniach i podatnościach, ich agregowane, analizowanie i korelowanie. Na podstawie przeprowadzonych analiz przekazywane będą ostrzeżenia do zainteresowanych stron na temat zagrożeń i podatności, co przyczyni się do ograniczenia skutków incydentów bezpieczeństwa w systemach teleinformatycznych instytucji publicznych i operatorów usług kluczowych;

5) budowę podsystemu telekomunikacyjnego systemu zarzadzania bieżącym bezpieczeństwem cyberprzestrzeni RP – podsystem zapewni dwustronną komunikację pomiędzy częścią centralną systemu i jego użytkownikami końcowymi;

6) budowę intranetu dla ministerstw i urzędów centralnych (realizacja I fazy budowy Rządowego Klastra Bezpieczeństwa) - celem przedsięwzięcia jest zbudowanie wewnętrznej, wydzielonej sieci komputerowej łączącej ministerstwa i urzędy centralne wraz z bezpiecznym wyjściem do Internetu publicznego. Rozwiązanie takie umożliwi funkcjonowanie administracji rządowej szczebla centralnego nawet w przypadku istotnych zakłóceń w sieci publicznej. Przyczyni się także do optymalizacji zapotrzebowania na usługi dostępu do Internetu i spowoduje obniżenie kosztów takich usług;

7) rozbudowa i utrzymanie zdolności w zakresie skoordynowanego reagowania na incydenty komputerowe na poziomie krajowym – rozbudowa narzędzi analitycznych, wypracowanie procedur współdziałania oraz rozwój infrastruktury sprzętowej pozwoli na utrzymanie i rozwój zdolności reagowania na zagrożenia i incydenty na poziomie krajowym (CSIRTy poziomu krajowego);

8) opracowanie i wdrożenie systemu obligatoryjnych, cyklicznych szkoleń i ćwiczeń kadr administracji państwowej na wszystkich szczeblach – ćwiczenia i testy są krytycznym czynnikiem procesu zwiększenia efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP, jak i doskonalenia systemu reagowania na incydenty;

9) ekspertyzy związane z opracowaniem modelu zarządzania zasobami ludzkimi w obszarze cyberbezpieczeństwa – ekspertyzy określą w jaki sposób kształtować przebieg rozwoju zawodowego specjalistów z zakresu cyberbezpieczeństwa oraz w jaki sposób efektywnie zarządzać tymi zasobami;

10) opracowanie i realizację planu podnoszenia świadomości społecznej w obszarze cyberbezpieczeństwa, prewencję cyberprzestępczości, koordynacja inicjatyw/kampanii społecznych podejmowanych przez poszczególne instytucje, organizacje pozarządowe, sektor prywatny – celem działania będzie uruchomienie kampanii społecznych, skierowanych do różnych grup docelowych (między innymi dzieci, rodziców, seniorów) a także podnoszenie świadomości zagrożeń i wiedzy dotyczącej dobrych praktyk cyberbezpieczeństwa (tzw. higiena bezpieczeństwa) wśród użytkowników systemów komputerowych;

11) organizacja Forum Cyberbezpieczeństwa – organizacja cyklicznego wydarzenia, jakim jest Forum Cyberbezpieczeństwa wynika z podjętych zobowiązań z partnerami współpracującymi w ramach Forum;

12) utrzymanie i rozwój funkcjonowania wszystkich linii obsługi zgłoszeń i monitorowania sytuacyjnego – w wyniku realizacji zadania zapewnione zostaną odpowiednie zasoby osobowe na wszystkich liniach działań operacyjnych Narodowego Centrum Cyberbezpieczeństwa niezbędnych do realizacji procesów NC Cyber w zakresie bezpieczeństwa cyberprzestrzeni - wraz z procesami wspierającymi;

13) wdrożenie technologii monitorowania aktywnego zagrożeń typu drive-by-download – efektem realizacji zadania jest działające rozwiązanie pozwalające na cykliczne monitorowanie popularnych zasobów w Internecie i wykrywanie zagrożeń typu drive-by-download;

14) rozbudowa systemów partnerskich w NC Cyber - wdrożenie technologii (systemów IT) i procedur współpracy dla systemów partnerskich NC Cyber (min. Strefa partnerów, Platforma Współpracy Analitycznej, Abuse Forum);

15) budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa.

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów