WNIOSEK
o wyrażenie zgody na utworzenie przez Ministra Sprawiedliwości instytucji gospodarki budżetowej pod nazwą „Centrum Cyberbezpieczeństwa Zamość"

Na podstawie art. 23 ust. 2 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o *finansach publicznych* (tj.: Dz. U. z 2019 r. poz. 869 z późn. zm.) wnoszę o wyrażenie przez Radę Ministrów zgody na utworzenie instytucji gospodarki budżetowej pod nazwą „**Centrum Cyberbezpieczeństwa Zamość"**, w treści wniosku zwaną: „**CCZ**".

Podstawowym celem utworzenia CCZ jest zwiększenie poziomu bezpieczeństwa cybernetycznego szeroko pojętego Resortu Sprawiedliwości. Zgodnie z badaniami prowadzonymi przez NASK utrzymuje się wieloletnia negatywna tendencja rosnącego poziomu zagrożenia cyberbezpieczeństwa. [1] W 2019 roku było 73,5% więcej incydentów cyberbezpieczeństwa niż w roku 2018. [2] Z dotychczasowych danych za rok 2020 wynika, że incydentów będzie prawdopodobnie dwa razy więcej niż w roku 2019. Pandemia wywołana przez wirus SARS-CoV-2 zdeterminowała sytuację, w której znacząca część pracowników Resortu Sprawiedliwości rozpoczęła pracę w trybie zdalnym, z wykorzystaniem narzędzi teleinformatycznych, co powoduje większe prawdopodobieństwo cyberataków. Jak wynika z wewnętrznych analiz Resortu Sprawiedliwości, obecna sytuacja epidemiologiczna spowodowała zwiększoną aktywność o charakterze cyberprzestępczym, która nie ustanie w wyniku zwalczenia stanu pandemii. Co więcej, tendencja wynikająca z zaistniałej sytuacji ma charakter stały, a zagrożenia rosną i brak jest danych wskazujących na zmniejszenie ich poziomu w najbliższym czasie.

Reasumując, konieczne jest zwiększenie potencjału niezbędnego do zabezpieczenia resortu przed rosnącym zagrożeniem cyberatakami.

Kolejnym celem utworzenia CCZ jest długoterminowa ekonomizacja działań Ministra Sprawiedliwości w obszarze cyberbezpieczeństwa, przy jednoczesnym zapewnieniu wysokiej dostępności i elastyczności właściwych dla utrzymania usług kluczowych dla tego organu. Trzeba bowiem mieć na uwadze fakt postępującej cyfryzacji zarówno Ministerstwa Sprawiedliwości, jak i jednostek podległych i nadzorowanych przez ministra kierującego działem „sprawiedliwość." W obsługiwanych przez w/w jednostki systemach teleinformatycznych przetwarzane są wrażliwe dane tysięcy osób, których ochrona stanowi nie tylko wyraz troski ale przede wszystkim wyzwanie stawiane przez rozwijające się społeczeństwo. Zapewnienie wysokiego poziomu cyberbezpieczeństwa Resortu Sprawiedliwości, a co za tym idzie bezpiecznego przetwarzania danych wrażliwych, jest warunkiem *sine qua non* sprawnego funkcjonowania nie tylko administracji publicznej i wymiaru sprawiedliwości ale również przedsiębiorstw i obywateli.

Projektowana jednostka ponadto będzie miała za zadanie świadczenie usług eksperckich dla Resortu Sprawiedliwości, jak również organizowania konferencji i konkursów służących podniesieniu bezpieczeństwa cyberprzestrzeni. Do jej zadań będzie należeć np.

wytwarzanie specjalistycznego oprogramowania z zakresu cyberbezpieczeństwa na zlecenie Prokuratora Generalnego, Ministerstwa Sprawiedliwości, czy też Funduszu Sprawiedliwości. Zadania te będą realizowane w sposób prostszy, tańszy, a przede wszystkim bez konieczności udostępniania wrażliwych danych firmom zewnętrznym.
CCZ – jako jednostka odpowiedzialna za cyberbezpieczeństwo – będzie w stanie organizować konferencje naukowe, które przyciągną analogiczne podmioty, odpowiedzialne za bezpieczeństwo biznesu, jak również administrację innych państw.
Niezależnie od powyższego zadaniem CCZ ma być świadczenie usług doradczych dla administracji publicznej. Świadczenie tego rodzaju usług przez jeden, wyspecjalizowany podmiot pozytywnie wpłynie na implementacje analogicznych rozwiązań w całej administracji, co nie tylko zwiększy bezpieczeństwo ale i obniży koszty funkcjonowania tych rozwiązań.

Organ administracji rządowej wykonujący funkcję organu założycielskiego:

Minister Sprawiedliwości.

Przedmiot działalności podstawowej:

Przedmiotem działalności podstawowej CCZ jest świadczenie usług na rzecz Ministra Sprawiedliwości oraz jednostek temu organowi podległych i przezeń nadzorowanych, jak również w przypadku zaistnienia takiej potrzeby także na rzecz innych organów administracji państwowej i samorządowej.

Przedmiot działalności podstawowej obejmuje:

- aktywny monitoring i reagowanie na incydenty cyberbezpieczeństwa,
- testy penetracyjne,
- audyty bezpieczeństwa,
- szkolenia z zakresu cyberbezpieczeństwa,
- usługi eksperckie z zakresu cyberbezpieczeństwa,

to jest usługi opisane w Działach 62 oraz 63 Polskiej Klasyfikacji Działalności, stanowiącej załącznik do Rozporządzenia Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz.U. Nr 251, poz. 1885 z późn. zm.).

Źródła przychodów

Źródłami przychodów CCZ będą:

a) działalność statutowa, w postaci odpłatnego świadczenia na rzecz Skarbu Państwa (jednostek organizacyjnych wymiaru sprawiedliwości i jednostek administracji publicznej), jak również krajowych i zagranicznych osób:
   - usług doradczych, szkoleniowych i eksperckich,

- usług rozwoju, integracji i utrzymywania rozwiązań z zakresu cyberbezpieczeństwa,
- usług audytu bezpieczeństwa,
- usług testów penetracyjnych,
- usług aktywnego monitoringu i reagowania na incydenty cyberbezpieczeństwa,

b) środki pochodzące z budżetu Unii Europejskiej i innych źródeł zagranicznych niepodlegających zwrotowi,
c) jednorazowa dotacja na pierwsze wyposażenie w środki obrotowe,
d) darowizny, spadki i zapisy.

Przeznaczenie zysku

Zysk uzyskany z prowadzonej działalności wykorzystywany będzie w celu finansowania inwestycji lub pokrycie ewentualnej straty netto.

UZASADNIENIE

Przedkładając niniejszy wniosek, jako naczelny organ administracji rządowej, dostrzegam celowość podjęcia skutecznych kroków, nakierowanych na zwiększenie standardów cyberbezpieczeństwa w Resorcie Sprawiedliwości. W mojej ocenie, właściwym sposobem uczynienia zadość wspomnianej powinności jest wykreowanie nowoczesnej jednostki, zdolnej do zapewnienia potencjału kompetencyjnego, kadrowego i technicznego, niezbędnego do zabezpieczenia zadań z zakresu cyberbezpieczeństwa, zgodnie ze Strategią Cyberbezpieczeństwa na lata 2019-2023.
Podzielając opinie zawarte w treści dokumentu „*System bezpieczeństwa cyberprzestrzeni RP"* opublikowanego przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, dostrzegam istotną potrzebę zwiększenia cyberbezpieczeństwa, poprzez powołanie specjalnej jednostki, której zadania będą dedykowane realizacji wskazanego celu. W obliczu zwiększających się zagrożeń wydaje się niezbędne rozpoczęcie wykonywania takich działań, jak testy penetracyjne, czy też zapewnienie usługi podnoszenia standardów bezpieczeństwa, uwzględniających specyfikę danego sektora zgodnie z wytycznymi SOC [3]. Tego rodzaju postulaty spełnić może jedynie jednostka posiadająca stosowny potencjał operacyjny, pozwalający na szybkie reagowanie na pojawiające się zagrożenia, jak również na pozyskiwanie ad hoc ekspertów z poszczególnych dziedzin szeroko pojętego bezpieczeństwa teleinformatycznego, celem eliminacji pojawiających się nowych zagrożeń, ale przede wszystkim - podejmowania działań prewencyjnych, przeciwdziałających ich powstawaniu.

Na problem cyberbezpieczeństwa w dobie COVID-19 zwracał uwagę Josep Borell – Wysoki Przedstawiciel Unii Europejskiej do spraw Zagranicznych i Polityki Bezpieczeństwa [4].

Ponadto w ocenie autora niniejszego wniosku, istnieje potrzeba wytwarzania oprogramowania specjalistycznego z zakresu cyberbezpieczeństwa na zlecenie prokuratur, Ministerstwa Sprawiedliwości, Funduszu Sprawiedliwości, czy też sądów. Przy czym istotną kwestią jest by oprogramowanie to – wytwarzane dla poszczególnych jednostek – było kompatybilne, a rozwiązania w nim implementowane analogiczne. Są to kwestie istotne tak z punktu widzenia administratora, jak i użytkownika końcowego. Na dzień dzisiejszy oprogramowanie zamawiane jest przez poszczególne jednostki budżetowe u różnych dostawców, co powoduje różnorodność rozwiązań i brak jednolitego podejścia do ochrony cyberprzestrzeni.

Utworzenie podmiotu, który w sposób profesjonalny realizować będzie zadania publiczne polegające na ochronie publicznej cyberprzestrzeni, a przy tym maksymalizacja zysku nie będzie dlań – jako podmiotu publicznego – kwestią najistotniejszą - pozwoli na zabezpieczenie funkcjonowania cybernetycznego administracji państwowej i ujednolicenia rozwiązań w niej funkcjonujących.
Ponadto, jak wskazano powyżej, CCZ – jako jednostka odpowiedzialna za cyberbezpieczeństwo – będzie w stanie organizować konferencje naukowe, podnoszące poziom zabezpieczeń cyberprzestrzeni, jak również świadczyć usługi doradcze dla administracji publicznej co niewątpliwie wpłynie pozytywnie na implementację analogicznych rozwiązań zwiększających bezpieczeństwo w całej administracji.

Reasumując, powołanie CCZ dokładnie realizuje zapisy dokumentu *„System bezpieczeństwa cyberprzestrzeni RP NASK / CERT Polska”*. Wynika z niego [5], że w niedalekiej przyszłości powinno powstać Centrum Analityczne, z szeregiem kompetencji, które jako CCZ (częściowo przynajmniej) winno realizować.
“*Do zadań Centrum Analitycznego należeć powinny w szczególności: wsparcie techniczne przy analizie szczególnie trudnych incydentów, przeprowadzanie zaawansowanych analiz złośliwego oprogramowania zagrażającego użytkownikom cyberprzestrzeni RP, analiza podatności, bieżące monitorowanie wskaźników zagrożeń takich jak: rozmiary botnetów, reputacje sieci – przede wszystkim na podstawie informacji zbieranych w Platformie Wymiany Informacji oraz w systemie monitorowania i ostrzegania o zagrożeniach, rozwój narzędzi i metod do wykrywania i zwalczania zagrożeń*.”

W tej samej części dokumentu znajdziemy uzasadnienie dla powstania IGB: „*Ze względu na zakres specjalistycznych kompetencji technicznych, którymi powinno dysponować Centrum Analityczne nie rekomendujemy umieszczenia go w którejkolwiek instytucji administracji publicznej. Ze względu na dużą konkurencyjność sektora prywatnego w zakresie wysokości płac, wiązałoby się to bowiem z potencjalnymi problemami z zatrudnieniem oraz utrzymaniem odpowiednio wyszkolonego personelu merytorycznego*”.

Wyrażam przekonanie, że powołanie do życia proponowanej jednostki uczyni zadość oczekiwaniom związanym z potrzebą zapewnienia bezpieczeństwa cybernetycznego.

Przedstawiane rozwiązania oraz inicjatywy pozwolą uzyskać długotrwały efekt ekonomiczny, wsparty funkcjonowaniem modelu organizacyjnego, przy jednoczesnym utrzymaniu wysokiej zdolności utrzymania jakości usług, a w szczególności:

a) zapewnienie elastyczności, dostępności, ciągłości i bezpieczeństwa usług IT dla resortu sprawiedliwości oraz innych resortów,
b) zapewnienie wyższego poziomu jakości usług, poprzez zwiększenie cyberbezpieczeństwa oraz dostępności i funkcjonalności obsługiwanych systemów informatycznych,
c) zapewnienia otwartości na współpracę i zabezpieczenie wzajemnej dostępności usług i zasobów IT różnych podmiotów administracji publicznej,
d) zmniejszenie kosztów ponoszonych na rzecz cyberbezpieczeństwa,
e) zmniejszenie wydatków ponoszonych przez budżet państwa, związanych z utrzymaniem i eksploatacją niewspółdzielonych zasobów teleinformatycznych.

Należy także zwrócić uwagę, że powołanie CCZ do życia w formie instytucji gospodarki budżetowej zapewni transparentność działań tej jednostki oraz skutecznego nad nią nadzoru przez Ministra Sprawiedliwości.

Minister Sprawiedliwości zakłada, że zadania przygotowawcze zakończone operacyjną gotowością CCZ zostaną rozpoczęte niezwłocznie i zostaną przeprowadzone do końca pierwszego kwartału 2021 r. Do tego czasu CCZ uzyska i wdroży pełną zdolność do realizacji postawionych celów w 2021 r.

Koncepcja finansowania CCZ

Podstawowym źródłem przychodów CCZ ma być działalność statutowa, w postaci odpłatnego świadczenia na rzecz Skarbu Państwa (jednostek organizacyjnych wymiaru sprawiedliwości i jednostek administracji publicznej), jak również krajowych i zagranicznych osób:

- usług audytu bezpieczeństwa,
- usług testów penetracyjnych,
- usług aktywnego monitoringu i reagowania na incydenty cyberbezpieczeństwa,
- usług doradczych, szkoleniowych i eksperckich,
- usług rozwoju, integracji i utrzymywania rozwiązań z zakresu cyberbezpieczeństwa.

Ponadto – pośród innych źródeł finansowania wskazanych na wstępie, CCZ zostanie wyposażona – stosownie do treści art. 24 ust. 4 ustawy o finansach publicznych – w środki obrotowe w oparciu o jednorazową dotację Ministra Sprawiedliwości.

Według obliczeń projektodawcy, zestawienie szacowanych kosztów realizacji zadań z zakresu cyberbezpieczeństwa w resorcie zakłada wydatek na poziomie 9 777 222,70 PLN a koszt wykonania znacznie szerszych zadań CCZ wynosi 4 250 000 PLN jako że usługi te świadczone mają być przez podmiot wykonujący zadania publiczne.

Podsumowanie

Proponowana forma prawna umożliwi elastyczne i adekwatne wykorzystanie zasobów CCZ do wzmocnienia bezpieczeństwa cybernetycznego zgodnie z wytycznymi zawartymi w Strategii Cyberbezpieczeństwa na lata 2019-2023. Skutkiem utworzenia jednostki będzie zapewnienie stabilności utrzymania, przy równoczesnym zachowaniu bezpieczeństwa cyberprzestrzeni.

Realizacja zadań teleinformatycznych przez CCZ pozwoli Ministrowi Sprawiedliwości na szybkie reagowanie w obliczu nowych wyzwań i potrzeb, stawianych przez rozwijające się społeczeństwo informacyjne. Zapewni także zwiększenie bezpieczeństwa cyberprzestrzeni oraz wygeneruje dodatkowe przychody dla budżetu państwa, przez transparentną jednostkę, dysponującą wysoko wykwalifikowaną kadrą techniczną.
Powołanie CCZ pozwoli na pozyskanie dodatkowych, dobrze opłacanych i wysoko wykwalifikowanych ekspertów, dysponujących pełną wiedzą na temat projektowania, wdrażania i eksploatacji systemów i zasobów informacyjnych. Pozwoli to na jak największe uniezależnienie się od zewnętrznych wykonawców i oparciu się na własnych wyspecjalizowanych zasobach ludzkich.

Powyższe okoliczności sprawią, że możliwe będzie sprostanie rosnącym i coraz bardziej zaawansowanym wymaganiom w zakresie usług związanych z bezpieczeństwem cyberprzestrzeni.
Przewiduje się, że powstanie CCZ i powierzenie mu opisanych wyżej zadań doprowadzi do znakomitego podniesienia bezpieczeństwa cyberprzestrzeni oraz sprawi, że bezpieczeństwo systemów IT zarządzanych przez CCZ ulegnie zwiększeniu.

Pozytywnego wpływu powstania CCZ formie instytucji gospodarki budżetowej należy upatrywać także w obszarze sektora finansów publicznych poprzez:

- zapewnienie ciągłości zadań realizowanych dla Ministra Sprawiedliwości i innych jednostek publicznych,
- obniżenie kosztów projektowania, wdrażania i eksploatacji systemów służących do np. testów penetracyjnych czy ochrony cyberprzestrzeni zarządzanych przez CCZ.

Mając powyższe argumenty na uwadze, wniosek niniejszy jest uzasadniony.

Źródła:
[1] https://www.nask.pl/pl/aktualnosci/3719,Oszustwa-komputerowe-i-wyludzenia-danych-wsrod-najczesciej-wykrywanych-zagrozen-.html
[2] https://www.nask.pl/pl/aktualnosci/3835,Dane-CERT-Polska-za-pierwszy-kwartal-2020-roku-pokazuja-ze-w-okresie-pandemii-li.html
[3] Pełny opis problematyki SOC jest dostępny w rozdziale 6.3.13 SOC (Security Operations Center) – https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf
[4] https://www.consilium.europa.eu/pl/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/
[5] *System bezpieczeństwa cyberprzestrzeni RP NASK / CERT Polska* str. 86-87