Podczas prowadzonej przeze mnie dyskusji której temat „Jak i skąd pozyskiwać finansowanie na cyberbezpieczeństwo" omówione zostały następujące kwestie.

1. Czym jest cyberbezpieczeństwo i jakie ryzyka są z tym obszarem związane

Niezależnie od tego, czy organizacja jest podmiotem funkcjonującym w obrocie gospodarczym czy podmiotem działającym w sferze publicznej lub samorządowej, jako organizacja przetwarzająca dane wrażliwe tj. objęte różnego rodzaju tajemnicami jak np. tajemnica przedsiębiorstwa, tajemnica bankowa, czy inne tajemnice, ma obowiązek te dane chronić. Oprócz kwestii prawnych związanych z obowiązkiem ich ochrony w grę wchodzą również kwestie ryzyka wizerunkowego w przypadku kradzieży tych danych, ich upublicznienia lub innej sytuacji mogącej w istotny sposób wpłynąć na wiarygodność i zaufanie klientów/partnerów biznesowych/obywateli.
Kwestia ich ochrony tj. kwestia zapewnienia odpowiedniego poziomu cyberbezpieczeństwa tych danych i informacji które każda organizacja powinna chronić – jest kluczowa dla każdej organizacji, gdzie cyberbezpieczeństwo rozumiemy wszystkie zabezpieczenia i środki organizacyjne użyte przez organizację w celu ochrony jej systemów informatycznych i użytkowników przed nieuprawnionym dostępem, atakiem lub szkodą, tak aby zapewnić poufność, integralność i dostępność informacji. Na cyberbezpieczeństwo składa się również zapobieganie i obsługa incydentów tj. wykrywanie, reagowanie oraz przywracanie działalności operacyjnej po takich incydentach.

2. Możliwe sposoby finansowania cyberbezpieczeństwa

Otwierając dyskusję przedstawiłem przykładowe, zidentyfikowane przeze mnie narzędzia i programy umożliwiające finansowanie obszaru cyberbezpieczeństwa tj:

a) Finansowanie OW wynikające z UKSC tj. Art. 93
b) Zgodnie z Art. 14 możliwość finansowania cyberbezpieczeństwa przez OUK poprzez powierzenie zadań zewnętrznemu podmiotowi realizującemu zadania wskazane w UKSC. Mając na uwadze sytuację związaną z brakiem dostępności na rynku pracy specjalistów z obszaru cyber, oraz – bardzo często – łatwiejszym finansowaniem umów „outsourcingowych" w stosunku do zatrudnienia własnych pracowników, jest to możliwy do zrealizowania przez OUK kierunek działania. Jednocześnie wskazałem na konieczność posiadania we własnej strukturze organizacyjnej OUK minimalnych zasobów będących w stanie nadzorować realizację umowy przez zewnętrznego dostawcę świadczącego usługi z obszaru cyber.
c) Przedstawiłem w ogólnym zarysie instrument finansowania obszaru cyberbezpieczeństwa ze środków UE poprzez program CEF (Connecting Europe Facility). Program CEF Program CEF jest formą grantów przyznawanych przez UE na rozwój obszarów transportowego, energetyczne oraz telekomunikacyjnego, gdzie w obszarze związanym z telekomunikacja wyodrębniony jest obszar cyberbezpieczeństwa. Łączna suma dofinansowania w obszarze telekomunikacji wynosi 67.4mln EUR. Przedstawiłem dotychczasowe działania CEF w obszarze cyberbezpieczeństwa UE. Uczestnikom dyskusji przekazałem informację o możliwości skorzystania z CEF w zakresie budpwy i rozwoju zespołów CSIRT, realizacji zadań OUK, DUC, pojedynczych punktów kontaktowych, oraz realizacji zadań OW. Wskazałem terminy nowego call for submission dla obszaru cyberbezpieczeństwa który startuje 30 czerwca a wnioski o dofinansowanie można składać do 5 listopada 2020. Uczestnikom dyskusji przekazałem również istotną informację dot. priorytetu w przyznawainu grantów dla OUK (zarówno w sektorze publicznym jak i prywatnym).
d) Przedstawiłem założenia programu „Partnerstwa dla Cyberbezpieczeństwa" realizowanego przez NASK PIB, który „powstał z myślą propagowania idei cyberbezpieczeństwa, dbania o bezpieczeństwo RP w sieci, budowania i wspierania kompetencji w zakresie cyberbezpieczeństwa, a także tworzenia realnych struktur

opartych na wzajemnej współpracy mogących odeprzeć pojawiające się coraz częściej ataki. Program Partnerstwo dla Cyberbezpieczeństwa to przede wszystkim bezpośrednia wymiana informacji pomiędzy Partnerami i NASK, a także w razie konieczności z przedstawicielami właściwej administracji publicznej i organami ścigania. Program partnerski to także spotkania, seminaria i wspólne ćwiczenia procedur reagowania." Wskazałem również na możliwość współpracy i wsparcia NASK w pozyskiwaniu środków z instytucji unijnych i krajowych dotujących badania i rozwój oraz inwestycje w struktury i rozwiązania podnoszące bezpieczeństwo teleinformatyczne które wpisują się w działania np. programu CEF wskazanego w lit. C)

3. Podczas dyskusji w której udział braki przedstawiciele sektora prywatnego, publicznego oraz jednostek samorządu terytorialnego, omawiane były przedstawione przeze mnie możliwości finansowania obszaru cyberbezpieczeństwa oraz problemy poszczególnych organizacji mierzących się z wyzwaniami z tym związanymi. Jako podsumowanie dyskusji poniżej przedstawiam zebrane postulaty i kwestie wymagające zaadresowania:

   a) Uczestnicy dyskusji wskazali na istotność i wrażliwość danych przetwarzanych przez JST (tj. dane wszystkich obywateli) oraz na brak scentralizowanych ośrodków które zapewniałyby usługi cyberbezpieczeństwa dla podmiotów których nie stać na samodzielne zadania w tym obszarze. Zostało to przedstawione w kontekście problemów JST których nie stać jest na cyberbezpieczeństwo. Analogicznie dla zaprezentowanego przeze mnie modelu wsparcia z obszaru rynku finansowego tj. zrzeszenia banków spółdzielczych realizującego dla tych banków szereg usług (m.in. z obszaru bezpieczeństwa) dyskutanci wskazali na potrzebę stworzenia tzw. Centrum usług cyberbezpieczeństwa dla JST.
   b) Dyskutanci wskazali na konieczność opracowania i wdrożenia przez organ odpowiedzialny za obszar cyberbezpieczeństwa w Polsce tj. Ministerstwo Cyfryzacji, szkolenia dedykowanego nie dla kadry informatycznej ale dla kierowników jednostek organizacyjnych np. Burmistrzów lub Prezydentów. Miałby to być program uświadamiający (nie techniczny) wskazujący na istotność obszaru cyber, ryzyka i zagrożenia związane z tym obszarem i wynikające z tych zagrożeń konsekwencje. Dyskutanci wskazali, że brak świadomości kierowników organizacyjnych jest główną barierą w pozyskiwaniu środków finansowych na cyberbezpieczeństwo a ww. program umożliwiłby – poprzez uświadomienie decydentów – zaadresowanie wyzwań wynikających z obszaru cyber.
   c) Podczas dyskusji jednoznacznie stwierdzono, że państwo polskie powinno spriorytetyzować kwestie związane z obszarem cyber wzorem państw zachodnich. Na rozwój tego obszaru powinny zostać przeznaczone środki finansowe w wysokości umożliwiającej zaadresowania tego obszaru przez uczestników krajowego systemu cyberbezpieczeństwa.
   d) Wskazano również na konieczność zintensyfikowania działań szkoleniowo-uświadamiających do momentu realizacji postulatu wskazanego w lit. C) tak aby w momencie pojawienia się tych środków finansowych, były już zbudowane odpowiednie struktury umożliwiające ich wykorzystanie.

4. Na koniec dyskusji przedstawiłem uczestnikom jej podsumowanie przechodząc przez omawiane punkty oraz postulaty wskazane w pkt. 3, podziękowałem jej uczestnikom a następnie zamknąłem dyskusję.