REKOMENDACJA EUROPEJSKIEGO KONGRESU FINANSOWEGO 2019

Rekomendacja w obszarze cyberbezpieczeństwa sektora finansowego

Uczestnicy Europejskiego Kongresu Finansowego podkreślili rolę innowacyjnych rozwiązań będących siłami napędowymi rozwoju sektora finansowego oraz całej gospodarki. Postęp w oparciu o rozbudowane łańcuchy wartości na które składają się różnorodni gracze, szybkość zachodzących zmian, i ich liczba sprawiają, że cyberbezpieczeństwo dla wszystkich uczestników staje się coraz większym wyzwaniem.

Zastosowanie odpowiednich rozwiązań pozwalających na optymalne działanie w tej rzeczywistości wymaga zastosowania zarówno technologii umożliwiających zwinne działanie, jak i rozwiązań organizacyjnych i prawnych bazujących na współpracy zarówno wewnątrz sektora jak i międzysektorowej. Dotyczy to zarówno podmiotów, które wchodzą w skład poszczególnych sektorów, jak również spółek/organizacji które dostarczają usługi i produkty dla podmiotów tzw „Łańcucha dostaw".

Powyższe, podkreśla potrzebę kontynuacji dotychczasowych rekomendacji powstałych w trakcie poprzednich edycji EKF, w szczególności w obszarze działania Bankowego Centrum Cyberbezpieczeństwa oraz działań informacyjno-edukacyjnych wśród społeczeństwa zmierzających do podniesienia poziomu świadomości dotyczących zagrożeń i możliwości ochrony jak również podjęcia nowych inicjatyw.

Cele rekomendowanych działań są następujące:

1. Kontynuacja efektywnej, kompleksowej i spójnej ochrony instytucji finansowych, bazującej zarówno na współpracy sektorowej jak poza sektorowej, stanowiącej istotny element bezpieczeństwa Państwa.
2. Adopcja rozwiązań zapewniających wysoki poziom bezpieczeństwa.
3. Dalsza operacjonalizacja współpracy wewnątrz sektora oraz międzysektorowych działań z zakresu cyberbezpieczeństwa, szczególnie dla nowych modeli procesów biznesowych opartych na otwartej bankowości i federacyjnej tożsamości cyfrowej.
4. Wypracowanie zmian regulacyjnych umożliwiających zastosowanie nowoczesnych technologii.

Rekomendowane działania:

Działania strategiczne i operacyjne

1. Wzmocnienie ekosystemu sektorowego przeciwdziałania fraudom i „praniu brudnych pieniędzy" poprzez wykorzystanie informacji gromadzonych przez KIR, BIK i ZBP, uwzględniające:
    a. Wiodącą rolę KIR w budowaniu rozwiązania wspierającego sektorowe działania AML,
    b. Współpracę KIR i BIK w budowaniu rozwiązania wspierającego sektorowe działania antyfraudowe,

   c. Koordynacyjną rolę ZBP w środowisku bankowym oraz współpracy z innymi sektorami i wypracowania propozycji niezbędnych rozwiązań prawnych oraz organizacyjnych.
2. Wprowadzenie w jak najszybszym czasie postulowanych przez sektor bankowy i uzgodniony z Ministerstwem Finansów, zmian regulacji umożliwiających wymianę danych między organizacjami wewnątrz sektora finansowego oraz z instytucjami nadzoru.
3. Zacieśnienie współpracy z innymi jednostkami państwa, w tym NASK oraz z sektorem telekomunikacyjnym w zakresie przeciwdziałania cyberprzestępczości
4. Wykorzystane rozwiązań chmury obliczeniowej w celu dokonania transformacji cyfrowej, w tym również rozwiązań oferowanych przez Operatora Chmury krajowej w sektorze finansowym, jako narzędzie zwiększenia efektywności, poprawy konkurencyjności sektora w stosunku do rosnącej konkurencji poza bankowej oraz zwiększenie poziomu bezpieczeństwa rozwiązań bankowych.
5. Zniesienie barier prawnych lub interpretacji prawnych stopujących adopcję rozwiązań chmurowych, poprzez;
   a. Przygotowanie opisów stosowanych lub planowanych standardów bezpieczeństwa dedykowanych dla rozwiązań sektora finansowego
   b. W dialogu z KNF przygotowanie propozycji zmian prawnych lub ich interpretacji prawnych mających w obszarach analizy ryzyka, podejścia do planów awaryjnych oraz odpowiedzialności outsourcera i podoutsourcerów,
   c. Opinia nadzorców zagadnienia przetwarzania zaszyfrowanych danych bankowych w chmurze w stosunku do tajemnicy bankowej oraz zgodności z RODO i braku konieczności zbierania zgód Klientów na takie rozwiązania.
6. Poszerzenie bazy podmiotów korzystających z platform KIR i BIK skutkujących poprawą skuteczności funkcji predykcyjnych.
7. Budowa modelu oceny ryzyka związanego z funkcjonowaniem „Łańcucha dostaw" (TPRM – Third Party Risk Management), w tym przygotowanie zestawu wymagań, dobrych praktyk w w/w obszarze co pozwoli na systemowe podniesienie bezpieczeństwa dostarczanych produktów/usług w ramach sektora finansowego (ochrona łańcucha dostaw).