REKOMENDACJE DOTYCZĄCE CYBERBEZPIECZEŃSTWA SEKTORA FINANSOWEGO

Postęp w rozwoju technologii informatycznych z jednej strony jest kluczowym czynnikiem rozwoju usług bankowych, z drugiej zaś strony generuje ryzyka związane ze wzrostem cyberzagrożeń oraz nowych scenariuszy ataków i z tego powodu wymaga kontynowania działań wynikających z rekomendacji z lat ubiegłych. Zmieniające się otoczenie skłoniło Europejski Kongres Finansowy do dodania nowych rekomendacji dotyczących cyberbezpieczeństwa sektora finansowego. EKF chciałby podkreślić również, że cyberbezpieczeństwo jest obszarem wspólnego budowania ochrony sektorowej, a nie budowania przewagi konkurencyjnej.

CELE:

1. zapewnienie efektywnej, kompleksowej i spójnej ochrony instytucji finansowych, bazującej zarówno na współpracy sektorowej, jak i pozasektorowej, stanowiącej istotny element bezpieczeństwa państwa,
2. zwiększenie świadomości zagrożeń i możliwości ochrony dla klientów instytucji finansowych związanych z dynamicznym rozwojem cyfryzacji życia społeczeństwa oraz dalsze budowanie i zwiększanie kompetencji ekspertów w zakresie bezpieczeństwa dzięki współdziałaniu z systemem edukacji,
3. dalsza operacjonalizacja współpracy wewnątrz sektora oraz międzysektorowych działań mających na celu zapewnienie cyberbezpieczeństwa, zwłaszcza dla nowych modeli procesów biznesowych opartych na otwartej bankowości i federacyjnej tożsamości cyfrowej,
4. wypracowanie odpowiednich i bezpiecznych warunków niezbędnych do implementacji przepisów prawa.

REKOMENDOWANE DZIAŁANIA:

DZIAŁANIA STRATEGICZNE I OPERACYJNE

1. Zacieśnienie współpracy wewnątrzsektorowej z udziałem Bankowego Centrum Cyberbezpieczeństwa:
    a. kontynuowanie prac nad wypracowaniem docelowych mechanizmów umożliwiających szybką i bezpieczną wymianę informacji,
    b. wdrożenie ciągłego procesu poszukiwania informacji o podatnościach i zagrożeniach oraz mechanizmów szybkiej ich dystrybucji wewnątrz sektora,
    c. dalsza poprawa i ujednolicenie standardów oraz sposobów reagowania w sytuacjach cyberzagrożenia w sektorze finansowym,

   d. wypracowanie kompletnego techniczno-organizacyjnego rozwiązania centralnego (hub PolishApi) bazującego na dostępnej infrastrukturze sektorowej w zakresie ochrony zmieniających się procesów biznesowych wynikających z wprowadzenia dyrektywy PSD2 oraz wdrożonej ustawy o tożsamości cyfrowej (mojeID),

   e. wypracowanie i implementacja dla całego sektora bankowego zcentralizowanego systemu wykrywania nadużyć, w szczególności centralizacji funkcji AML, pracującego w trybie rzeczywistym (bazując na systemie STIR), jak również regularne organizowanie ćwiczeń i testów postępowania w sytuacjach kryzysowych z realnymi scenariuszami zagrożeń,

   f. rozszerzenie współpracy pomiędzy sektorami oraz jednostkami administracji publicznej,

2. wypracowanie koncepcji formalno-prawnej i systemowej implementacji chmury obliczeniowej o zasięgu sektorowym i międzysektorowym uwzględniającej wymagania regulacyjne w Polsce,

3. skoordynowanie przez BCC spójności wypracowanych rozwiązań, jak również nadzór nad wdrożeniem optymalnych mechanizmów bezpieczeństwa w ramach wprowadzania kluczowych regulacji.

INFORMACJA I EDUKACJA

1. kontynuowanie i koordynacja działań informacyjno-edukacyjnych wśród klientów instytucji finansowych zmierzających do podniesienia poziomu świadomości dotyczącej zagrożeń i możliwości ochrony:

   a. wypracowanie sposobu oraz określenie źródeł finansowania i zasad partycypacji podmiotów w przeprowadzeniu kampanii bezpieczeństwa skierowanej do klientów sektora finansowego,

   b. wypracowanie oraz wdrożenie nowoczesnych standardów i form komunikacyjnych zapewniających maksymalnie szeroki przekaz informacji dotyczących cyberbezpieczeństwa,

   c. podjęcie działań zmierzających do opracowania międzysektorowych kampanii informacyjno-edukacyjnych,

2. zdefiniowanie i określenie potrzeb sektora finansowego pod względem profilu kompetencyjnego z obszaru cyberbezpieczeństwa, a także opracowanie i wdrożenie odpowiedniego programu edukacyjnego przy współpracy z organami oświaty i administracji publicznej.