EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
ul. Do Studzienki 63
80-227 Gdańsk

tel. 58 524 49 01
fax. 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Rekomendacja Europejskiego Kongresu Finansowego 2017

Cyberbezpieczeństwo sektora finansowego

Mimo aktywnych działań w zakresie cyberbezpieczeństwa realizowanych sektorowo i indywidualnie przez instytucje finansowe ochrona przed zagrożeniem ze strony cyberprzestępców jest w dalszym ciągu jednym z najistotniejszych wyzwań stojących przed sektorem finansowym.

Kontynuując i rozwijając dotychczasowe działania, Europejski Kongres Finansowy po raz kolejny pragnie podkreślić istotę zagadnienia poprzez wydanie poniższej Rekomendacji.

Cele:

1. Zapewnienie efektywnej, kompleksowej i spójnej ochrony instytucji finansowych.
2. Zwiększenie świadomości zagrożeń i możliwości ochrony wśród klientów instytucji sektora finansowego poprzez zdefiniowanie spójnych form przekazu.
3. Operacjonalizacja współpracy wewnątrz sektora oraz międzysektorowych działań z zakresu cyberbezpieczeństwa.
4. Stworzenie odpowiednich i bezpiecznych warunków do implementacji przepisów prawa.

Rekomendacje

INFORMACJA I EDUKACJA

1. Intensyfikacja działań informacyjno-edukacyjnych zmierzających do podniesienia poziomu świadomości zagrożeń i możliwości ochrony wśród klientów instytucji finansowych:
    a. Przeprowadzenie analizy zapotrzebowania klientów sektora finansowego w kwestii zakresu, sposobu i formy informowania o zagadnieniach dotyczących cyberbezpieczeństwa.
    b. Wypracowanie oraz wdrożenie nowoczesnych standardów i form komunikacyjnych zapewniających maksymalnie szeroki zakres przekazu informacji dotyczących cyberbezpieczeństwa.
    c. Podjęcie działań zmierzających do opracowania międzysektorowych kampanii informacyjno-edukacyjnych.
2. Zdefiniowanie i określenie potrzeb sektora finansowego w zakresie profilu kompetencyjnego z obszaru cyberbezpieczeństwa, wypracowanie oraz wdrożenie odpowiedniego programu edukacyjnego przy współpracy z organami oświaty.

DZIAŁANIA STRATEGICZNE I OPERACYJNE

1. Zacieśnienie współpracy wewnątrzsektorowej z wykorzystaniem Bankowego Centrum Cyberbezpieczeństwa:
    a. Intensyfikacja prac nad stworzeniem docelowych mechanizmów umożliwiających szybką i bezpieczną wymianę informacji.
    b. Wdrożenie na poziomie sektora ciągłego procesu poszukiwania informacji o podatnościach i zagrożeniach we wszystkich dostępnych zasobach oraz mechanizmów szybkiej dystrybucji odnalezionych informacji wewnątrz sektora.
    c. Stworzenie zestawów reguł i procedur postępowania, które mają na celu poprawę i ujednolicenie sposobów reagowania w określonych sytuacjach związanych z cyberbezpieczeństwem z uwzględnieniem sytuacji kryzysowych.
    d. Wdrożenie jednolitej polityki informacyjnej o zdarzeniach z zakresu cyberbezpieczeństwa.
    e. Regularne organizowanie ćwiczeń postępowania w sytuacjach kryzysowych w oparciu o realne scenariusze zagrożeń.
2. Kontynuacja współpracy międzysektorowej ze szczególnym naciskiem na kooperację z Narodowym Centrum Cyberbezpieczeństwa oraz jednostkami administracji publicznej.
3. Skoordynowanie przez BCC spójności wypracowanych rozwiązań, jak również nadzór nad wdrożeniem optymalnych mechanizmów bezpieczeństwa w ramach wprowadzania kluczowych regulacji (PSD II, RODO, eIDAS).