EUROPEAN FINANCIAL CONGRESS

CYBERBEZPIECZEŃSTWO SEKTORA FINANSOWEGO

Zarządy największych banków w Polsce wskazują, że cyberbezpieczeństwo jest kluczowym wyzwaniem, z którym sektor musi się zmierzyć w najbliższym czasie. Niniejsza rekomendacja jest rozwinięciem rekomendacji dotyczącej cyberbezpieczeństwa z 2015 roku.

Cele

1. Zapewnienie efektywnej, spójnej, jednolitej ochrony instytucji finansowych.
2. Zapewnienie bezpieczeństwa obecnie funkcjonujących i planowanych rozwiązań w sektorze finansowym.
3. Wykorzystanie doświadczeń z zakresu cyberbezpieczeństwa sektora finansowego w działaniach realizowanych we współpracy z Narodowym Centrum Cyberbezpieczeństwa (NCC).

Rekomendowane działania

1. Kontynuacja koordynacji działań sektora finansowego w zakresie wymiany informacji i przeciwdziałania cyberzagrożeniom w ramach powstałego Bankowego Centrum Cyberbezpieczeństwa (BCC).
2. Współdziałanie z Narodowym Centrum Cyberbezpieczeństwa:
   - wdrożenie modelu i struktury współpracy BCC i NCC;
   - wprowadzenie procesów umożliwiających szybkie wykrywanie zagrożeń dotyczących świadczonych usług cyfrowych i reagowanie na nie, z uwzględnieniem zaangażowania organów ścigania;
   - zdefiniowanie kluczowych międzybankowych procesów biznesowych podlegających monitoringowi bezpieczeństwa w trybie 24/7;
   - współpraca z innymi kluczowymi sektorami.
3. Wypracowanie wraz z firmami telekomunikacyjnymi, dostawcami usług internetowych i firmami technologicznymi wspólnych standardów oraz zdefiniowanie działań mających na celu podniesienie poziomu bezpieczeństwa użytkownika końcowego.
4. Opracowanie powszechnego programu edukacyjno-informacyjnego dla obywateli w zakresie bezpiecznego korzystania z internetu oraz bankowości elektronicznej, czy też szerzej – usług cyfrowych.
5. Zdefiniowanie i wdrożenie w ramach działalności BCC katalogu wspólnych usług dotyczących bezpieczeństwa dla uczestników sektora bankowego w celu wyrównania i zapewnienia wysokiego poziomu bezpieczeństwa (m.in. rozwiązania anty-fraud, anty-phishing, analiza złośliwego oprogramowania).
6. Współpraca uczestników sektora bankowego przy implementacji regulacji krajowych i europejskich (m.in. PSD II, eIDAS) w celu zapewnienia jednolitych standardów i mechanizmów bezpieczeństwa, z zachowaniem dobrych praktyk i zasad bezpieczeństwa przyjętych w polskim systemie bankowym; w szczególności utrzymania zasady poufności narzędzi uwierzytelniających wykorzystywanych w bankowości elektronicznej.