EUROPEAN FINANCIAL CONGRESS

TECHNOLOGIE I CYBERBEZPIECZEŃSTWO

Rekomendacje zostały opracowane na podstawie dyskusji *Technologicznego Okrągłego Stołu EKF* oraz eksperckiej debaty na temat cyberbezpieczeństwa w sektorze bankowym podczas Europejskiego Kongresu Finansowego 2026.

1

EUROPEAN FINANCIAL CONGRESS

CYBERBEZPIECZEŃSTWO

Coraz większa skala wspieranych przez AI ataków ukierunkowanych na klientów banków, działania dezinformacyjne oraz rozwój zaawansowanych technik socjotechnicznych, zwiększają ryzyko podważania zaufania do usług cyfrowych. Jednocześnie cyberbezpieczeństwo sektora bankowego wykracza poza sam sektor i wymaga ścisłej współpracy z dostawcami usług cyfrowych, operatorami telekomunikacyjnymi oraz administracją publiczną.

Rekomendacje:

- Wzmacnianie bezpieczeństwa klientów banków poprzez rozwój narzędzi ochronnych, edukację oraz wspólne kampanie zwiększające świadomość zagrożeń związanych z AI, socjotechniką i dezinformacją.
- Rozwój sektorowych mechanizmów ograniczania nadużyć i oszustw, w szczególności rozwiązań wspólnych dla całego sektora, obejmujących wymianę informacji, przeciwdziałanie fraudom oraz usługi oparte na weryfikacji danych.
- Pogłębianie współpracy sektora bankowego z podmiotami infrastruktury krytycznej i administracją publiczną w celu budowy odporności systemowej oraz skutecznej ochrony procesów krytycznych dla państwa.

2

GENERATYWNA SZTUCZNA INTELIGENCJA

Sztuczna inteligencja przestaje być wyłącznie narzędziem poprawy efektywności, staje się jednym z głównych czynników umożliwiających transformację modeli operacyjnych, obsługi klienta oraz organizacji pracy. Skuteczne wykorzystanie AI wymaga równoczesnej transformacji procesów, rozwoju kompetencji oraz zapewnienia zgodności z regulacjami, zasadami etycznymi i wymaganiami bezpieczeństwa.

Rekomendacje:

- Uwzględnienie AI jako trwałego elementu strategii banków i transformacji cyfrowej organizacji.
- Dostosowanie procesów operacyjnych i modeli pracy do efektywnego wykorzystania generatywnej i agentowej AI, z zachowaniem zasady human-in-the-loop bądź human-in-the-lead.
- Rozwój kompetencji pracowników w zakresie praktycznego wykorzystania AI oraz przygotowanie organizacji do nowych ról i sposobów pracy.
- Wykorzystanie AI do zwiększenia produktywności, jakości obsługi klientów oraz rozwoju nowych modeli interakcji, w tym bankowości konwersacyjnej.
- Zapewnienie zgodności wdrożeń AI z wymaganiami regulacyjnymi, zasadami etycznymi, ochroną własności intelektualnej oraz cyberbezpieczeństwem.

3

EUROPEAN FINANCIAL CONGRESS

MODERNIZACJA SYSTEMÓW BANKOWYCH

Architektura IT polskiego sektora bankowego wymaga dalszej modernizacji w kierunku modularności, interoperacyjności oraz odporności operacyjnej. Transformacja technologiczna staje się warunkiem pełnego wykorzystania potencjału AI, utrzymania konkurencyjności wobec fintechów i nowych uczestników rynku oraz zapewnienia długoterminowej stabilności sektora.

Rekomendacje:

- Kontynuacja działań ograniczających dług technologiczny oraz modernizacja systemów centralnych jako element budowy odporności i konkurencyjności sektora.
- Projektowanie architektury w oparciu o modularność, interoperacyjność i automatyzację, umożliwiające szybsze, bezpieczniejsze oraz bardziej efektywne wdrażanie nowych usług i technologii.
- Wykorzystanie AI do wspierania rozwoju, utrzymania i testowania systemów przy jednoczesnym zachowaniu wymagań bezpieczeństwa i stabilności. Wymiana doświadczeń pomiędzy instytucjami w zakresie modernizacji architektury oraz wykorzystania dobrych praktyk technologicznych.

4

CIĄGŁOŚĆ DZIAŁANIA BANKÓW I CYFROWEJ GOSPODARKI

Rosnąca niestabilność geopolityczna, nowe obowiązki regulacyjne oraz uznanie sektora bankowego za element systemu bezpieczeństwa państwa zwiększają znaczenie odporności operacyjnej. Zapewnienie ciągłości działania wymaga dziś nie tylko przygotowania pojedynczych instytucji, lecz także skoordynowanych działań sektorowych i międzysektorowych.

Rekomendacje:

- Przejście od planowania do regularnego testowania zdolności działania w scenariuszach kryzysowych obejmujących sektor finansowy i jego kluczowych partnerów.
- Uzgodnienie procesów krytycznych, zasad współpracy oraz modeli komunikacji pomiędzy sektorem bankowym, administracją publiczną i operatorami infrastruktury krytycznej.
- Uwzględnianie w planach ciągłości działania zmieniającego się katalogu zagrożeń, w tym ryzyk geopolitycznych, technologicznych i związanych z łańcuchem dostaw.
- Rozwijanie zdolności do utrzymania kluczowych usług finansowych w warunkach długotrwałych zakłóceń funkcjonowania gospodarki.