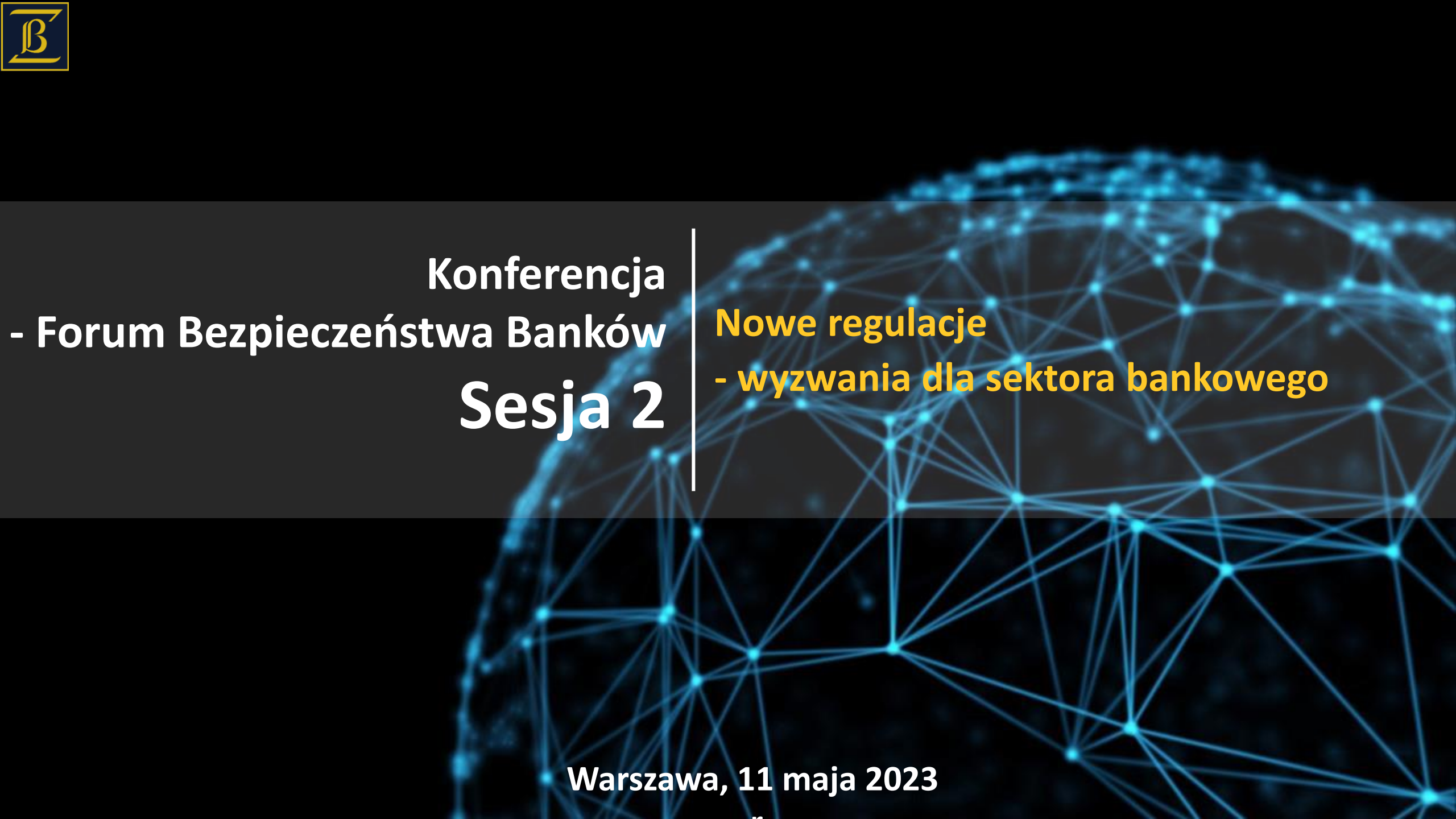
Konferencja
- Forum Bezpieczeństwa Banków
Sesja 2

Nowe regulacje
- wyzwania dla sektora bankowego



Warszawa, 11 maja 2023

Ustawa o zapobieganiu kradzieży tożsamości (zastrzeganie pesel)

Projekt ustawy o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości (UD472) – etap konsultacji (Rada Ministrów).

Projekt wprowadza możliwość zastrzeżenia numeru pesel – ochrona przed zaciągnięciem zobowiązania.

Zostanie utworzony rejestr zastrzeżeń numerów PESEL (odnotowanie zastrzeżenia i cofnięcia zastrzeżenia PESEL)

Cel: uniknięcie ryzyka wyłudzenia zobowiązania na skradzioną tożsamość.

Zastrzeżenie: przez Internet (profil zaufany) lub online w systemie transakcyjnym. Osobiście w dowolnym urzędzie gminy,

w placówce Poczty Polskiej lub banku krajowym.

Cofnięcie: osobiście w dowolnym urzędzie gminy.

Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej

Projekt skierowano do Sejmu

Celem ustawy jest walka ze zjawiskiem spoofing’u, smishing’u oraz innych nadużyć w komunikacji elektronicznej (w tym ataków DoS, DDoS)

W uzasadnieniu podano:

Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu, niż obecnie, ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników.

Obowiązki przedsiębiorców telekomunikacyjnych

Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane ze zwalczaniem nadużyć w komunikacji elektronicznej.

Przedsiębiorcy telekomunikacyjnie będą obowiązani, w szczególności do:

1) **podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu przeciwdziałanie nadużyciom w komunikacji elektronicznej;**
2) **blokowania krótkich wiadomości tekstowych, które zawierają treści zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK;**
3) **blokowania połączeń głosowych, które mają na celu podszywanie się pod inną osobę lub instytucję.**

Calling Line Identity (CLI) Spoofing, Caller ID spoofing

Wykaz numerów służących wyłącznie do odbierania połączeń głosowych

- W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny będzie zobligowany do blokowania połączeń głosowych albo ukrywania identyfikacji numeru wywołującego dla użytkownika końcowego.
- Zgodnie z projektem, Prezes Urzędu Komunikacji Elektronicznej będzie prowadził wykaz numerów służących wyłącznie do odbierania połączeń głosowych i będzie publikował wykaz w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.
- Prezes UKE będzie dokonywał wpisu numeru do wykazu na wniosek:
  - Banków,
  - Firm inwestycyjnych
  - Funduszy inwestycyjnych
  - Instytucji płatniczych
  - Jednostki sektora finansów publicznych
  - KSKOK
  - TFI
  - SKOK
  - Instytucji kredytowej
  - Zakładów ubezpieczeń i zakładów reasekuracji

Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu numeru do wykazu, będzie zobligowany do blokowania połączeń przychodzących do jego sieci z wykorzystaniem numeru wpisanego do tego wykazu.

Pozostałe rozwiązania

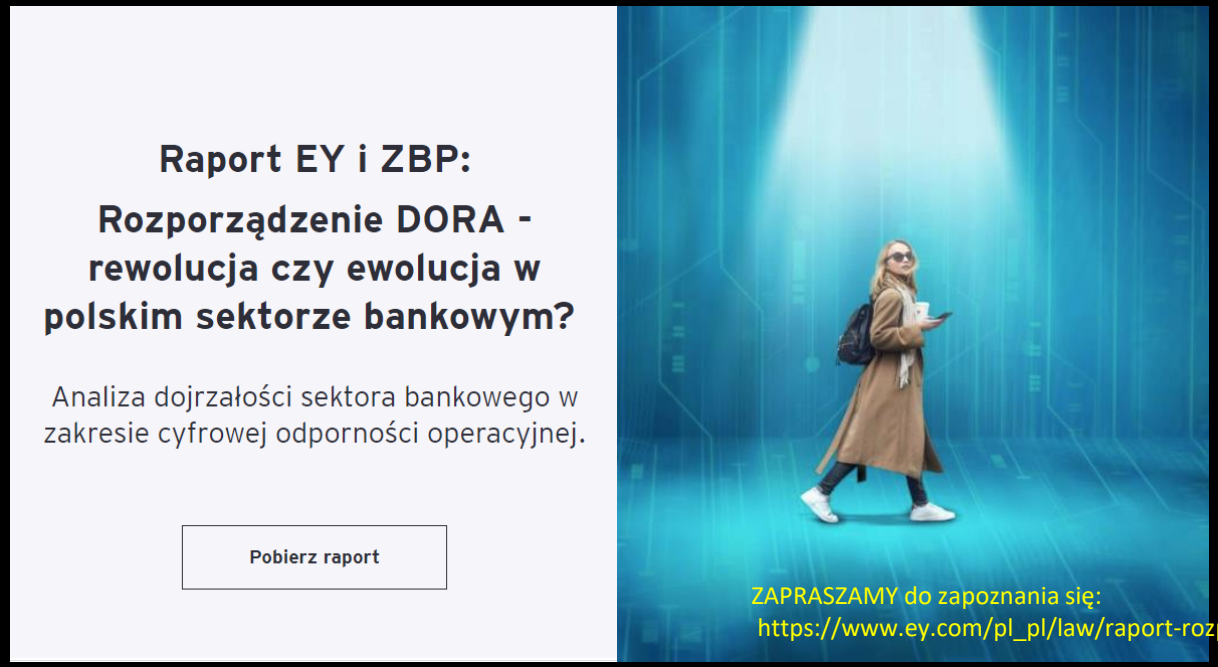
- Zespół CSIRT NASK będzie monitorował występowanie smishingu i przekazywał przedsiębiorcom telekomunikacyjnym wzorce wiadomości wskazujące na wystąpienie smishingu.
- Na listę ostrzeżeń wpisywane będą domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i doprowadzenie do wyłudzenia ich danych lub niekorzystnego rozporządzenia środkami finansowymi.
- Każdy będzie mógł zgłosić domenę internetową mogącą służyć do wyłudzeń danych i środków finansowych do CSIRT NASK. Zgłoszenie domeny internetowej może zawierać uzasadnienie.
- Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej.
- Podmiot posiadający tytuł prawny do domeny internetowej wpisanej na listę ostrzeżeń będzie mógł wnieść do Prezesa UKE sprzeciw wobec wpisania domeny internetowej na listę ostrzeżeń.

Przedsiębiorca telekomunikacyjny, który dokona następujących nadużyć w komunikacji elektronicznej: generowania sztucznego ruchu, smishingu, CLI spoofingu, nieuprawnionej zmiany informacji adresowej będzie podlegał karze pieniężnej.

DORA i NIS2

– opublikowane 27.12.2022 r.

- DORA (Digital Operational Resilience Act) - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego.
- DORA weszła w życie 17 stycznia 2023 roku, a obowiązek stosowania nastąpi 17 stycznia 2025 r.
- NIS2 (The Network and Information Security Directive 2) - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.
- Dyrektywa NIS2 weszła w życie 17 stycznia 2023 roku. Jako dyrektywa podlega obowiązkowi implementacji przez państwa członkowskie do krajowych porządków prawnych. Transpozycja ma nastąpić do 17 października 2024 roku, do kiedy to państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania dyrektywy i stosują te przepisy od 18 października 2024 r.



ZAPRASZAMY do zapoznania się:
https://www.ey.com/pl_pl/law/raport-rozporzadzenie-dora-rewolucja-czy-ewolucja-w-polskim-sektorze-bankowym

DORA – kontekst wymiany informacji

W art. 45 DORA przewidziano możliwość prowadzenia międzybankowej wymiany informacji i danych wywiadowczych na temat cyberzagrożeń.

Ma to służyć zwiększeniu świadomości na temat ryzyka związanego z ICT, zminimalizować jego rozprzestrzenianie się, wspierać zdolności obronne podmiotów finansowych oraz techniki wykrywania zagrożeń.

DORA wskazała, że podmioty finansowe wymieniają się informacjami w zaufanych społecznościach i mogą do tej wymiany na określonych warunkach zaprosić organy publiczne.

Celem tego przepisu jest realizacja m.in. motywu 32 DORA, czyli umożliwienie podmiotom finansowym zapobieganie zagrożeniom i wspólne reagowanie na nie, poprzez ograniczenie rozpowszechnienia skutków materializacji ryzyka związanego z ICT i utrudnienie wystąpienia potencjalnego efektu domina dla wszystkich uczestników rynku usług finansowych.

Art. 45 upoważnia banki (też inne podmioty finansowe) do współpracy na polu wymiany informacji. Podmioty finansowe mogą wymieniać między sobą informacjami i wynikami analiz takiego cyberzagrożenia, jeżeli udział w zrzeszeniu:

- ma na celu zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych;
- zapewnienie ochrony potencjalnie poufnego charakteru wymienianych informacji;
- opiera się na ustalonych zasadach z pełnym poszanowaniem tajemnicy przedsiębiorstwa, ochrony danych osobowych i wytycznych dotyczących polityki konkurencji;
- opiera się na ustalonych warunkach przystąpienia.

Sesja 2
Nowe regulacje – wyzwania dla sektora bankowego

Maciej Górski, Dyrektor Departamentu Zarządzania Systemami, Kancelaria Prezesa Rady Ministrów

Paweł Rzewuski, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, Urząd Komisji Nadzoru Finansowego

mł. insp. Piotr Tofiluk, Naczelnik Wydziału Nadzoru i Koordynacji, Centralne Biuro Zwalczania Cyberprzestępczości

Daniel Krzywiec, Dyrektor Departamentu Cyberbezpieczeństwa, SGB-Bank SA

Andrzej Karpiński, Dyrektor Departamentu Bezpieczeństwa, Biuro Informacji Kredytowej

Justyna Wilczyńska-Baraniak, Partner EY Law, Lider Zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych, EY Polska

Jarosław Biegański – Zastępca Dyrektora Zespołu Bezpieczeństwa Banków, Związek Banków Polskich - *Moderator*

Zapraszam do dyskusji