Wstęp

Dzień dobry wszystkim.

Dzisiejszym tematem naszej prezentacji są regulacje prawne dotyczące cyberbezpieczeństwa w finansach — czyli wszystko to, co sprawia, że nasze pieniądze nie znikają z konta szybciej niż kieszonkowe po wypłacie. Cyberbezpieczeństwo może brzmieć jak jakaś nudna informatyczna gadka, ale w rzeczywistości to coś, co decyduje o tym, czy ktoś nam ukradnie dane, przejmie konto bankowe albo zrobi zakupy za nasze pieniądze, kiedy my śpimy.

Podczas tej prezentacji wyjaśnimy takie pojęcia jak: RODO, PSD2, KSC, DORA, NIS2 oraz silne uwierzytelnianie klienta. Celem jest pokazanie, że bez tych przepisów sektor finansowy działałby jak bank bez drzwi — niby stoi, ale każdy mógłby wejść i wynieść, co chce.

Slajd 1 – Dlaczego cyberbezpieczeństwo jest ważne

Na początku warto odpowiedzieć sobie na pytanie: po co w ogóle mówić o cyberbezpieczeństwie?

Sektor finansowy to jedno z ulubionych miejsc cyberprzestępców. Tam są pieniądze, dane, konta, transakcje — czyli wszystko, co można ukraść, zhakować albo sprzedać. Bez odpowiednich regulacji człowiek w intrenecie jest jak turysta w obcym kraju bez mapy — niby idzie, ale nie wie dokąd i łatwo go oskubać.

Znajomość podstawowych zasad cyberbezpieczeństwa pomaga chronić swoje dane, pieniądze i nie dać się zrobić w bambuko.

Slajd 2 – RODO

RODO to europejskie rozporządzenie dotyczące ochrony danych osobowych. W skrócie: banki i firmy muszą pilnować naszych danych jak oka w głowie.

Jeśli dojdzie do naruszenia, mają 72 godziny na zgłoszenie tego odpowiednim instytucjom. RODO powstało po to, żeby nasze dane nie latały po Internecie jak ulotki na wietrze.

Slajd 3 – PSD2

PSD2 to dyrektywa dotycząca płatności elektronicznych. Wprowadza **silne uwierzytelnianie klienta (SCA)**, czyli dodatkowe potwierdzanie tożsamości.

Tak, to przez PSD2 musimy potwierdzać każdą transakcję kodem, odciskiem palca albo aplikacją. Czasem wkurza, ale dzięki temu nikt nie kupi sobie nowego telefonu za nasze pieniądze, bo zna nasze hasło z 2015 roku.

Slajd 4 – KSC

KSC, czyli Ustawa o Krajowym Systemie Cyberbezpieczeństwa, to polskie przepisy regulujące bezpieczeństwo usług kluczowych — w tym banków.

Określa, co instytucje muszą robić, żeby działać stabilnie i nie padły po jednym większym cyberataku. Bez KSC banki mogłyby działać „na słowo honoru”, a to w finansach działa mniej więcej tak dobrze jak parasol z dziurą.

Slajd 5 – DORA

DORA to nowe unijne rozporządzenie dotyczące odporności cyfrowej instytucji finansowych.

Wymaga testów bezpieczeństwa, kontroli dostawców IT, planów awaryjnych i gotowości na incydenty. Dzięki temu banki mają działać nawet wtedy, gdy w Internecie dzieje się totalny chaos.

Slajd 6 – NIS2

NIS2 to dyrektywa, która podnosi poziom cyberbezpieczeństwa w sektorach kluczowych, takich jak energetyka, transport, zdrowie i oczywiście finanse.

Ma sprawić, że państwa UE będą lepiej przygotowane na cyberzagrożenia — bo dziś atak na systemy informatyczne może wyrządzić więcej szkód niż niejedna tradycyjna broń.

Slajd 7 – Silne uwierzytelnianie klienta (SCA)

SCA to dodatkowe potwierdzanie tożsamości podczas logowania lub płatności.

Może to być:

- coś, co **wiesz** (hasło),
- coś, co **masz** (telefon),
- coś, czym **jesteś** (odcisk palca, twarz).

Dzięki temu cyberprzestępcy mają trudniej, a my mamy większe bezpieczeństwo — nawet jeśli czasem musimy klikać więcej niż byśmy chcieli.

Slajd 8 – Incydenty bezpieczeństwa

Incydent bezpieczeństwa to każde zdarzenie, które narusza poufność, integralność lub dostępność danych.

Może to być:

- włamanie do systemu,
- wyciek danych,
- atak hackerski,
- awaria serwera.

Instytucje finansowe muszą takie incydenty zgłaszać i reagować na nie natychmiast, żeby nie doszło do większych szkód.

Slajd 9 – Podsumowanie

Podsumowując, poznaliśmy dziś najważniejsze regulacje dotyczące cyberbezpieczeństwa w finansach. RODO, PSD2, KSC, DORA i NIS2 tworzą fundament bezpieczeństwa cyfrowego, który chroni nasze dane, pieniądze i stabilność gospodarki.

Bez tych przepisów sektor finansowy działałby jak bankomat bez PIN-u — niby działa, ale każdy mógłby z niego korzystać. A teraz przejdźmy do quizu, żeby sprawdzić, ile z tego zapamiętaliście.