Podczas zajęć z informatyki uczniowie klasy 8 Zespołu Szkół nr 2 w Sosnowcu zaprezentowali prezentację pt. **„Regulacje prawne dotyczące cyberbezpieczeństwa w finansach”**, której celem było wyjaśnienie, dlaczego banki, płatności internetowe i dane klientów muszą być chronione jak skarb narodowy. Wystąpienie miało pokazać, że w cyfrowym świecie pieniądze to nie tylko cyferki na ekranie, ale coś, co może zniknąć szybciej niż bateria w telefonie, jeśli nie ma odpowiednich przepisów.

Dlaczego cyberbezpieczeństwo jest ważne?

Na początku uczniowie wyjaśnili, że cyberbezpieczeństwo to ochrona systemów, danych i usług przed atakami w sieci. Podkreślili, że sektor finansowy jest jednym z najczęściej atakowanych, bo tam są pieniądze — a gdzie są pieniądze, tam zawsze znajdzie się ktoś, kto chce je ukraść. Bez podstawowej wiedzy o cyberzagrożeniach człowiek jest jak użytkownik internetu bez antywirusa — niby działa, ale ryzyko katastrofy wisi nad nim cały czas.

RODO – dane osobowe pod specjalną ochroną

Jednym z kluczowych zagadnień było **RODO**, czyli europejskie rozporządzenie dotyczące ochrony danych osobowych. Uczniowie wyjaśnili, że banki muszą chronić dane klientów jak oka w głowie, a każde naruszenie trzeba zgłosić w ciągu 72 godzin. RODO ma zapobiegać sytuacjom, w których dane klientów wypływają do sieci szybciej niż memy po premierze nowego iPhone’a.

PSD2 – bezpieczeństwo płatności elektronicznych

Kolejnym pojęciem była **PSD2**, czyli dyrektywa regulująca płatności elektroniczne. Wprowadza ona **silne uwierzytelnianie klienta (SCA)** — czyli dodatkowe potwierdzanie tożsamości, żeby nikt nie zrobił zakupów za czyjeś pieniądze tylko dlatego, że zna jego hasło. Uczniowie podkreślili, że PSD2 zwiększa bezpieczeństwo, nawet jeśli czasem człowiek ma ochotę rzucić telefonem, bo musi potwierdzać każdą transakcję jakby kupował rakietę kosmiczną.

KSC – polskie zasady bezpieczeństwa

W prezentacji omówiono również **Ustawę o Krajowym Systemie Cyberbezpieczeństwa (KSC)**. To ona określa obowiązki operatorów usług kluczowych, takich jak banki. Uczniowie wyjaśnili, że KSC ma zapewnić, aby instytucje finansowe działały stabilnie i były przygotowane na cyberataki. Bez takich przepisów banki mogłyby działać „na słowo honoru”, a to w finansach działa mniej więcej tak dobrze, jak parasol z dziurą podczas ulewy.

DORA – odporność cyfrowa instytucji finansowych

Kolejnym ważnym elementem była **DORA**, czyli nowe unijne rozporządzenie dotyczące odporności cyfrowej. Uczniowie wyjaśnili, że DORA wymaga testów bezpieczeństwa, kontroli dostawców IT i gotowości na incydenty. Dzięki temu banki i inne instytucje finansowe mają działać stabilnie nawet wtedy, gdy w sieci dzieje się totalny chaos.

NIS2 – cyberbezpieczeństwo dla sektorów kluczowych

W prezentacji pojawiła się także dyrektywa **NIS2**, która podnosi poziom bezpieczeństwa w sektorach kluczowych, takich jak energetyka, transport czy finanse. Uczniowie podkreślili, że NIS2 ma sprawić, aby państwa UE były lepiej przygotowane na cyberzagrożenia — bo w XXI wieku atak na systemy informatyczne może wyrządzić więcej szkód niż niejedna tradycyjna broń.

Podsumowanie

Prezentacja pokazała, że regulacje prawne dotyczące cyberbezpieczeństwa są absolutnie niezbędne, aby chronić pieniądze, dane i stabilność gospodarki. RODO, PSD2, KSC, DORA i NIS2 tworzą fundament bezpieczeństwa cyfrowego, bez którego sektor finansowy działałby jak bank bez sejfu. Dzięki takim zajęciom uczniowie lepiej rozumieją, jak ważne jest prawo w świecie technologii i dlaczego cyberbezpieczeństwo to nie tylko informatyka, ale realna ochrona przed stratami, oszustwami i chaosem.

Mikołaj Ślęzak, klasa 8c