Zabezpieczenie danych osobowychw systemach bankowościinternetowej: wyzwaniai rozwiązania informatyczne

Dima Poliakov

Wprowadzenie

Bankowośćinternetowa stała sięintegralnączęściąwspółczesnego zarządzania finansami. Zwiększająca sięliczba transakcji online rodzi nowe wyzwania związane z bezpieczeństwem danych osobowych.Celem prezentacji jest omówienie wyzwań związanych z ochronądanych oraz przedstawienie dostępnych rozwiązań informatycznych.

Rola danych osobowych w bankowości internetowej

Dane osobowe wsystemach bankowych:imi,ę,nazwisko, adres,numer konta, dane karty płatniczej, historia transakcji.Wartośćtych danych: przyciągającone uwagę cyberprzestępców.Ochrona danych jest kluczowa zarówno dla banków, jak i dla klientów, aby zapobiec kradzieży tożsamości, oszustwom finansowym czy w yłu dze ni om.

Wyzwania związane z bezpieczeństwem danych osobowych

Cyberzagrożenia:Phishing, malware, ransomware.Ataki typu „Man-in-the-middle” (MITM) i przechwytywanie danych podczas transmisji.Błędy ludzkie:Nieświadome udostępnianie danych, używanie słabych haseł, brak aktualizacji oprogramowania.Złożonośćsystemów:Integracja różnych technologii i platform (mobilne aplikacje bankowe, internetowe systemy bankowe, systemy bezpieczeństwa).Brak świadomości użytkowników:Niska edukacja w zakresie cyberbezpieczeństwa.

Rozwiązania w bankowości internetowej

Bezpiecznesystemy autoryzacji:Zastosowanietokenów i certyfikatów.Używanie jednorazowych haseł (OTP).Monitorowanie i analiza ruchu sieciowego:Wykorzystanie sztucznej inteligencji (AI) do wykrywania anomalii.Systemy wykrywania i zapobiegania włamaniom (IDS/IPS).Zarządzanie dostępem i uprawnieniami:Przypisywanie minimalnych uprawnień, ochrona przed nieautoryzowanym dostępem do danych.

Co to jest 2FA?

2FA, czyli uwierzytelnianie dwuskładnikowe (ang. Two-Factor Authentication), to metoda zabezpieczania dostępu do konta lub usługi online, która wymaga dwóch różnych form weryfikacji tożsamości.

Przyszłośćochrony danych w bankowości internetowej

Rozwójsztucznejinteligencjiwwykrywaniu zagrożeń.Wzrostpopularnościrozwiązań opartych na blockchain do przechowywania danych i realizacji transakcji.Powszechne stosowanie biometrii oraz innych technologii tożsamościowych w bankowości mobilnej.Wzrost znaczenia edukacji użytkowników i świadomości cyberbezpieczeństwa.

Podsumowanie

Zabezpieczenie danych osobowych w bankowości internetowej jest kluczowe dla ochrony klientów oraz instytucji finansowych.Stosowanie nowoczesnych technologii, przestrzeganie norm prawnych oraz edukacja użytkowników stanowiąpodstawęskutecznej ochrony danych.Wyzwania wciążistnieją, ale rozwój technologii i świadomości zapewnia coraz lepsze zabezpieczenia.

Koniec

Dziękuję za uwagę