Politechnika Wrocławska
Wydział Informatyki i Telekomunikacji
Dokumentacja Projektowa

Aplikacja bankowości elektronicznej

Analiza ryzyka i reakcja na incydenty

Autorzy:
Tomasz Gudyka, Malwina Terelak

Elektronicznie
podpisany przez
Tomasz Gudyka 272240
Data: 2026.05.25
14:55:55 +02'00'

Marzec-Maj 2026

Spis treści

1 Opis projektu

Niniejsze opracowanie stanowi analizę ryzyka oraz plan reakcji na incydenty dla systemu lokalnej bankowości elektronicznej **SafeBank**. W warunkach komercyjnych, ze względu na stopień skomplikowania systemów klasy Enterprise, pełna analiza ryzyka jest procesem złożonym i wieloetapowym, realizowanym przez dedykowane zespoły (SecOps, Compliance, DevOps). W takim modelu każda grupa robocza analizuje wyznaczony segment architektury (np. moduł transakcyjny, bazy danych, integracje zewnętrzne), aby ostatecznie stworzyć kompleksowy obraz bezpieczeństwa organizacji.

Na potrzeby niniejszego projektu, zakres został celowo zawężony do krytycznego obszaru, jakim jest **ścieżka logowania i autoryzacji użytkowników**. Takie podejście pozwala na przeprowadzenie pogłębionej analizy ścieżki dostępu do systemu, która z perspektywy bezpieczeństwa banku stanowi najbardziej eksponowany punkt styku z potencjalnym agresorem i jest kluczowa dla zachowania poufności dostępów.

1.1 Cel i zakres analizy

Głównym celem projektu jest identyfikacja zagrożeń oraz ocena odporności procesów uwierzytelniania w platformie webowej banku. System logowania jest punktem, w którym krzyżują się procesy przetwarzania danych uwierzytelniających, metadanych sesyjnych oraz mechanizmów ochrony tożsamości. Analiza uwzględnia wymagania ochrony danych osobowych oraz standardy odporności operacyjnej sektora finansowego [12, 13].

W ramach projektu analizie podlegają wyłącznie funkcjonalności ścieżki logowania:

- proces bezpiecznego przesyłania poświadczeń (Login/Hasło) kanałami szyfrowanymi,
- mechanizmy autoryzacji wieloskładnikowej (MFA – Multi-Factor Authentication) [3, 17],
- zarządzanie sesją użytkownika i wystawianie tokenów autoryzacyjnych (JWT),
- mechanizmy ochrony przed atakami typu Brute-force, DDoS oraz Credential Stuffing [7, 11],
- interfejs API dla podmiotów zewnętrznych [8].

Wyłączenia z zakresu analizy: Zgodnie z przyjętymi założeniami projektowymi, aby zachować precyzję opisu wybranego segmentu, z analizy wyłączono:

- bezpieczeństwo fizyczne placówek stacjonarnych, bankomatów oraz dedykowane aplikacje mobilne,
- **wszelkie moduły funkcjonalne dostępne po zalogowaniu** (np. realizacja przelewów, zarządzanie produktami, historia transakcji),
- systemy bankowości korporacyjnej oraz rynków kapitałowych,
- systemy transakcyjne podmiotów trzecich oraz obsługę portfeli cyfrowych.

1.2 Metodyka analizy ryzyka

Analiza ryzyka została przeprowadzona w oparciu o uznane standardy międzynarodowe, łącząc podejście procesowe z oceną techniczną. Jako główne metodyki przyjęto *NIST SP 800-30 Rev. 1* (jako szkielet procesowy), *OWASP Risk Rating Methodology* (do technicznej oceny podatności aplikacji webowych) oraz wytyczne *KNF* dla sektora finansowego [14, 10, 5].

Proces analizy podzielono na etapy obejmujące: identyfikację źródeł zagrożeń specyficznych dla procesów uwierzytelniania, analizę podatności wybranych komponentów technicznych (w tym analizę znanych podatności CVE) oraz ocenę ryzyka z wykorzystaniem algorytmu *OWASP* [10]. Końcowym etapem jest dokumentacja wyników w formie rejestru ryzyk, uwzględniająca 5-stopniową matrycę dotkliwości (od bardzo niskiej do bardzo wysokiej), co pozwala na precyzyjne rozróżnienie ryzyka wbudowanego (*inherent*) od rezydualnego.

Szczegółowy aparat matematyczny, definicje poziomów prawdopodobieństwa i wpływu oraz macierz klasyfikacji zostały szczegółowo opisane w Rozdziale 3.

1.3 Kontekst prawny i ochrona danych

Projekt koncentruje się na przetwarzaniu danych o najwyższym stopniu wrażliwości — poświadczeń dostępowych stanowiących klucz do tajemnicy bankowej [15]. W ramach analizy uwzględniono obowiązki administratora wynikające z RODO w zakresie ochrony poufności i integralności procesów logowania [12] oraz wymogi dotyczące cyberodporności operacyjnej wynikające z rozporządzenia DORA [13], szczególnie w kontekście zapobiegania nieuprawnionemu dostępowi do systemów krytycznych oraz zapewnienia ciągłości procesów autoryzacji.

2 Architektura systemu

System SafeBank opiera się na architekturze trójwarstwowej, zaprojektowanej z myślą o wysokiej dostępności oraz ścisłej izolacji danych finansowych od publicznych sieci telekomunikacyjnych. Model ten jest zgodny z wymaganiami w zakresie bezpieczeństwa systemów teleinformatycznych w sektorze bankowym [4]. W niniejszym rozdziale przedstawiono całościowy model systemu w celu zapewnienia pełnego kontekstu operacyjnego. Zgodnie z przyjętymi założeniami projektowymi, **szczegółowa analiza ryzyka i podatności w dalszej części opracowania została zawężona wyłącznie do ścieżki logowania i autoryzacji użytkowników (ang. Login Path)**, co jest kluczowe dla spełnienia wymogów silnego uwierzytelniania klienta [3].

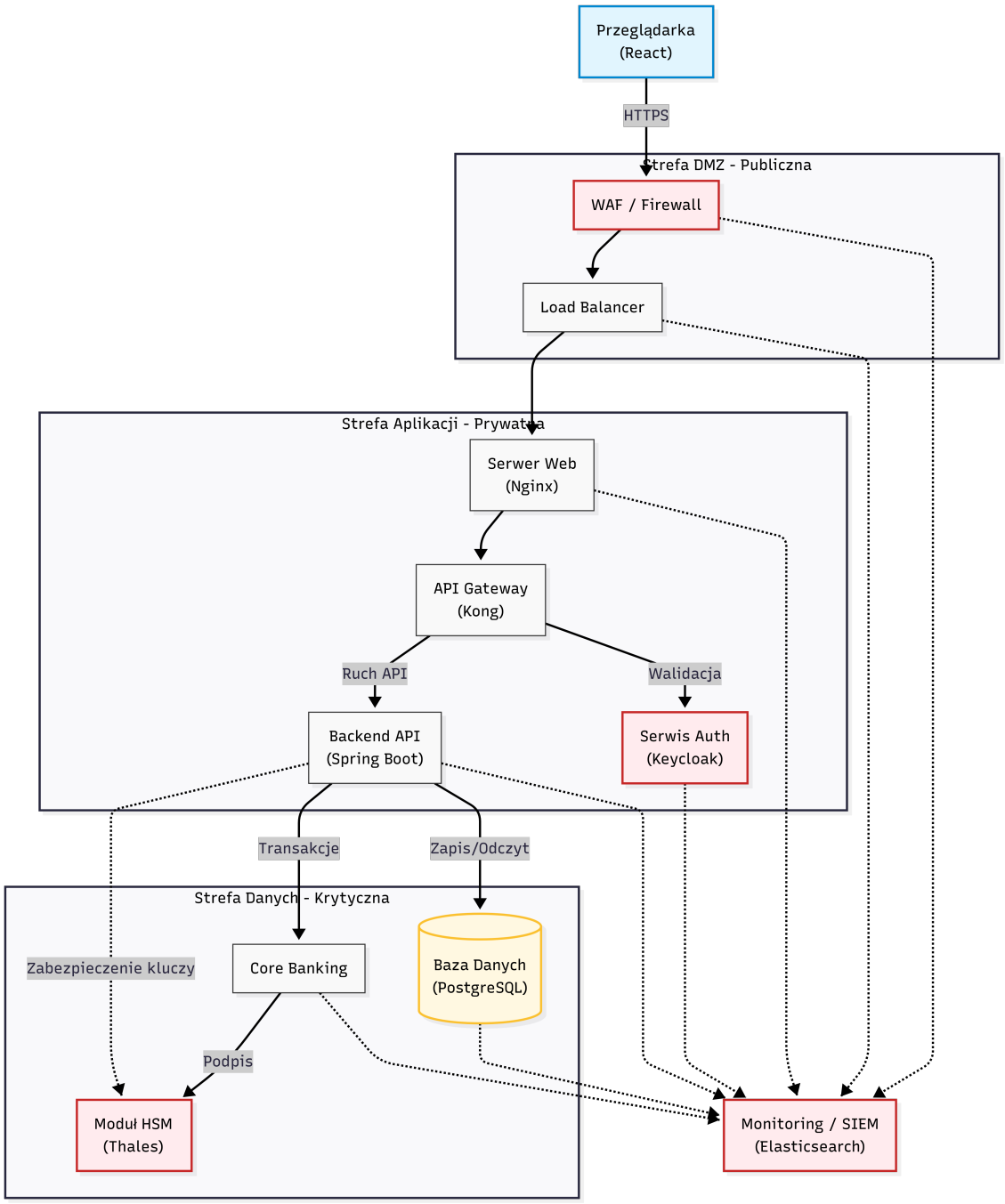
Takie podejście pozwala na przeprowadzenie pogłębionego badania ścieżki logowania do systemu, która z perspektywy bankowości elektronicznej stanowi najbardziej eksponowany punkt styku z potencjalnym agresorem i jest kluczowa dla zachowania poufności dostępów [7].

2.1 Schemat blokowy architektury

Architektura fizyczna i logiczna systemu została podzielona na trzy główne strefy sieciowe, odizolowane od siebie za pomocą systemów firewall oraz reguł routingu, zgodnie z najlepszymi praktykami segmentacji sieci [5]:

1. **Strefa publiczna (DMZ):** Pierwsza linia obrony, przyjmująca ruch z sieci Internet. Znajdują się tu mechanizmy WAF, Anty-DDoS oraz Load Balancer.
2. **Strefa aplikacji (Prywatna):** Zawiera logikę biznesową systemu (Backend), API Gateway oraz serwery uwierzytelniania. Ruch w tej strefie jest monitorowany i ograniczony wyłącznie do niezbędnych wywołań API [8].
3. **Strefa danych (Krytyczna):** Najbardziej chroniony segment sieci, w którym znajdują się bazy danych, system Core Banking oraz sprzętowe moduły bezpieczeństwa (HSM).

Poniżej przedstawiono Master Architekturę systemu (Rysunek 1), która stanowi tło dla wszystkich procesów bankowych.



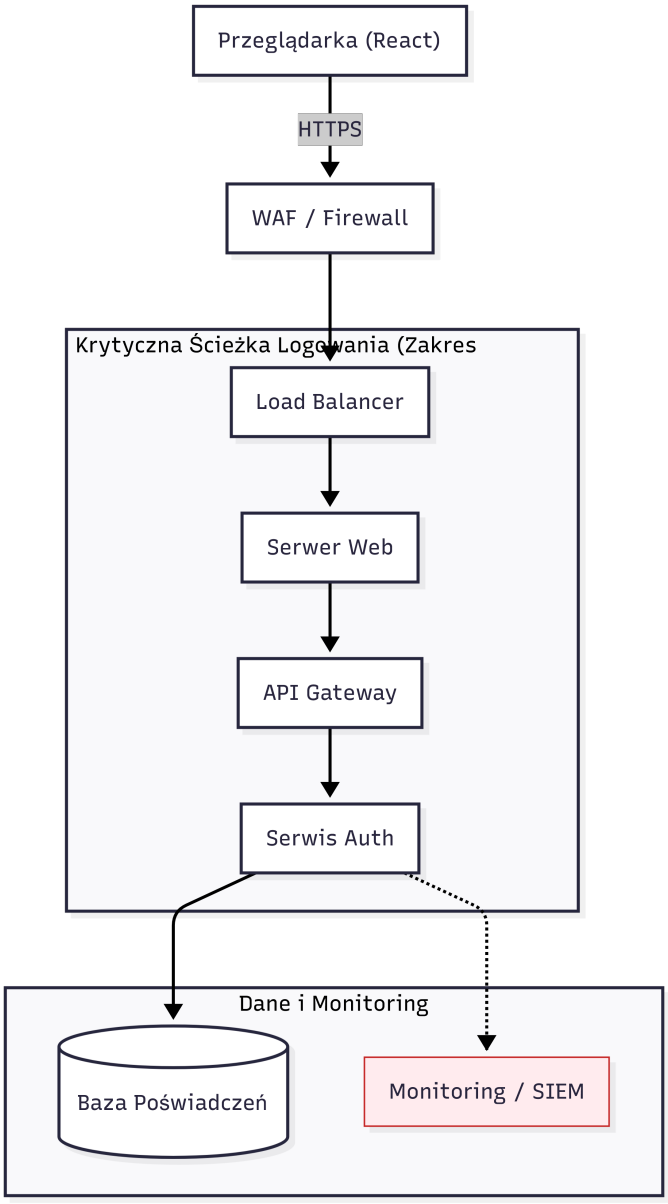
Rysunek 1: Całościowy schemat architektury systemu (Kontekst ogólny).

Przerywane linie na schemacie kierowane do SIEM oznaczają ciągłe przesyłanie zdarzeń do centralnego systemu monitorowania. Zapewnienie ciągłego nadzoru nad zdarzeniami jest kluczowym wymogiem w procesie reagowania na incydenty [6]. Poszczególne komponenty raportują następujące typy danych:

- **WAF/Firewall:** Logi bezpieczeństwa, zablokowane ataki, w tym próby wykorzystania błędów typu Injection [11].
- **Load Balancer:** Metryki ruchu sieciowego i obciążenia węzłów.
- **Serwer Web i API Gateway:** Logi dostępowe (Access logs) oraz metryki zapytań API [8].

- **Serwis Auth (Keycloak):** Zdarzenia logowania, błędne autoryzacje, zarządzanie sesją zgodnie ze standardami uwierzytelniania [17].
- **Backend API (Spring Boot):** Logi aplikacyjne, błędy wykonania, wyjątki w kodzie.
- **Baza Danych (PostgreSQL):** Logi audytowe (np. zapytania zmieniające strukturę lub wrażliwe dane) [15].
- **Core Banking i HSM:** Logi operacji transakcyjnych oraz błędne żądania kryptograficzne.

Ze względu na wybrany zakres analizy, na Rysunku 2 wyodrębniono komponenty bezpośrednio biorące udział w procesie „wejścia" użytkownika do systemu. Skupienie się na tym segmencie pozwala na precyzyjną ocenę mechanizmów MFA, ochrony przed atakami Brute-force oraz bezpieczeństwa przechowywania poświadczeń [17].

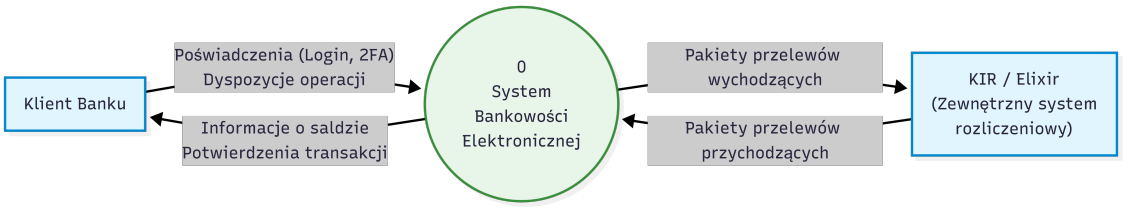


Rysunek 2: Architektura ścieżki logowania (Zakres szczegółowy analizy).

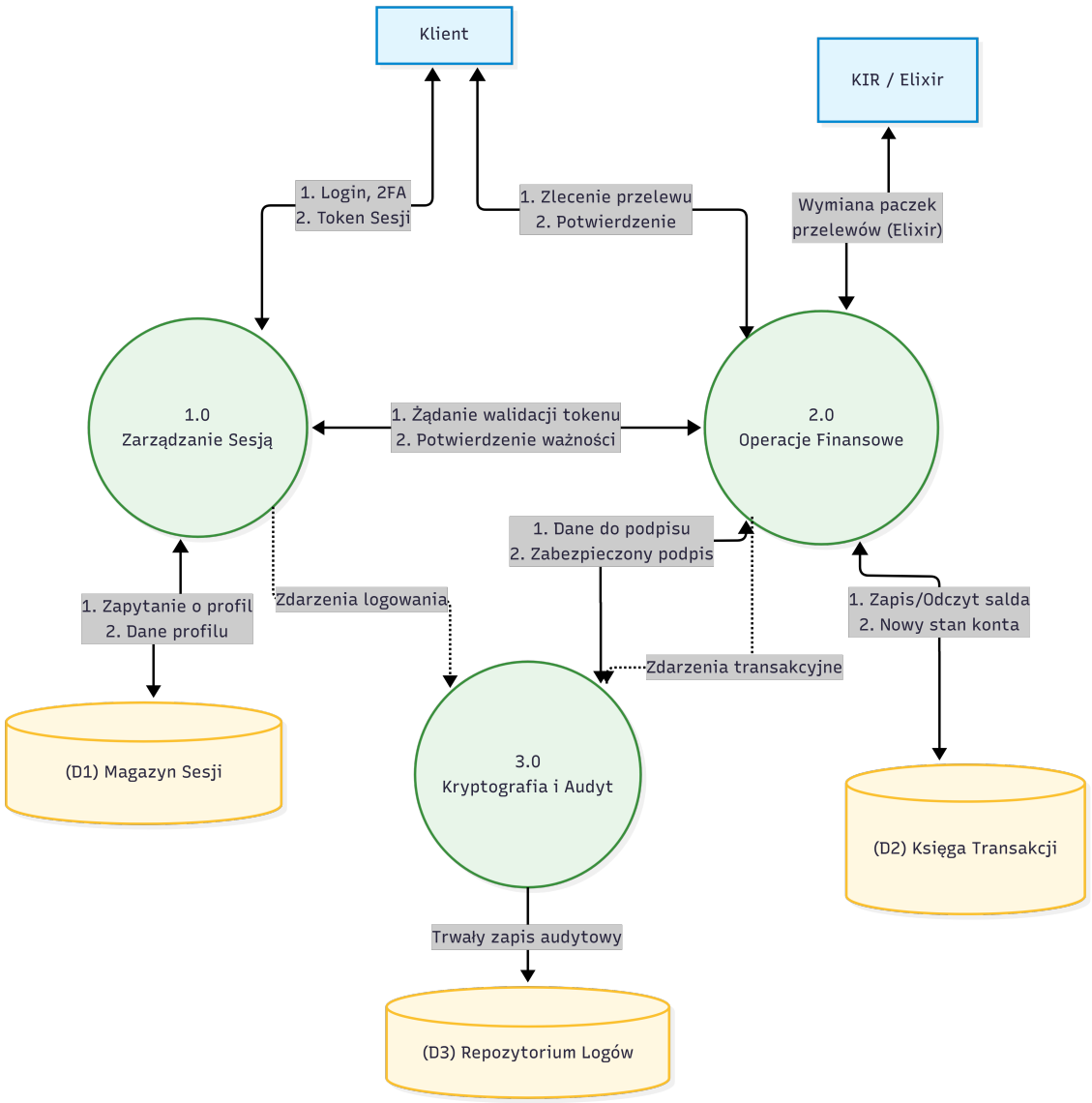
2.2 Diagramy przepływu danych (Data Flow Diagram)

W celu precyzyjnej identyfikacji punktów styku oraz potencjalnych wektorów ataków, przeprowadzono analizę przepływu danych (DFD). Podejście to pozwala na odizolowanie logicznego przetwarzania informacji od fizycznej architektury sieciowej, co ułatwia lokalizację miejsc przetwarzania danych osobowych podlegających ochronie [12].

Na poziomie kontekstowym – Poziom 0 (Rysunek 3), system wymienia informacje z Klientem oraz systemem rozliczeniowym KIR/Elixir. Poziom 1 (Rysunek 4) dekomponuje system na trzy główne procesy: Uwierzytelnianie (1.0), Operacje Finansowe (2.0) oraz Kryptografię i Audyt (3.0).

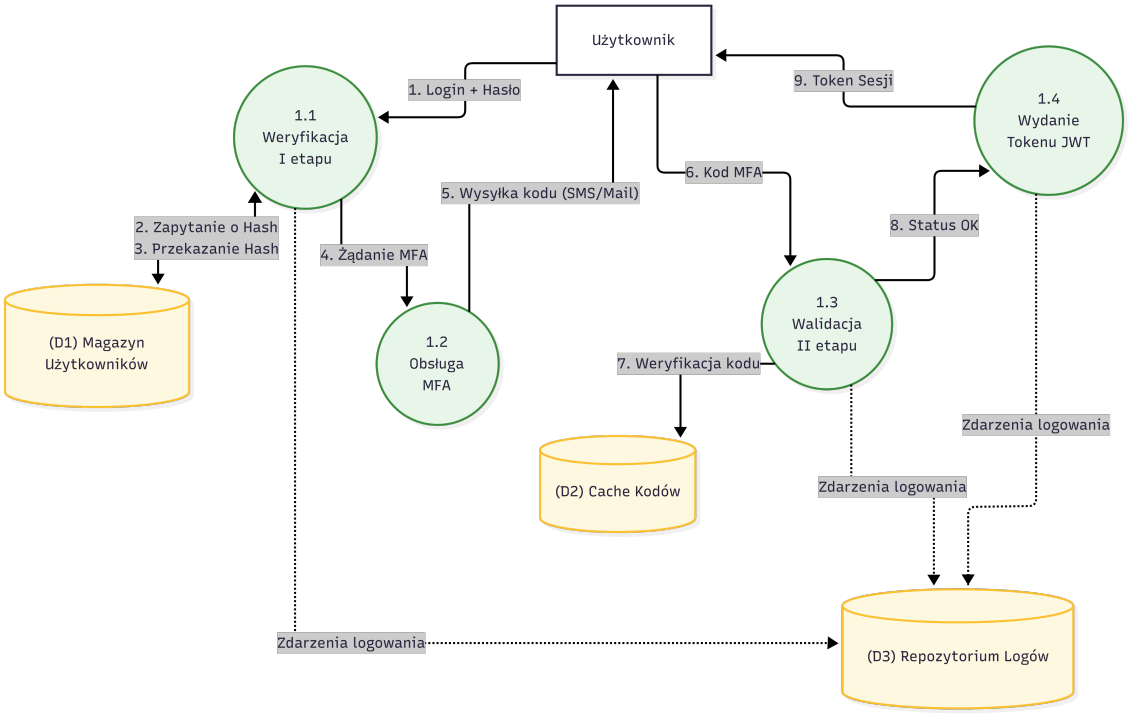


Rysunek 3: Data Flow Diagram poziom 0 (Diagram Kontekstowy).



Rysunek 4: Data Flow Diagram Poziom 1 (Dekompozycja funkcjonalna).

Zgodnie z przyjętym zakresem analizy, opracowano szczegółowy **Diagram Poziomu 2 (Rysunek 5)**, który dekomponuje Proces 1.0 (Uwierzytelnianie). Diagram ten przedstawia krytyczną logikę logowania dwuetapowego (MFA), w tym interakcje z magazynem haseł oraz tymczasowym cachem kodów autoryzacyjnych, zgodnie z wytycznymi dotyczącymi bezpiecznego uwierzytelniania [3, 17].



Rysunek 5: DFD Poziom 2: Szczegółowy przepływ procesu logowania i walidacji MFA.

2.3 Identyfikacja punktów przetwarzania danych osobowych

Mapowanie danych pozwala na nałożenie odpowiednich mechanizmów kontrolnych (maskowanie, szyfrowanie) w punktach o najwyższym priorytecie, co stanowi istotny element oceny skutków dla ochrony danych [2].

Zestawienie punktów przetwarzania

Poniższa tabela przedstawia mapowanie kluczowych komponentów systemu na rodzaje przetwarzanych w nich danych. W dalszej części pracy analiza skupi się na komponentach oznaczonych jako zakres „Głęboki", uwzględniając restrykcyjne wymogi w zakresie poufności i integralności [12, 5].

Warstwa	**Komponent**	**Zakres danych wrażliwych**	**Zakres analizy**
Interfejs	Frontend	Dane profilowe, saldo, sesja.	Ogólny
Dostęp	WAF / API Gateway	Adresy IP, logi dostępowe, tokeny JWT.	**Głęboki**
Logika	Serwis Auth	Login, e-mail, skrót hasła, kody MFA.	**Głęboki**
Logika	Core Banking	Saldo, historia operacji finansowych.	Wyłączony
Dane	Baza poświadczeń	Dane tożsamościowe, hashe, metadane.	**Głęboki**
Dane	SIEM / Monitoring	Logi zdarzeń, próby logowań, błędy.	**Głęboki**
Krypto	Moduł HSM	Klucze prywatne, kody PIN.	Ogólny

Tabela 2: Punkty przetwarzania danych osobowych z określeniem głębokości analizy.

2.4 Zestawienie komponentów technologicznych

W przypadku instytucji o skali lokalnej, architektura technologiczna opiera się w dużej mierze na rozwiązaniach typu *Open Source* oraz konsolidacji wielu funkcji na wspólnym sprzęcie serwerowym. Poniższa tabela odzwierciedla stan faktyczny zasobów wykorzystywanych w procesie logowania, uwzględniając wykorzystanie oprogramowania darmowego oraz sprzętu ogólnego przeznaczenia. Ma to bezpośredni wpływ na profil ryzyka w obszarze bezpieczeństwa łańcucha dostaw oprogramowania [16].

Blok Funkcjonalny	Opis i zawartość pakietu	Zakres Analizy
Systemy Brzegowe i Dystrybucji Ruchu	Zintegrowane rozwiązanie pełniące funkcję zapory ogniowej (Firewall), ochrony przed atakami aplikacyjnymi (WAF) oraz równoważenia obciążenia (Load Balancing).	**Głęboki**
Moduł Zarządzania Tożsamością (IAM)	Usługi katalogowe, silnik uwierzytelniania wieloskładnikowego (MFA) oraz system zarządzania sesjami użytkowników [17].	**Głęboki**
Warstwa Dostępu i Serwera Web	Serwery pośredniczące (Reverse Proxy) oraz bramy API (Gateway), odpowiedzialne za terminację szyfrowanych połączeń i routing do usług wewnętrznych [8].	**Głęboki**
Systemy Składowania Poświadczeń	Relacyjne bazy danych oraz systemy pamięci podręcznej (cache) przechowujące skróty haseł, dane profilowe i tymczasowe kody autoryzacyjne.	**Głęboki**
Platforma Nadzoru i Audytu	Rozwiązania służące do agregacji logów zdarzeń, monitorowania wydajności oraz wykrywania incydentów w czasie rzeczywistym [6].	**Głęboki**
Infrastruktura i Kryptografia	Fizyczne zasoby serwerowe, warstwa wirtualizacji oraz programowe moduły obsługi kluczy szyfrujących (Software-based Crypto).	Ogólny

Tabela 4: Logiczne grupy komponentów systemu logowania poddane analizie.

Wybór powyższych komponentów niesie za sobą specyficzne wyzwania dla analizy ryzyka. Wykorzystanie darmowych wersji oprogramowania (Community Edition) bez płatnego wsparcia producenta nakłada na dział IT obowiązek samodzielnego śledzenia biuletynów bezpieczeństwa i ręcznego wdrażania poprawek, co jest istotne z punktu widzenia zapewnienia odporności cyfrowej [13]. Brak sprzętowego modułu HSM wymusza natomiast realizację operacji kryptograficznych w warstwie programowej, co czyni klucze prywatne bardziej podatnymi na próby kradzieży w przypadku skompromitowania systemu operacyjnego.

2.5 Wstępne zestawienie komponentów kosztowych

Zgodnie z założeniami projektowymi, architektura analizowanego modułu logowania opiera się w głównej mierze na zasobach zastanych (on-hand) oraz oprogramowaniu darmowym (Open Source). Wstępna lista komponentów kosztowych, które wpływają na funkcjonowanie systemu, obejmuje:

- utrzymanie i amortyzację sprzętu serwerowego (CAPEX),
- wykorzystanie oprogramowania bazowego bez płatnych licencji (np. systemy Linux, Keycloak CE, PostgreSQL),
- koszty bieżącej obsługi administracyjnej i monitorowania przez zespół wewnętrzny IT (OPEX),
- usługi weryfikacji bezpieczeństwa, w tym coroczne testy penetracyjne (OPEX).

Szczegółowe zestawienie kosztów, w tym wycena wprowadzanych mechanizmów bezpieczeństwa oraz analiza wskaźnika zwrotu z inwestycji (ROSI), zostały przedstawione w Rozdziale 7 (*Analiza finansowa*).

3 Identyfikacja zagrożeń i podatności

Identyfikacja zagrożeń (threats) oraz podatności (vulnerabilities) stanowi kluczowy etap procesu analizy ryzyka zgodnie z metodyką NIST SP 800-30 [14]. Na tym etapie określane są potencjalne zdarzenia mogące negatywnie wpłynąć na system oraz słabości, które mogą zostać wykorzystane przez aktorów zagrożeń.

Zgodnie z wytycznymi projektowymi analiza obejmuje trzy elementy:

- identyfikację zagrożeń,
- identyfikację podatności,
- powiązanie ich w scenariusze ryzyka.

3.1 Definicje operacyjne

Na potrzeby niniejszego projektu przyjęto następujące definicje:

- **Zagrożenie (threat)** – potencjalne zdarzenie, działanie lub podmiot mogący spowodować szkodę w systemie.
- **Podatność (vulnerability)** – słabość systemu, procesu lub konfiguracji możliwa do wykorzystania przez zagrożenie.
- **Ryzyko (risk)** – kombinacja prawdopodobieństwa wykorzystania podatności oraz wpływu tego zdarzenia na organizację.

Podejście to jest zgodne z metodyką NIST, gdzie ryzyko definiowane jest jako funkcja prawdopodobieństwa i wpływu.

3.2 Podejście do identyfikacji zagrożeń

Proces identyfikacji zagrożeń został przeprowadzony na podstawie:

- analizy architektury systemu (warstwa klienta, API, backend, baza danych),
- standardu OWASP Top 10:2025 [11],
- analizy aktualnych trendów cyberzagrożeń w sektorze finansowym,
- identyfikacji wektorów ataku specyficznych dla bankowości internetowej.

OWASP Top 10 stanowi globalny standard identyfikacji najważniejszych zagrożeń aplikacji webowych [11, 8]. W wersji 2025 szczególny nacisk położono na problemy systemowe, takie jak błędna konfiguracja, bezpieczeństwo łańcucha dostaw oraz kontrola dostępu.

3.3 Katalog głównych zagrożeń

Na podstawie przeprowadzonej analizy zidentyfikowano główne kategorie zagrożeń istotne dla systemu bankowości elektronicznej. W przeciwieństwie do ogólnego opisu klas zagrożeń, poniższe zestawienie przypisuje każde zagrożenie do konkretnego komponentu systemu, typowej podatności oraz potencjalnego skutku. Taki sposób prezentacji pozwala bezpośrednio powiązać identyfikację zagrożeń z późniejszą oceną ryzyka i doborem zabezpieczeń.

Tabela 5: Źródłowe zagrożenia, komponenty systemu i powiązane podatności

Zagrożenie	**Komponent**	**Podatność / przyczyna**	**Możliwy skutek**	**Źródło / kategoria**
Nieprawidłowa kontrola dostępu	Backend API, API Gateway, moduł rachunków	Brak kontroli dostępu po stronie backendu, brak sprawdzania właściciela zasobu, błędne role użytkowników	dostęp do profilu użytkownika, zmiana numeru telefonu do MFA	OWASP A01:2025 Broken Access Control
BOLA / IDOR w API	endpointy weryfikacji MFA, zarządzania sesją i resetu hasła	Możliwość zmiany identyfikatora obiektu w żądaniu API bez ponownej autoryzacji	przejęcie sesji lub obejście autoryzacji drugiego etapu	OWASP A01:2025 Broken Access Control
Błędna konfiguracja środowiska	Nginx, API Gateway, firewall, serwery aplikacyjne, baza danych	Tryb debug, otwarte endpointy administracyjne, domyślne konta, zbyt szerokie reguły sieciowe	Ujawnienie informacji o systemie, dostęp do paneli administracyjnych, ułatwienie dalszego ataku	OWASP A02:2025 Security Misconfiguration
Atak na łańcuch dostaw	Frontend, backend, kontenery, pipeline CI/CD	Podatne biblioteki, brak kontroli zależności, brak SBOM, nieskanowane obrazy kontenerowe	Wprowadzenie podatnego lub złośliwego komponentu do systemu produkcyjnego	OWASP A03:2025 Software Supply Chain Failures, CVE/NVD
Błędy kryptograficzne	Komunikacja TLS, baza danych, HSM/KMS, kopie zapasowe	Brak szyfrowania, słabe algorytmy, błędne zarządzanie kluczami, nieprawidłowa konfiguracja certyfikatów	Ujawnienie danych osobowych, danych logowania, historii transakcji lub tajemnicy bankowej	OWASP A04:2025 Cryptographic Failures
SQL Injection	Backend API, formularze, warstwa dostępu do bazy danych	Brak walidacji danych wejściowych, dynamiczne zapytania SQL, niewłaściwe użycie ORM	odczyt i modyfikacja bazy poświadczeń (kradzież skrótów haseł i metadanych klientów)	OWASP A05:2025 Injection

Zagrożenie	Komponent	Podatność / przyczyna	Możliwy skutek	Źródło / kategoria
XSS	formularz logowania, ekrany odzyskiwania hasła	Brak sanitizacji danych, niebezpieczne renderowanie treści, niewłaściwa konfiguracja CSP	Kradzież tokenu sesyjnego, manipulacja widokiem klienta, wykonanie złośliwego kodu w przeglądarce	OWASP A05:2025 Injection
Niebezpieczny projekt systemu	luki w procesie odzyskiwania dostępu lub logice wydawania tokenów JWT	Brak limitów, brak mechanizmów antyfraudowych, brak analizy scenariuszy nadużyć	Realizacja nieautoryzowanych lub podejrzanych operacji mimo poprawnej implementacji technicznej	OWASP A06:2025 Insecure Design
Błędy uwierzytelniania	Keycloak, moduł logowania, obsługa sesji	Brak MFA, słaba ochrona przed brute-force, długi czas życia sesji, brak rotacji tokenów	Przejęcie konta klienta, przejęcie sesji, obejście mechanizmów logowania	OWASP A07:2025 Authentication Failures
Brak logowania i alertowania	SIEM, aplikacja backendowa, API Gateway, Keycloak, baza danych	Brak centralnych logów, brak korelacji zdarzeń, brak alertów, niewystarczająca retencja logów	Opóźnione wykrycie incydentu, utrudniona analiza powłamaniowa, brak materiału dowodowego	OWASP A09:2025 Security Logging and Alerting Failures
DDoS	Load Balancer, WAF, firewall, warstwa publiczna DMZ	Brak ochrony anty-DDoS, brak rate limitingu, brak skalowania i filtracji ruchu	Niedostępność systemu bankowości elektronicznej, przerwa w obsłudze klientów, straty reputacyjne	Zagrożenie infrastrukturalne / dostępność usług
Phishing i socjotechnika	Klient, infolinia, proces odzyskiwania dostępu, komunikacja e-mail/SMS	Niska świadomość użytkowników, brak jasnych procedur weryfikacji, podszywanie się pod bank	Wyłudzenie danych logowania, zatwierdzenie fałszywej operacji, przejęcie konta	Raporty CERT / zagrożenia sektorowe
Nadużycie uprawnień administracyjnych	Konta administratorów, baza danych, infrastruktura, systemy IAM/PAM	Nadmiarowe uprawnienia, brak regularnych przeglądów dostępów, brak rejestrowania sesji uprzywilejowanych	Nieuprawniony dostęp do danych, zmiana konfiguracji, wyłączenie mechanizmów bezpieczeństwa	Ryzyko operacyjne / insider threat

Zestawienie pokazuje, że największa część zagrożeń dotyczy komponentów publicznie dostępnych lub bezpośrednio przetwarzających dane klientów, takich jak frontend, API Gateway, backend, system uwierzytelniania oraz baza danych. Szczególne znaczenie mają również zagrożenia operacyjne i zewnętrzne, ponieważ ich źródłem nie jest wyłącznie kod aplikacji, ale także konfiguracja, procesy utrzymaniowe, dostawcy zależności oraz zachowanie użytkowników.

3.4 Identyfikacja podatności

Na podstawie powyższego zestawienia zidentyfikowano kluczowe podatności systemu. Nie są one traktowane jako abstrakcyjna lista słabości, lecz jako konkretne punkty, które mogą zostać wykorzystane w komponentach opisanych w tabeli 5.

- brak walidacji i sanitizacji danych wejściowych,
- brak kontroli dostępu po stronie backendu,
- brak kontroli właściciela zasobu w API,
- brak lub niewystarczające MFA,
- brak ochrony przed brute-force i credential stuffing,
- nieprawidłowe zarządzanie sesją,
- brak tokenów CSRF lub błędna konfiguracja atrybutu SameSite,
- brak szyfrowania danych lub słaba konfiguracja kryptografii,
- brak nagłówków bezpieczeństwa przeglądarki,
- wykorzystanie nieaktualnych lub podatnych komponentów,
- brak kontroli zależności i brak SBOM,
- błędna konfiguracja środowiska produkcyjnego,
- zbyt szerokie reguły sieciowe lub brak segmentacji,
- brak centralnego logowania, monitorowania i alertowania,
- nadmiarowe uprawnienia administracyjne,
- brak regularnych przeglądów dostępów i zmian konfiguracyjnych.

Podatności te stanowią podstawę do dalszego powiązania zagrożeń z konkretnymi scenariuszami ryzyka. W kolejnej części rozdziału zostaną one ocenione z wykorzystaniem macierzy prawdopodobieństwa i wpływu.

3.5 Zależność zagrożenie–podatność–ryzyko oraz macierz klasyfikacji

Relacja pomiędzy zagrożeniem, podatnością oraz ryzykiem została określona zgodnie z metodyką OWASP oraz NIST, gdzie ryzyko definiowane jest jako:

$$R = P \times I \tag{1}$$

gdzie:

- R – poziom ryzyka,
- P – prawdopodobieństwo (Probability),
- I – wpływ (Impact).

Podejście to jest standardem w analizie bezpieczeństwa aplikacji webowych i stanowi podstawę metodologii OWASP Risk Rating [10]. W niniejszym projekcie zastosowano uproszczony model punktowy inspirowany metodyką OWASP, dostosowany do charakteru dokumentacji projektowej oraz wymagań dotyczących macierzy ryzyka.

Opis przyjętej skali prawdopodobieństwa

W celu ujednolicenia oceny przyjęto pięciostopniową skalę prawdopodobieństwa. Każdy poziom odnosi się do realności wystąpienia zdarzenia w systemie bankowości elektronicznej, z uwzględnieniem atrakcyjności systemu dla atakujących, dostępności narzędzi ataku, ekspozycji komponentów oraz możliwości wykrycia podatności.

Poziom	Nazwa	Znaczenie i uzasadnienie
1	Bardzo niskie	Zdarzenie jest mało prawdopodobne i wymaga szczególnych warunków, dostępu uprzywilejowanego lub wystąpienia wielu niezależnych błędów jednocześnie. Poziom stosowany dla ryzyk silnie ograniczonych przez architekturę, segmentację sieci, kontrolę dostępu lub brak ekspozycji komponentu do Internetu.
2	Niskie	Zdarzenie jest możliwe, ale wymaga wysokich kompetencji atakującego, specyficznej konfiguracji lub wcześniejszej kompromitacji innego elementu systemu. Poziom właściwy dla scenariuszy trudnych do przeprowadzenia, lecz nadal realnych w środowisku bankowym.
3	Średnie	Zdarzenie może wystąpić w typowych warunkach eksploatacji systemu, szczególnie przy błędach konfiguracyjnych, opóźnieniach aktualizacji lub niewystarczającym monitoringu. Poziom stosowany dla ryzyk znanych i obserwowanych w praktyce, ale niewystępujących masowo bez spełnienia dodatkowych warunków.
4	Wysokie	Zdarzenie jest prawdopodobne, podatność może zostać wykryta lub wykorzystana przy użyciu dostępnych narzędzi, a system jest atrakcyjnym celem dla atakujących. Poziom właściwy dla podatności aplikacyjnych, błędów kontroli dostępu, podatności API i popularnych technik ataku.
5	Bardzo wysokie	Zdarzenie jest bardzo prawdopodobne, dotyczy powszechnych wektorów ataku, może być automatyzowane lub jest szczególnie typowe dla bankowości elektronicznej. Poziom stosowany m.in. dla przejęcia konta, credential stuffing, phishingu, błędnej konfiguracji usług publicznych lub masowych prób logowania.

Tabela 6: Opis skali prawdopodobieństwa

Opis przyjętej skali wpływu

Wpływ określa potencjalne konsekwencje materializacji danego ryzyka dla poufności, integralności i dostępności systemu, a także dla finansów, zgodności regulacyjnej i reputacji organizacji.

Poziom	Nazwa	Znaczenie i uzasadnienie
1	Bardzo niski	Zdarzenie powoduje niewielkie zakłócenie, bez wpływu na dane osobowe, dane finansowe, transakcje lub dostępność usług krytycznych. Skutki ograniczają się do pojedynczego komponentu pomocniczego albo zdarzenia testowego bez wpływu na klienta.
2	Niski	Zdarzenie powoduje lokalny problem techniczny, krótkotrwałe utrudnienie lub ograniczony błąd bez istotnej szkody dla klienta i organizacji. Możliwa jest szybka naprawa bez konieczności uruchamiania pełnej procedury incydentowej.
3	Średni	Zdarzenie wpływa na pojedynczą funkcję systemu, część użytkowników, integralność wybranych danych lub wymaga interwencji zespołu bezpieczeństwa. Skutki są zauważalne operacyjnie, ale nie prowadzą do pełnej utraty poufności, integralności ani dostępności systemu.
4	Wysoki	Zdarzenie może prowadzić do poważnego naruszenia poufności, integralności lub dostępności, obejmować wielu klientów, wymagać zgłoszenia incydentu lub powodować istotne koszty. Poziom właściwy dla zdarzeń wpływających na dane osobowe, dane finansowe, uwierzytelnianie lub ciągłość działania usług.
5	Bardzo wysoki	Zdarzenie może prowadzić do masowego wycieku danych, nieautoryzowanych transakcji, długotrwałej niedostępności systemu, naruszenia regulacji lub utraty zaufania do instytucji. Poziom stosowany dla scenariuszy krytycznych dla bankowości elektronicznej, w których skutki obejmują klientów, regulatora, finanse i reputację organizacji.

Tabela 7: Opis skali wpływu

Macierz klasyfikacji ryzyka

W celu ujednolicenia oceny zastosowano macierz 5×5:

P / I	**1**	**2**	**3**	**4**	**5**
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Tabela 8: Macierz ryzyka (prawdopodobieństwo × wpływ)

Na podstawie macierzy przyjęto następującą klasyfikację wyników:

- **20–25** – ryzyko krytyczne, wymagające natychmiastowych działań lub formalnej decyzji kierownictwa,
- **13–16** – ryzyko bardzo wysokie, wymagające priorytetowej mitygacji,
- **10–12** – ryzyko wysokie, wymagające planu ograniczenia i przypisania właściciela,
- **5–9** – ryzyko średnie, wymagające monitorowania oraz zaplanowania działań w standardowym cyklu zarządzania bezpieczeństwem,
- **1–4** – ryzyko niskie, zasadniczo akceptowalne, wymagające okresowego przeglądu.

Rozróżnienie rodzajów ryzyka

W analizie zastosowano dwa równoległe sposoby klasyfikacji ryzyk. Pierwszy dotyczy stanu ryzyka w cyklu zarządzania, a drugi źródła pochodzenia ryzyka.

Ryzyko wbudowane (inherent risk) oznacza poziom ryzyka przed uwzględnieniem dodatkowych zabezpieczeń zaproponowanych w projekcie. Jest to ryzyko wynikające z samej natury systemu bankowości elektronicznej, jego publicznej dostępności, przetwarzania danych osobowych i finansowych oraz integracji z komponentami infrastrukturalnymi.

Ryzyko rezydualne (residual risk) oznacza poziom ryzyka pozostający po zastosowaniu zabezpieczeń technicznych, organizacyjnych i proceduralnych. Ryzyko rezydualne nie musi wynosić zero, ponieważ nawet po wdrożeniu kontroli nadal mogą istnieć zagrożenia wynikające np. z błędów ludzkich, ataków zero-day, awarii dostawców lub ograniczeń budżetowych.

Ryzyko operacyjne oznacza ryzyko wynikające z działania samej organizacji, procesów, ludzi, konfiguracji, eksploatacji systemu, monitoringu, aktualizacji, zarządzania dostępami i reagowania na incydenty. Przykładami są błędna konfiguracja, brak monitorowania, niewłaściwe zarządzanie uprawnieniami lub opóźnione aktualizacje.

Ryzyko zewnętrzne oznacza ryzyko wynikające z czynników pozostających częściowo lub całkowicie poza bezpośrednią kontrolą organizacji. Obejmuje ono m.in. ataki DDoS, phishing klientów, podatności w zewnętrznych bibliotekach, awarie dostawców, zagrożenia łańcucha dostaw oraz działania wyspecjalizowanych grup przestępczych.

W praktyce jedno ryzyko może mieć jednocześnie charakter operacyjny i zewnętrzny. Przykładowo atak supply chain jest inicjowany zewnętrznie, ale jego skuteczność zależy również od operacyjnych procesów kontroli zależności, skanowania komponentów i zarządzania aktualizacjami.

Tabela klasyfikacji ryzyk dla zidentyfikowanych podatności

Na podstawie wcześniej zidentyfikowanych zagrożeń i podatności przypisano im wartości prawdopodobieństwa oraz wpływu:

Zagrożenie	Podatność	P	I	R	Poziom
Przejęcie konta (ATO)	brak MFA / brak ochrony brute-force	5	5	25	Krytyczne
SQL Injection	brak walidacji danych wejściowych	4	5	20	Krytyczne
BOLA (API)	brak kontroli dostępu na poziomie obiektu	4	5	20	Krytyczne
XSS	brak sanitizacji danych	4	3	12	Wysokie
CSRF	brak tokenów CSRF	3	4	12	Wysokie
Błędna konfiguracja	debug mode / otwarte endpointy	5	3	15	Bardzo wysokie
Brak szyfrowania	HTTP / słaba kryptografia	3	5	15	Bardzo wysokie
Przejęcie sesji	brak bezpiecznego zarządzania sesją	4	4	16	Bardzo wysokie
Supply chain attack	brak kontroli zależności	3	5	15	Bardzo wysokie
DDoS	brak ochrony infrastrukturalnej	3	4	12	Wysokie
Brak logowania	brak SIEM / monitoringu	4	3	12	Wysokie

Tabela 9: Klasyfikacja ryzyk dla zidentyfikowanych podatności

Rejestr ryzyk

Poniższy rejestr ryzyk stanowi rozwinięcie wcześniejszej identyfikacji zagrożeń i podatności. Dla każdego scenariusza wskazano źródło ryzyka, podatność, poziom ryzyka wbudowanego, istniejące lub proponowane zabezpieczenia, poziom ryzyka rezydualnego oraz uzasadnienie oceny. Wartości ryzyka wbudowanego odnoszą się do stanu przed pełnym wdrożeniem mechanizmów z rozdziału 4, natomiast wartości ryzyka rezydualnego zakładają wdrożenie wskazanych zabezpieczeń.

Tabela 10: Rejestr ryzyk dla systemu bankowości elektronicznej

ID	**Scenariusz ryzyka**	**Źródło**	**Podatność / przyczyna**	**Ryzyko wbud. P/I/R**	**Ryzyko rez. P/I/R**	**Zabezpieczenia i właściciel**
R1	Przejęcie konta klienta przez credential stuffing, phishing lub brute-force	Zewn. + oper.	Brak lub niewystarczające MFA, brak rate limitingu, brak detekcji anomalii logowania	5/5/25 – kryt.	2/5/10 – wys.	MFA, aplikacja mobilna lub WebAuthn/passkeys, rate limiting, blokada po wielu próbach, analiza behawioralna logowań, alerty SIEM. **Właściciel:** Zespół IAM / SOC.
R2	SQL Injection prowadzące do odczytu bazy skrótów haseł i danych uwierzytelniających	Oper.	Brak walidacji danych wejściowych, dynamiczne zapytania SQL, brak testów bezpieczeństwa	4/5/20 – kryt.	1/5/5 – śr.	Parametryzacja zapytań, ORM, walidacja danych, WAF, testy SAST/DAST, testy penetracyjne, ograniczenie uprawnień kont bazodanowych. **Właściciel:** Zespół Backend / AppSec.
R3	BOLA / IDOR w API umożliwiające modyfikację preferencji autoryzacji (np. numeru telefonu MFA) dla innego klienta	Oper.	Brak kontroli dostępu na poziomie obiektu w backendzie	4/5/20 – kryt.	2/5/10 – wys.	Autoryzacja po stronie backendu dla każdej operacji, sprawdzanie właściciela zasobu, testy kontroli dostępu, reguły API Gateway, przeglądy kodu. **Właściciel:** Zespół Backend / API Owner.

ID	Scenariusz ryzyka	Źródło	Podatność / przyczyna	Ryzyko wbud. P/I/R	Ryzyko rez. P/I/R	Zabezpieczenia i właściciel
R4	XSS prowadzący do kradzieży tokenu sesyjnego lub manipulacji widokiem klienta	Oper. + zewn.	Brak sanitizacji danych, niewłaściwa konfiguracja CSP, niebezpieczne renderowanie danych	4/3/12 – wys.	2/3/6 – śr.	Escapowanie danych, walidacja wejścia i wyjścia, Content Security Policy, HttpOnly i Secure cookies, testy DAST, przegląd komponentów frontendowych. **Właściciel:** Zespół Frontend / AppSec.
R5	CSRF skutkujący wykonaniem operacji w imieniu zalogowanego użytkownika	Oper.	Brak tokenów CSRF, niewłaściwa konfiguracja SameSite, brak dodatkowej autoryzacji operacji krytycznych	3/4/12 – wys.	1/4/4 – nis.	Tokeny CSRF, SameSite cookies, ponowna autoryzacja operacji wysokiego ryzyka, potwierdzenia transakcji, walidacja Origin/Referer. **Właściciel:** Zespół Backend / Frontend.
R6	Błędna konfiguracja środowiska produkcyjnego ujawniająca dane lub panele administracyjne	Oper.	Debug mode, otwarte endpointy, domyślne konta, zbyt szerokie reguły firewall	5/3/15 – b. wys.	2/3/6 – śr.	Hardening konfiguracji, checklisty wdrożeniowe, Infrastructure as Code, skanowanie konfiguracji, przeglądy zmian, zasada least privilege. **Właściciel:** DevOps / Administrator infrastruktury.
R7	Ujawnienie danych w transmisji lub w spoczynku wskutek słabej kryptografii	Oper.	Brak TLS, słabe algorytmy, błędne zarządzanie kluczami, niewłaściwe szyfrowanie danych	3/5/15 – b. wys.	1/5/5 – śr.	TLS 1.3, HSTS, szyfrowanie danych w spoczynku, HSM/KMS, rotacja kluczy, polityka zarządzania certyfikatami. **Właściciel:** Zespół Security / Administrator bazy danych.

ID	Scenariusz ryzyka	Źródło	Podatność / przyczyna	Ryzyko wbud. P/I/R	Ryzyko rez. P/I/R	Zabezpieczenia i właściciel
R8	Przejęcie sesji użytkownika	Zewn. + oper.	Nieprawidłowe zarządzanie sesją, brak rotacji tokenów, długi czas życia sesji, podatność na XSS	4/4/16 – b. wys.	2/4/8 – śr.	Krótkie czasy życia tokenów, rotacja tokenów, HttpOnly/Secure/SameSite cookies, wykrywanie anomalii sesji, unieważnianie sesji po zmianie hasła. **Właściciel:** Zespół IAM / Backend.
R9	Atak na łańcuch dostaw oprogramowania przez podatną lub złośliwą zależność	Zewn. + oper.	Brak kontroli zależności, brak SBOM, brak skanowania obrazów i bibliotek, brak procesu aktualizacji	3/5/15 – b. wys.	2/5/10 – wys.	SCA, SBOM, Dependabot/Snyk/OWASP Dependency-Check, podpisywanie artefaktów, skanowanie kontenerów, zatwierdzanie zależności. **Właściciel:** DevSecOps / AppSec.
R10	Niedostępność systemu wskutek ataku DDoS	Zewn.	Brak ochrony anty-DDoS, brak rate limitingu, brak skalowania i filtracji ruchu	3/4/12 – wys.	2/4/8 – śr.	Ochrona anty-DDoS, CDN/scrubbing center, rate limiting, WAF, autoskalowanie, procedury przełączenia ruchu. **Właściciel:** Zespół infrastruktury / SOC.
R11	Brak skutecznego monitorowania i opóźnione wykrycie incydentu	Oper.	Brak SIEM, brak korelacji logów, brak alertów, brak procedur eskalacji	4/3/12 – wys.	2/3/6 – śr.	Centralne logowanie, SIEM, reguły korelacyjne, alerty SOC, retencja logów, regularne testy detekcji. **Właściciel:** SOC / Security Officer.

ID	Scenariusz ryzyka	Źródło	Podatność / przyczyna	Ryzyko wbud. P/I/R	Ryzyko rez. P/I/R	Zabezpieczenia i właściciel
R12	Nadużycie uprawnień administracyjnych lub błąd operatora	Oper.	Nadmiarowe uprawnienia, brak PAM, brak przeglądów dostępów, brak rozdziału obowiązków	3/5/15 – b. wys.	2/5/10 – wys.	PAM, zasada najmniejszych uprawnień, okresowe przeglądy uprawnień, rejestrowanie sesji administratorów, rozdział obowiązków. **Właściciel:** Administrator IAM / Security Officer.

Uzasadnienie ocen w rejestrze ryzyk. Najwyższe wartości ryzyka wbudowanego przypisano scenariuszom R1, R2 oraz R3, ponieważ dotyczą one bezpośrednio przejęcia konta, nieuprawnionego dostępu do danych klientów lub manipulacji poświadczeniami. W tych przypadkach wpływ oceniono na bardzo wysoki, ponieważ skuteczny atak może prowadzić do naruszenia poufności danych osobowych, kradzieży tożsamości, strat finansowych oraz utraty zaufania do systemu bankowości elektronicznej.

Ryzyka R4, R5, R6, R8 oraz R11 mają charakter przede wszystkim operacyjny, ponieważ ich prawdopodobieństwo zależy od jakości implementacji, konfiguracji, monitorowania oraz procedur utrzymaniowych. Po wdrożeniu zabezpieczeń, takich jak CSP, tokeny CSRF, bezpieczne zarządzanie sesją, hardening konfiguracji oraz SIEM, prawdopodobieństwo ich materializacji ulega obniżeniu. Nie oznacza to jednak całkowitego usunięcia ryzyka, ponieważ część zagrożeń może pojawić się ponownie po zmianach aplikacyjnych lub konfiguracyjnych.

Ryzyka R9 i R10 mają silny komponent zewnętrzny. W przypadku R9 źródłem zagrożenia mogą być dostawcy bibliotek, obrazów kontenerowych lub narzędzi CI/CD, natomiast w przypadku R10 atak może pochodzić z infrastruktury całkowicie niezależnej od organizacji. Z tego powodu ryzyko rezydualne pozostaje istotne nawet po wdrożeniu mechanizmów ograniczających, takich jak SCA, SBOM, skanowanie kontenerów, ochrona anty-DDoS i rate limiting.

Ryzyko R12 pozostaje wysokie również po zastosowaniu kontroli, ponieważ dotyczy kont uprzywilejowanych oraz błędów operatorów. Nawet przy wdrożeniu PAM, rejestrowaniu sesji i regularnych przeglądach uprawnień nie można całkowicie wyeliminować ryzyka wynikającego z czynnika ludzkiego, błędnej decyzji administracyjnej lub nadużycia uprawnień.

Interpretacja wyników

Wyniki analizy wskazują, że największy priorytet powinny otrzymać ryzyka związane z przejęciem konta, błędami kontroli dostępu, podatnościami aplikacyjnymi oraz

bezpieczeństwem łańcucha dostaw. Są to scenariusze, w których połączenie wysokiego prawdopodobieństwa i dużego wpływu może bezpośrednio naruszyć poufność, integralność lub dostępność systemu bankowości elektronicznej.

Porównanie ryzyka wbudowanego i rezydualnego pokazuje, że zaproponowane zabezpieczenia obniżają poziom większości ryzyk, jednak nie eliminują ich całkowicie. Ryzyka pozostające na poziomie wysokim powinny zostać objęte dalszym monitorowaniem, testami bezpieczeństwa oraz okresową ponowną oceną.

Rejestr ryzyk stanowi podstawę do dalszego doboru zabezpieczeń w rozdziale 4 oraz do opracowania scenariuszy reagowania na incydenty w rozdziale 5. W kolejnych etapach projektu szczególną uwagę należy przypisać ryzykom o najwyższym poziomie rezydualnym, ponieważ to one wymagają najbardziej konsekwentnej kontroli operacyjnej.

4 Zestawienie zabezpieczeń

Celem niniejszego rozdziału jest wskazanie zabezpieczeń ograniczających ryzyka zidentyfikowane w rozdziale 3. Zabezpieczenia nie są tu traktowane jako ogólna lista narzędzi bezpieczeństwa, lecz jako kontrole przypisane do konkretnych scenariuszy ryzyka. Dla każdej grupy ryzyk określono mechanizm ograniczający, sposób weryfikacji skuteczności, orientacyjny koszt wdrożenia oraz poziom ryzyka rezydualnego po zastosowaniu kontroli.

Przyjęto trzy kategorie zabezpieczeń:

- **techniczne** - mechanizmy wdrażane w aplikacji, infrastrukturze, sieci i systemach monitorowania,
- **organizacyjne** - polityki, role, odpowiedzialności i procesy zarządzania bezpieczeństwem,
- **proceduralne** - powtarzalne sposoby postępowania w przypadku zmian, incydentów, audytów i obsługi zgłoszeń.

Poziom kosztu określono jakościowo jako niski, średni, wysoki lub bardzo wysoki. Nie oznacza on dokładnej wyceny finansowej, lecz relatywny nakład wdrożenia, utrzymania, licencji, pracy zespołu oraz złożoności organizacyjnej. Szczegółowe oszacowanie kosztów zostało przedstawione w rozdziale dotyczącym analizy finansowej.

4.1 Mapa zabezpieczeń dla zidentyfikowanych ryzyk

Tabela 11 przedstawia powiązanie ryzyk z rejestru ryzyk z kontrolami bezpieczeństwa. Nie powtarza pełnego rejestru z rozdziału 3, lecz wskazuje, jakie zabezpieczenia należy zastosować, jak sprawdzić ich skuteczność oraz jaki poziom ryzyka pozostaje po wdrożeniu kontroli [9, 16]. Szczegółowe uzasadnienie wartości prawdopodobieństwa i wpływu znajduje się w tabeli 10.

Tabela 11: Mapowanie ryzyk na zabezpieczenia, weryfikację, koszt i ryzyko rezydualne

ID	Ryzyko	Kontrola / zabezpieczenie	Sposób weryfikacji	Koszt	Ryzyko rezydualne
R1	Przejęcie konta klienta	MFA, WebAuthn/passkeys lub aplikacja mobilna, rate limiting, blokada po wielu próbach, detekcja anomalii logowania, edukacja antyphishingowa	Test wymuszenia MFA, test blokady konta, symulacja credential stuffing, kontrola alertów SIEM, symulacje phishingowe	Średni / wysoki	2/5/10 - wysokie
R2	SQL Injection	Parametryzacja zapytań, ORM, walidacja danych wejściowych, ograniczenie uprawnień kont bazodanowych, WAF	SAST, DAST, testy penetracyjne, próby wstrzyknięcia w parametrach API, przegląd zapytań SQL	Średni	1/5/5 - średnie

ID	Ryzyko	Kontrola / zabezpieczenie	Sposób weryfikacji	Koszt	Ryzyko rezydualne
R3	BOLA / IDOR w API	Autoryzacja obiektowa po stronie backendu, RBAC/ABAC, kontrola właściciela zasobu, testy kontroli dostępu	Test zmiany identyfikatorów obiektów w API, testy ról, testy dostępu do zasobów innych użytkowników, przegląd kodu	Średni	2/5/10 - wysokie
R4	XSS	Escapowanie danych, walidacja wejścia i wyjścia, CSP, bezpieczne cookies, ograniczenie przechowywania tokenów w przeglądarce	Testy payloadów XSS, weryfikacja CSP, kontrola nagłówków bezpieczeństwa, test sposobu przechowywania tokenów	Niski / średni	2/3/6 - średnie
R5	CSRF	Tokeny CSRF, SameSite cookies, walidacja Origin/Referer, autoryzacja zmian ustawień logowania i bezpieczeństwa konta	Test żądań bez tokenu CSRF, test fałszywego formularza, kontrola konfiguracji cookies, test operacji zmieniających stan	Niski	1/4/4 - niskie
R6	Błędna konfiguracja środowiska	Hardening, Infrastructure as Code, checklisty wdrożeniowe, przegląd reguł firewall, skanowanie konfiguracji	Skan konfiguracji, przegląd IaC, kontrola portów, test braku trybu debug, kontrola kont domyślnych	Średni	2/3/6 - średnie
R7	Słaba kryptografia lub brak szyfrowania	TLS 1.3, HSTS, szyfrowanie danych w spoczynku, HSM/KMS, rotacja kluczy, polityka certyfikatów	Test konfiguracji TLS, audyt certyfikatów, kontrola szyfrowania bazy, test rotacji kluczy, przegląd konfiguracji HSM/KMS	Wysoki	1/5/5 - średnie
R8	Przejęcie sesji użytkownika	Krótkie czasy życia tokenów, rotacja tokenów, HttpOnly/Secure/SameSite cookies, unieważnianie sesji po zmianie hasła	Test czasu życia sesji, próba ponownego użycia tokenu, test wylogowania globalnego, analiza cookies	Średni	2/4/8 - średnie
R9	Atak na łańcuch dostaw	SCA, SBOM, skanowanie zależności, skanowanie kontenerów, podpisywanie artefaktów, zatwierdzanie nowych zależności	Skan zależności, skan obrazów kontenerowych, weryfikacja SBOM, audyt pipeline CI/CD, kontrola podpisów artefaktów	Średni / wysoki	2/5/10 - wysokie

ID	Ryzyko	Kontrola / zabezpieczenie	Sposób weryfikacji	Koszt	Ryzyko rezydualne
R10	DDoS i niedostępność usługi	Ochrona anty-DDoS, CDN lub scrubbing center, rate limiting, autoskalowanie, procedury przełączenia ruchu, BCP/DRP	Testy obciążeniowe, test rate limiting, test przełączenia awaryjnego, analiza logów WAF/CDN, ćwiczenia ciągłości działania	Wysoki / bardzo wysoki	2/4/8 - średnie
R11	Brak skutecznego monitorowania	Centralne logowanie, SIEM, reguły korelacyjne, alerty SOC, retencja logów, scenariusze eskalacji	Test generowania zdarzeń, test reguł korelacyjnych, kontrola retencji logów, ćwiczenia SOC, pomiar czasu reakcji	Średni / wysoki	2/3/6 - średnie
R12	Nadużycie uprawnień administracyjnych	PAM, zasada najmniejszych uprawnień, przeglądy dostępów, rejestrowanie sesji administratorów, rozdział obowiązków	Przegląd ról, test kont uprzywilejowanych, kontrola nagrań sesji PAM, test odebrania uprawnień po zmianie stanowiska	Wysoki	2/5/10 - wysokie

Zestawienie pokazuje, że większość kontroli ogranicza przede wszystkim prawdopodobieństwo skutecznego ataku. Wpływ wielu ryzyk pozostaje wysoki, ponieważ system przetwarza dane osobowe, dane finansowe i informacje objęte tajemnicą bankową. Z tego powodu ryzyka R1, R3, R9 i R12 pozostają na poziomie wysokim nawet po wdrożeniu zabezpieczeń i wymagają szczególnego monitorowania.

4.2 Zabezpieczenia techniczne

Zabezpieczenia techniczne mają bezpośrednio ograniczyć możliwość wykorzystania podatności w aplikacji, infrastrukturze i komunikacji sieciowej. W projekcie priorytetowo potraktowano zabezpieczenia dotyczące uwierzytelniania, autoryzacji, ochrony API, szyfrowania, monitorowania oraz bezpieczeństwa łańcucha dostaw.

Uwierzytelnianie i ochrona kont użytkowników

Dla ryzyka przejęcia konta klienta kluczowe znaczenie ma wdrożenie MFA oraz mechanizmów ograniczających automatyczne próby logowania. Preferowane powinny być metody silniejsze niż SMS, np. aplikacja mobilna, WebAuthn lub passkeys. Dobór metod uwierzytelniania powinien uwzględniać wymagania dotyczące silnych uwierzytelniaczy oraz odporności na przejęcie poświadczeń [17]. W kontekście płatności elektronicznych istotne są również wymagania silnego uwierzytelniania klienta wynikające z regulacyjnych standardów technicznych PSD2 [3]. Dodatkowo należy wdrożyć rate limiting, blokowanie podejrzanych prób logowania oraz alertowanie w SIEM.

Skuteczność kontroli należy potwierdzać przez testy prób brute-force, testy credential stuffing w środowisku testowym, sprawdzenie wymuszenia MFA oraz weryfikację alertów SOC. Kontrola ogranicza głównie ryzyko R1 oraz częściowo R8.

Autoryzacja i kontrola dostępu

Dla ryzyk związanych z BOLA/IDOR oraz nieprawidłową kontrolą dostępu najważniejsza jest autoryzacja wykonywana po stronie backendu. Każda operacja API powinna sprawdzać nie tylko rolę użytkownika, ale także to, czy użytkownik jest właścicielem zasobu, którego dotyczy żądanie. Kontrola dostępu po stronie interfejsu użytkownika może być wyłącznie mechanizmem pomocniczym.

Weryfikacja powinna obejmować testy zmiany identyfikatorów obiektów w żądaniach API, testy ról, testy poziomej i pionowej eskalacji uprawnień oraz przeglądy kodu. Kontrola ogranicza przede wszystkim ryzyko R3 oraz częściowo R12.

Walidacja danych i ochrona przed Injection

Ryzyko SQL Injection należy ograniczać przez parametryzację zapytań, poprawne użycie ORM, walidację danych wejściowych oraz ograniczenie uprawnień kont bazodanowych. WAF może stanowić dodatkową warstwę ochrony, ale nie zastępuje poprawnej implementacji aplikacji.

Weryfikacja powinna obejmować testy SAST, DAST, testy penetracyjne oraz ręczne próby wstrzyknięcia danych w formularzach i parametrach API. Kontrola dotyczy głównie ryzyka R2.

Ochrona przeglądarki, sesji i operacji użytkownika

Dla ryzyk XSS, CSRF i przejęcia sesji należy wdrożyć zestaw zabezpieczeń przeglądarkowych: Content Security Policy, bezpieczne nagłówki HTTP, cookies z atrybutami HttpOnly, Secure i SameSite, tokeny CSRF oraz ograniczenie przechowywania tokenów w localStorage lub sessionStorage. Operacje wysokiego ryzyka powinny wymagać dodatkowej autoryzacji.

Weryfikacja powinna obejmować testy payloadów XSS, kontrolę nagłówków bezpieczeństwa, testy żądań bez tokenu CSRF, analizę cookies oraz testy ponownego użycia tokenu sesyjnego. Kontrole te ograniczają ryzyka R4, R5 i R8.

Szyfrowanie i zarządzanie kluczami

Dane w transmisji powinny być chronione z wykorzystaniem TLS 1.3 oraz HSTS, a dane w spoczynku powinny być szyfrowane na poziomie bazy danych, kopii zapasowych i nośników. Klucze kryptograficzne powinny być zarządzane przez HSM lub KMS, z uwzględnieniem rotacji, kontroli dostępu i audytu użycia kluczy.

Weryfikacja obejmuje test konfiguracji TLS, kontrolę certyfikatów, audyt kluczy, test rotacji kluczy oraz sprawdzenie, czy kopie zapasowe i baza danych są szyfrowane. Kontrola ogranicza ryzyko R7.

Monitoring, SIEM i detekcja incydentów

System powinien centralnie gromadzić logi z aplikacji, API Gateway, Keycloak, WAF, firewalli, bazy danych i komponentów infrastrukturalnych. SIEM (np. Wazuh) powinien korelować zdarzenia i generować alerty dla prób przejęcia konta, podejrzanych żądań API, eskalacji uprawnień, zmian administracyjnych oraz anomalii ruchu.

Weryfikacja polega na generowaniu kontrolowanych zdarzeń testowych, sprawdzeniu reguł korelacyjnych, analizie retencji logów oraz pomiarze czasu reakcji SOC. Kontrola ogranicza przede wszystkim R11, ale wspiera także R1, R6, R8, R10 i R12.

Bezpieczeństwo infrastruktury i dostępności

Ochrona infrastruktury obejmuje NGFW, IDS/IPS, WAF, segmentację sieci, ochronę anty-DDoS, rate limiting oraz procedury przełączenia ruchu. Mechanizmy te mają ograniczać ekspozycję usług, filtrować ruch zewnętrzny oraz utrzymać dostępność bankowości elektronicznej podczas ataku lub awarii.

Weryfikacja powinna obejmować przegląd reguł firewall, testy ekspozycji portów, testy rate limiting, testy obciążeniowe oraz ćwiczenia przełączenia awaryjnego. Kontrole te ograniczają głównie R6, R10 i R11.

Bezpieczeństwo łańcucha dostaw

Aplikacja wykorzystuje zewnętrzne biblioteki, kontenery i narzędzia CI/CD, dlatego konieczne jest wdrożenie kontroli zależności. Wymagane są skanowanie bibliotek, generowanie SBOM, skanowanie obrazów kontenerowych, zatwierdzanie nowych zależności oraz podpisywanie artefaktów wdrożeniowych.

Weryfikacja obejmuje skan zależności, skan obrazów kontenerowych, kontrolę SBOM, audyt pipeline CI/CD i sprawdzenie podpisów artefaktów. Kontrola ogranicza ryzyko R9.

4.3 Zabezpieczenia organizacyjne

Kontrole organizacyjne zapewniają, że zabezpieczenia techniczne są utrzymywane, aktualizowane i egzekwowane. W projekcie najważniejsze są: zarządzanie ryzykiem IT, zarządzanie dostępem, klasyfikacja danych, szkolenia oraz plan ciągłości działania.

Zarządzanie ryzykiem IT

Rejestr ryzyk powinien być utrzymywany jako dokument roboczy, a nie jednorazowy element projektu. Po każdej istotnej zmianie systemu, wykryciu nowej podatności lub incydencie należy ponownie ocenić ryzyko wbudowane i rezydualne. Każde ryzyko powinno mieć właściciela odpowiedzialnego za decyzję o mitygacji, akceptacji lub dalszym monitorowaniu.

Kontrola ta obejmuje wszystkie ryzyka z rejestru i jest podstawą spójności całej analizy.

Zarządzanie dostępem i uprawnieniami

Uprawnienia pracowników i administratorów powinny być nadawane zgodnie z zasadą najmniejszych uprawnień. Dostępy uprzywilejowane powinny być obsługiwane przez PAM, rejestrowane i okresowo przeglądane. Zmiana stanowiska lub zakończenie współpracy powinny automatycznie uruchamiać procedurę odebrania dostępów.

Weryfikacja obejmuje przeglądy uprawnień, audyt ról, kontrolę sesji PAM oraz test odebrania uprawnień po zmianie stanowiska. Kontrola ogranicza przede wszystkim R12.

Klasyfikacja i zarządzanie danymi

Dane przetwarzane w systemie powinny zostać przypisane do klas ochrony, np. dane publiczne, wewnętrzne, poufne i ściśle poufne. Dane klientów, dane logowania, skróty haseł, numery telefonów do MFA i dane autoryzacyjne powinny należeć do najwyższych klas ochrony.

Dla każdej klasy danych należy określić zasady przechowywania, szyfrowania, retencji, dostępu, archiwizacji i usuwania. Kontrola ta wspiera ograniczanie R2, R3, R7 i R12.

Szkolenia i świadomość

Szkolenia powinny obejmować rozpoznawanie phishingu, bezpieczną obsługę klientów, ochronę danych, reagowanie na incydenty oraz procedury eskalacji. Szczególnie istotne są szkolenia dla infolinii i pracowników mających kontakt z klientem, ponieważ mogą oni ograniczyć skutki kampanii socjotechnicznych.

Weryfikacja obejmuje testy wiedzy, symulacje phishingowe oraz analizę sposobu obsługi zgłoszeń bezpieczeństwa. Kontrola ogranicza głównie R1, R8 i R12.

Plan ciągłości działania

Plan ciągłości działania powinien określać sposób utrzymania lub odtworzenia usług bankowości elektronicznej po awarii, cyberataku lub niedostępności infrastruktury. Powinien zawierać role, procedury przełączenia ruchu, zasady komunikacji, parametry RTO i RPO oraz sposób odtwarzania danych.

Weryfikacja obejmuje test odtworzenia kopii zapasowej, test przełączenia awaryjnego oraz ćwiczenia kryzysowe. Kontrola ogranicza przede wszystkim skutki R10, ale wspiera także obsługę poważnych incydentów z R1, R2, R3 i R9.

4.4 Zabezpieczenia proceduralne

Zabezpieczenia proceduralne określają sposób powtarzalnego postępowania w sytuacjach, które mogą wpływać na bezpieczeństwo systemu. Mają one szczególne znaczenie tam, gdzie źródłem ryzyka są zmiany, dostawcy, błędy operatorów lub opóźniona reakcja na incydent.

Zarządzanie incydentami

Procedura zarządzania incydentami powinna obejmować wykrycie, klasyfikację, eskalację, ograniczenie skutków, usunięcie przyczyny, przywrócenie działania, raportowanie i analizę poincydentową. Powinna również określać odpowiedzialność zespołów SOC, administratorów, właścicieli aplikacji i osób decyzyjnych.

Weryfikacja obejmuje ćwiczenia tabletop, symulacje incydentów, testy eskalacji oraz analizę czasu reakcji. Procedura wspiera wszystkie ryzyka, które mimo wdrożenia kontroli pozostają na poziomie średnim lub wysokim.

Zarządzanie zmianą

Każda zmiana w aplikacji, infrastrukturze, konfiguracji lub zależnościach powinna być oceniona pod kątem wpływu na bezpieczeństwo. Zmiany powinny przechodzić przez środowisko testowe, przegląd kodu, testy bezpieczeństwa i formalne zatwierdzenie.

Weryfikacja obejmuje audyt zmian, kontrolę pull requestów, analizę wyników testów CI/CD oraz sprawdzenie, czy zmiana nie wprowadziła nowych podatności. Procedura ogranicza R2, R3, R4, R6, R8 i R9.

Zarządzanie dostawcami

Dostawcy oprogramowania, usług infrastrukturalnych i komponentów bezpieczeństwa powinni być oceniani pod kątem zgodności z wymaganiami bezpieczeństwa. Umowy powinny określać wymagania dotyczące aktualizacji, zgłaszania incydentów, dostępności usług i ochrony danych.

Weryfikacja obejmuje przegląd umów, audyt dostawców, kontrolę SLA oraz ocenę podatności komponentów dostarczanych przez podmioty zewnętrzne. Procedura ogranicza przede wszystkim R9 i R10.

Audyty i testy okresowe

Audyty wewnętrzne i zewnętrzne powinny okresowo potwierdzać zgodność systemu z politykami bezpieczeństwa, wymaganiami regulacyjnymi i przyjętym modelem ryzyka. Zakres audytu powinien obejmować konfigurację, uprawnienia, logowanie, szyfrowanie, proces zmian, rejestr ryzyk oraz skuteczność procedur incydentowych.

Wyniki audytów powinny prowadzić do konkretnych działań naprawczych, przypisania właściciela i określenia terminu realizacji. Audyty są kontrolą przekrojową dla wszystkich ryzyk.

4.5 Weryfikacja skuteczności zabezpieczeń

Skuteczność zabezpieczeń powinna być oceniana cyklicznie. Samo wdrożenie kontroli nie oznacza, że ryzyko zostało skutecznie ograniczone. Każda kontrola powinna mieć mierzalny sposób weryfikacji, np. test techniczny, przegląd konfiguracji, symulację incydentu, audyt lub analizę logów.

W przypadku aplikacji webowej szczególne znaczenie mają testy SAST, DAST, testy penetracyjne, testy kontroli dostępu, testy konfiguracji nagłówków bezpieczeństwa, skanowanie zależności i skanowanie obrazów kontenerowych.Zakres weryfikacji aplikacji webowej może zostać oparty na OWASP ASVS, który porządkuje wymagania bezpieczeństwa możliwe do przetestowania w aplikacji i jej środowisku [9]. Dla infrastruktury istotne są przeglądy reguł firewall, testy ekspozycji usług, testy obciążeniowe i kontrola segmentacji sieci.

Szczególnie istotnym aspektem są regularne audyty (wewnętrzne i zewnętrzne), które pozwalają na weryfikację poziomu bezpieczeństwa poszczególnych komponentów. Główną częścią powinny stanowić skanery podatności (takie jak np. OpenVAS czy Nessus), pozwalające na półautomatyczną identyfikację zagrożeń. Testy penetracyjne pozwalają doświadczonemu zespołowi na ręczną próbę exploitacji systemu, znajdowanie także błędów i potencjalnych wektorów ataków. Całość powinna być odpowiednio raportowana.

Mechanizmy organizacyjne i proceduralne powinny być weryfikowane przez ćwiczenia tabletop, audyty, testy odtworzenia danych, przeglądy uprawnień i symulacje incydentów. Szczególnie ważne jest potwierdzenie, że procedury są znane osobom odpowiedzialnym i możliwe do wykonania w rzeczywistych warunkach.

Po każdym istotnym wdrożeniu, zmianie architektury, wykryciu nowej podatności CVE lub incydencie należy ponownie ocenić poziom ryzyka rezydualnego w rejestrze ryzyk. Dzięki temu rozdział 4 stanowi nie tylko opis zabezpieczeń, ale również mierzalny plan ograniczania ryzyka.

4.6 Podsumowanie zabezpieczeń

Zaproponowane zabezpieczenia tworzą model ochrony oparty na powiązaniu ryzyk z konkretnymi kontrolami. Największe znaczenie mają kontrole ograniczające przejęcie konta, błędy kontroli dostępu, podatności aplikacyjne, błędy konfiguracji, słabą kryptografię, ataki na łańcuch dostaw i brak monitorowania.

Najniższy poziom ryzyka rezydualnego osiągnięto tam, gdzie zabezpieczenia są jednoznaczne technicznie i łatwe do przetestowania, np. przy CSRF, konfiguracji TLS lub parametryzacji zapytań. Wyższy poziom ryzyka rezydualnego pozostaje przy przejęciu konta, błędach kontroli dostępu, łańcuchu dostaw i uprawnieniach administracyjnych, ponieważ te obszary zależą nie tylko od narzędzi, ale również od procesów, ludzi i czynników zewnętrznych.

Wdrożenie zabezpieczeń powinno być traktowane jako proces ciągły. Kontrole należy testować, aktualizować i odnosić do rejestru ryzyk, aby zachować spójność między identyfikacją zagrożeń, analizą ryzyka, planem zabezpieczeń i reakcją na incydenty.

5 Reagowanie na incydenty

Incydent bezpieczeństwa to zdarzenie operujące na poziomie ochrony całego lub części systemu bankowego. W kontekście tej pracy szczególne znaczenie mają incydenty, które mogą prowadzić do przejęcia konta klienta, obejścia mechanizmów autoryzacji, ujawnienia danych osobowych, nieautoryzowanego dostępu do API lub niedostępności systemu.

Plan reagowania został opracowany zgodnie z podejściem procesowym opisanym w NIST SP 800-61 Rev. 3, w którym reagowanie na incydenty traktowane jest jako cykl obejmujący przygotowanie, wykrycie i analizę, ograniczenie skutków, usunięcie przyczyny, przywrócenie działania oraz wyciągnięcie wniosków po incydencie [6].

5.1 Założenia planu reagowania

Plan reagowania na incydenty został przygotowany dla lokalnego banku korzystającego z architektury opisanej w rozdziale 2. Ze względu na ograniczony budżet i mały zespół, plan zakłada realistyczny model operacyjny, w którym część zadań realizowana jest przez niewielki zespół IT, administratorów infrastruktury oraz osobę odpowiedzialną za bezpieczeństwo informacji. W przypadku poważniejszych incydentów możliwe jest wsparcie zewnętrznego dostawcy usług bezpieczeństwa lub zespołu reagowania na incydenty.

Plan obejmuje przede wszystkim incydenty dotyczące następujących komponentów:

- **Frontend i warstwa dostępu** - formularze logowania, mechanizmy sesji, cookies, nagłówki bezpieczeństwa,
- **API Gateway i Reverse Proxy** - routing żądań, rate limiting, kontrola dostępu do endpointów,
- **Serwis Auth / IAM** - logowanie, MFA, wydawanie tokenów, reset hasła, sesje użytkowników,
- **Baza poświadczeń** - hashe haseł, dane tożsamościowe, metadane logowania,
- **Cache kodów MFA** - tymczasowe kody autoryzacyjne i ograniczenia czasowe,
- **SIEM / monitoring** - logi zdarzeń, alerty, korelacja incydentów,
- **WAF, firewall, Load Balancer** - ochrona brzegowa i dostępność usług.

5.2 Definicja i klasyfikacja incydentu

Na potrzeby niniejszego projektu przyjęto następującą definicję:

> *Incydent bezpieczeństwa to zdarzenie lub seria zdarzeń, które faktycznie naruszają albo mogą naruszyć poufność, integralność lub dostępność systemu, danych użytkowników, mechanizmów uwierzytelniania, sesji, tokenów, logów bezpieczeństwa lub infrastruktury odpowiedzialnej za proces logowania.*

Nie każde zdarzenie bezpieczeństwa jest incydentem. Pojedyncza nieudana próba logowania użytkownika jest zdarzeniem operacyjnym. Seria tysięcy prób logowania na wiele kont, pochodząca z różnych adresów IP jest już incydentem wymagającym reakcji. Takie rozróżnienie jest konieczne, aby zespół bezpieczeństwa nie był przeciążony zdarzeniami rutynowymi, a jednocześnie szybko reagował na incydenty.

Poziomy krytyczności incydentów

Dla systemu *SafeBank* przyjęto czterostopniową klasyfikację incydentów. Skala uwzględnia wpływ na klientów, dane osobowe, dostępność usługi, obowiązki prawne oraz potencjalne konsekwencje finansowe i reputacyjne. W większych środowiskach bankowych zazwyczaj poziomy krytyczności są rozbite na różne zespoły operacyjne, które mogą eskalować lub deeskalować typ incydentu do poziomów wyższych lub niższych. W opisywanym środowisku mamy do czynienia z jednym zespołem.

Poziom	Nazwa	Kryteria klasyfikacji	Przykład w SafeBank
P1	Krytyczny	Incydent powoduje lub może powodować masowe przejęcie kont, wyciek danych osobowych, utratę integralności mechanizmu logowania, długotrwałą niedostępność bankowości elektronicznej albo konieczność zgłoszenia do organu nadzorczego.	Skuteczny credential stuffing obejmujący wiele kont klientów, kompromitacja bazy poświadczeń, aktywne wykorzystanie podatności BOLA w API logowania, poważny DDoS blokujący logowanie.
P2	Wysoki	Incydent dotyczy ograniczonej grupy użytkowników lub ważnego komponentu bezpieczeństwa, ale skutki są kontrolowane. Istnieje ryzyko naruszenia danych lub eskalacji do poziomu krytycznego.	Przejęcie pojedynczego konta, obejście MFA dla wybranej grupy użytkowników, wykryta podatność SQL Injection bez potwierdzonego wycieku danych.
P3	Średni	Zdarzenie wymaga interwencji zespołu bezpieczeństwa, ale nie ma potwierdzonego naruszenia danych ani istotnej niedostępności systemu.	Seria prób brute-force na pojedyncze konto, wykrycie podejrzanych żądań API, błędna konfiguracja nagłówków bezpieczeństwa po wdrożeniu.
P4	Niski	Zdarzenie nie powoduje istotnego wpływu na bezpieczeństwo, ale powinno zostać odnotowane i przeanalizowane trendowo.	Pojedyncze skanowanie portów, pojedynczy zablokowany payload XSS przez WAF, nieudane logowanie z nietypowej lokalizacji bez dalszych anomalii.

Tabela 13: Klasyfikacja krytyczności incydentów bezpieczeństwa

5.3 Role i odpowiedzialności

Skuteczne reagowanie na incydenty wymaga jednoznacznego przypisania odpowiedzialności. W lokalnym banku z ograniczonym zespołem technicznym ta sama osoba może pełnić kilka ról, jednak formalny podział odpowiedzialności powinien zostać zachowany. Jest to szczególnie istotne przy incydentach wymagających raportowania do organów nadzorczych, komunikacji z klientami lub zachowania materiału

dowodowego.

Rola	Zakres odpowiedzialności i główne działania
Koordynator incydentu	Prowadzi incydent, nadaje priorytet P1-P4, uruchamia procedurę, koordynuje eskalację, ma kontakt z zarządem i zamyka incydenty.
SOC / osoba monitorująca SIEM	Wykrywa incydenty, analizuje logi, koreluje zdarzenia i przygotowuje oś czasu na podstawie danych z Keycloak, WAF, API Gateway, firewalli, bazy danych i systemu operacyjnego.
Administrator IAM	Zarządza kontami, sesjami, MFA i resetem haseł; blokuje konta, unieważnia sesje oraz zmienia polityki uwierzytelniania.
Administrator infrastruktury	Odpowiada za serwery, sieć, firewalle, WAF, reverse proxy, load balancer i dostępność usług; blokuje ruch, izoluje serwery i odtwarza usługi.
Zespół aplikacyjny / DevOps	Analizuje błędy aplikacyjne i podatności kodu, obsługuje pipeline CI/CD, przygotowuje poprawki, hotfixy lub rollback wdrożenia.
Inspektor Ochrony Danych / osoba ds. RODO	Ocenia naruszenia ochrony danych osobowych, decyduje o obowiązkach zgłoszeniowych i przygotowuje komunikaty dla osób, których dane dotyczą.
Zarząd / kierownictwo banku	Podejmuje decyzje biznesowe, akceptuje ryzyko i koszty działań awaryjnych, zatwierdza komunikację kryzysową oraz ewentualne czasowe wyłączenie usługi.

Tabela 15: Role i odpowiedzialności w procesie reagowania na incydenty

W przypadku incydentów P1 i P2 należy wyznaczyć jednego koordynatora incydentu. Pozwala to uniknąć sytuacji, w której równoległe działania wielu osób prowadzą do utraty dowodów, niespójnej komunikacji albo przypadkowego pogorszenia dostępności systemu.

5.4 Źródła wykrywania incydentów

Podstawą skutecznego reagowania jest zdolność do szybkiego wykrycia incydentu. W systemie SafeBank wykrywanie powinno opierać się na centralnej analizie logów, regułach korelacyjnych SIEM, alertach infrastrukturalnych, zgłoszeniach użytkowników oraz sygnałach od dostawców i zewnętrznych źródeł informacji o podatnościach.

Kluczowe źródła logów

Źródło	Znaczenie dla reakcji
WAF / firewall	Rejestruje zablokowane żądania, payloady SQLi/XSS, nietypowe nagłówki, skanowanie i anomalie adresów IP; umożliwia wczesne wykrycie ataków aplikacyjnych oraz rozpoznania systemu.
API Gateway / Reverse Proxy	Gromadzi adresy IP, ścieżki endpointów, statusy HTTP, częstotliwość żądań oraz błędy 401/403/429/500; pomaga wykrywać brute-force, credential stuffing, BOLA, nadużycia API i przeciążenia usług.
Serwis Auth / IAM	Dostarcza logi udanych i nieudanych logowań, błędów MFA, resetów haseł, zmian danych kontaktowych i wydawania tokenów; jest kluczowym źródłem detekcji przejęcia konta.
Baza danych	Rejestruje nietypowe zapytania, błędy SQL, operacje administracyjne, eksport danych i zmiany schematu; wspiera wykrywanie SQL Injection, nadużyć administracyjnych oraz dostępu do danych.
System operacyjny	Obejmuje logowania administratorów, użycie sudo, zmiany plików konfiguracyjnych i procesy systemowe; pozwala wykrywać kompromitację serwera, błędy operatora i nadużycia uprawnień.
CI/CD i repozytorium kodu	Rejestruje nowe zależności, zmiany pipeline, podpisy artefaktów, wyniki SAST/SCA i wdrożenia; pomaga wykrywać ataki supply chain oraz podatności wprowadzane przez zmiany.
Zgłoszenia klientów i infolinii	Obejmują informacje o podejrzanych SMS-ach, nieznanych logowaniach, zmianach danych i problemach z dostępem; wspierają wykrywanie phishingu, przejęcia kont i kampanii socjotechnicznych.

Tabela 17: Źródła wykrywania incydentów w systemie SafeBank

5.5 Ogólna procedura reagowania

Procedura reagowania w SafeBank obejmuje siedem etapów, które porządkują działania od momentu wykrycia incydentu do wdrożenia usprawnień po jego zakończeniu. Kolejność etapów ma charakter logiczny, jednak w praktyce analiza techniczna, ograniczanie skutków i raportowanie mogą być prowadzone równolegle.

Etap 1 - Przyjęcie i potwierdzenie zgłoszenia. Incydent może zostać wykryty przez alert SIEM, zgłoszenie klienta, administratora, test bezpieczeństwa, komunikat dostawcy lub ostrzeżenie o podatności. Każde zgłoszenie należy zarejestrować, wskazując co najmniej: datę i godzinę wykrycia, źródło zgłoszenia, osobę przyjmującą, krótki opis, dotknięty komponent, wstępny poziom krytyczności, powiązane ryzyko oraz pierwsze podjęte działania.

Etap 2 - Klasyfikacja i eskalacja. Koordynator incydentu klasyfikuje zdarzenie zgodnie z tabelą 13. Incydenty P1 i P2 wymagają natychmiastowej eskalacji do kierownictwa, administratorów, właściciela aplikacji oraz osoby odpowiedzialnej za ochronę danych. Do poziomu P1 należy eskalować zwłaszcza przejęcie wielu kont, podejrzenie wycieku danych lub poświadczeń, dostęp do danych innego użytkownika, niedostępność logowania, aktywną podatność zero-day albo nadużycie konta administratora.

Etap 3 - Analiza i zabezpieczenie dowodów. Przed działaniami zmieniającymi stan systemu należy zabezpieczyć materiał dowodowy, szczególnie przy incydentach P1 i P2. Obejmuje to eksport logów z SIEM, WAF, API Gateway, IAM, bazy danych i systemu operacyjnego, zapis adresów IP, identyfikatorów kont, tokenów, sesji i endpointów, kopię konfiguracji oraz odnotowanie działań administratorów. Dowody należy przechowywać w kontrolowanym repozytorium z ograniczonym dostępem, zgodnie z zasadą minimalizacji danych [12].

Etap 4 - Ograniczenie skutków incydentu. Celem jest zatrzymanie ataku i ograniczenie wpływu na klientów oraz system. Działania powinny być proporcjonalne do krytyczności incydentu i mogą obejmować blokadę adresów IP, zaostrzenie rate limitingu, wymuszenie MFA, unieważnienie sesji, blokadę przejętych kont, wyłączenie podatnego endpointu, rollback wdrożenia, izolację serwera lub przełączenie ruchu na zapasową infrastrukturę.

Etap 5 - Usunięcie przyczyny. Po ograniczeniu skutków należy usunąć źródło incydentu. Może to oznaczać poprawkę kodu, zmianę konfiguracji, aktualizację zależności, zmianę reguł WAF, rotację kluczy, reset haseł, usunięcie nadmiarowych uprawnień lub wyłączenie niebezpiecznej funkcji. Zmiany powinny przejść kontrolę zgodną z procedurą zarządzania zmianą.

Etap 6 - Przywrócenie działania. System można przywrócić do normalnej pracy dopiero po potwierdzeniu skuteczności poprawek. Minimalne warunki to test poprawki lub konfiguracji, brak alertów wskazujących na kontynuację ataku, poprawne działanie logowania i MFA, dostępność API Gateway oraz serwisu Auth, zachowana integralność logów i akceptacja koordynatora incydentu.

Etap 7 - Analiza poincydentowa. Po zamknięciu incydentu należy ustalić przyczynę źródłową, wykorzystaną podatność, wpływ na klientów i system, skuteczność zabezpieczeń oraz szybkość detekcji i reakcji. Wynikiem analizy powinny być konkretne działania naprawcze, przypisani właściciele, termin ponownej weryfikacji oraz decyzja o aktualizacji rejestru ryzyk. Takie podejście jest zgodne z cyklem doskonalenia reagowania na incydenty opisanym w NIST SP 800-61 Rev. 3 [6].

5.6 Scenariusze incydentów

Poniżej przedstawiono pięć scenariuszy incydentów najbardziej adekwatnych dla analizowanej ścieżki logowania i autoryzacji użytkowników. Scenariusze wynikają bezpośrednio z rejestru ryzyk i obejmują przejęcie konta, nadużycia API, podatność w komponencie logowania, przejęcie sesji oraz niedostępność procesu logowania.

Scenariusz I1 - Przejęcie konta klienta przez credential stuffing

Opis incydentu. Atakujący wykorzystuje listy loginów i haseł pochodzące z wycieków zewnętrznych serwisów, a następnie automatycznie testuje je w formularzu logowania SafeBank. Celem jest przejęcie kont klientów, którzy używali tego samego hasła w wielu usługach. Scenariusz odpowiada głównie ryzyku R1 i jest jednym z najważniejszych zagrożeń dla ścieżki logowania.

Wykrywanie. Incydent można rozpoznać po gwałtownym wzroście nieudanych prób logowania, próbach logowania na wiele kont z jednego adresu IP, próbach na jedno konto z wielu lokalizacji, zwiększonej liczbie błędów MFA oraz zgłoszeniach klientów o nieznanych powiadomieniach autoryzacyjnych.

Działania natychmiastowe. Należy sklasyfikować incydent jako P1 lub P2 zależnie od skali, zaostrzyć rate limiting, zablokować źródła ataku, wymusić MFA dla podejrzanych logowań, tymczasowo zablokować konta z dużą liczbą błędnych prób oraz unieważnić sesje kont, na których wykryto skuteczne podejrzane logowanie.

Usunięcie przyczyny i przywrócenie działania. Dla kont objętych incydentem należy wymusić zmianę hasła, zweryfikować skuteczność MFA, sprawdzić czy nie zmieniono danych kontaktowych klienta oraz dostroić reguły SIEM i WAF. Po ograniczeniu ataku system logowania może wrócić do normalnego trybu pracy, przy utrzymaniu podwyższonego monitoringu.

Raportowanie. Jeżeli doszło do skutecznego przejęcia konta i istnieje ryzyko naruszenia danych osobowych, należy przeprowadzić ocenę naruszenia zgodnie z RODO oraz wytycznymi EROD dotyczącymi zgłaszania naruszeń [12, 1]. W przypadku wysokiego ryzyka dla klientów należy rozważyć ich poinformowanie.

Działania poincydentowe. Po incydencie należy przeanalizować skuteczność MFA, rozważyć silniejsze metody uwierzytelniania, zaktualizować reguły detekcji credential stuffing, przeprowadzić działania edukacyjne dla klientów oraz ponownie ocenić ryzyko R1.

Scenariusz I2 - Obejście kontroli dostępu w API logowania lub profilu użytkownika

Opis incydentu. Atakujący manipuluje identyfikatorem zasobu w żądaniu API, próbując uzyskać dostęp do danych innego użytkownika, np. danych profilu, informacji o sesjach, historii logowań lub procesu odzyskiwania dostępu. Scenariusz odpowiada ryzyku R3 i odnosi się do podatności BOLA/IDOR.

Wykrywanie. Sygnałem incydentu może być nietypowa liczba odpowiedzi 403 lub 404, odwołania do wielu identyfikatorów użytkowników z jednej sesji, sekwencyjne zmiany parametrów w żądaniach API, alerty z testów bezpieczeństwa lub zgłoszenie użytkownika o widocznych cudzych danych.

Działania natychmiastowe. Należy tymczasowo wyłączyć podatny endpoint lub ograniczyć go regułą API Gateway, zablokować podejrzane sesje i tokeny, zabezpieczyć logi API Gateway, backendu oraz IAM, a następnie ustalić zakres danych, do których uzyskano dostęp. Jeżeli incydent dotyczy wielu użytkowników, powinien zostać sklasyfikowany jako P1.

Usunięcie przyczyny i przywrócenie działania. Należy wdrożyć kontrolę właściciela zasobu po stronie backendu, dodać testy autoryzacji obiektowej, przejrzeć podobne endpointy oraz wykonać testy kontroli dostępu przed ponownym udostępnieniem funkcji. Sama kontrola po stronie interfejsu użytkownika nie jest wystarczająca.

Raportowanie. Jeżeli potwierdzono dostęp do danych innego klienta, incydent należy ocenić jako potencjalne naruszenie ochrony danych osobowych. Trzeba określić zakres danych, liczbę osób, czas ekspozycji oraz możliwe skutki dla klientów [12, 1].

Działania poincydentowe. Po incydencie należy wykonać przegląd autoryzacji w API, zaktualizować standard implementacji endpointów, dodać testy BOLA do pipeline CI/CD, przeszkolić zespół backendowy i ponownie ocenić ryzyko R3.

Scenariusz I3 - SQL Injection w komponencie logowania lub uwierzytelniania

Opis incydentu. Atakujący wykorzystuje niewłaściwie zabezpieczony parametr formularza logowania lub endpointu uwierzytelniania w celu wykonania nieautoryzowanego zapytania SQL. Skutkiem może być odczyt danych użytkowników, modyfikacja danych logowania albo obejście mechanizmu uwierzytelniania. Scenariusz odpowiada ryzyku R2 i mieści się w kategorii podatności aplikacyjnych opisywanych przez OWASP Top 10 [11].

Wykrywanie. Incydent może zostać wykryty przez alerty WAF dotyczące payloadów SQLi, błędy 500 w endpointach logowania, nietypowe zapytania w logach bazy danych, wzrost liczby błędów SQL albo wynik testu SAST, DAST lub testu penetracyjnego.

Działania natychmiastowe. Należy zablokować źródła ataku na WAF lub firewallu, czasowo wyłączyć podatną funkcję, zabezpieczyć logi aplikacji i bazy danych oraz sprawdzić, czy doszło do odczytu lub modyfikacji danych. Przy podejrzeniu ujawnienia sekretów należy przeprowadzić rotację haseł technicznych i kluczy.

Usunięcie przyczyny i przywrócenie działania. Podatne zapytania należy zastąpić zapytaniami parametryzowanymi, zweryfikować użycie ORM, ograniczyć uprawnienia konta bazodanowego aplikacji oraz dodać test regresyjny dla wykrytej podatności. Przed przywróceniem funkcji wymagany jest ponowny test DAST lub test penetracyjny.

Raportowanie. Jeżeli analiza wykaże możliwość odczytu danych osobowych lub poświadczeń, incydent wymaga oceny pod kątem zgłoszenia naruszenia danych osobowych. W przypadku istotnego wpływu na usługę bankowości elektronicznej należy również rozważyć obowiązki wynikające z DORA i wytycznych KNF [13, 5].

Działania poincydentowe. Po incydencie należy przejrzeć wszystkie miejsca budowania zapytań SQL, rozszerzyć testy SAST i DAST, zaktualizować checklistę code review, przeszkolić zespół z bezpiecznego dostępu do bazy danych i ponownie ocenić ryzyko R2.

Scenariusz I4 - Przejęcie sesji użytkownika po zalogowaniu

Opis incydentu. Atakujący uzyskuje dostęp do aktywnej sesji użytkownika przez kradzież tokenu, XSS, błędną konfigurację cookies, malware na urządzeniu klienta lub ponowne użycie tokenu. Jest to szczególnie istotne dla ścieżki logowania, ponieważ przejęta sesja może pozwolić ominąć ponowne podanie hasła i MFA. Scenariusz odpowiada ryzyku R8 oraz częściowo R4.

Wykrywanie. Podejrzenie incydentu może wynikać z użycia tej samej sesji z różnych adresów IP, nagłej zmiany User-Agent, równoczesnej aktywności z odległych lokalizacji, alertu CSP/XSS albo zgłoszenia klienta o nieznanym aktywnym urządzeniu.

Działania natychmiastowe. Należy unieważnić podejrzaną sesję, wymusić ponowne logowanie i MFA, zablokować konto w przypadku potwierdzonego przejęcia, sprawdzić inne sesje tego samego użytkownika oraz ustalić, czy źródłem incydentu była podatność aplikacyjna, czy urządzenie klienta.

Usunięcie przyczyny i przywrócenie działania. Należy skrócić czas życia tokenów, włączyć rotację tokenów odświeżających, wymusić atrybuty cookies HttpOnly, Secure i SameSite, zaktualizować CSP oraz wdrożyć lub dostroić mechanizm wykrywania anomalii sesji.

Raportowanie. Jeżeli przejęta sesja umożliwiła dostęp do danych osobowych lub zmianę danych klienta, incydent należy ocenić pod kątem RODO. Jeżeli problem dotyczy wielu kont albo mechanizmu sesji jako całości, incydent powinien zostać potraktowany jako krytyczny.

Działania poincydentowe. Po incydencie należy przeanalizować konfigurację zarządzania sesją, sposób przechowywania tokenów po stronie klienta, wykonać testy XSS i CSP, zaktualizować reguły SIEM dla anomalii sesji oraz ponownie ocenić ryzyka R4 i R8.

Scenariusz I5 - Niedostępność procesu logowania wskutek ataku DDoS

Opis incydentu. Atakujący generuje duży ruch, np. w formularzu logowania, API Gateway, reverse proxy lub serwisie Auth, powodując opóźnienia albo brak możliwości zalogowania się przez klientów. Scenariusz odpowiada ryzyku R10 i dotyczy bezpośrednio dostępności ścieżki logowania.

Wykrywanie. Incydent można rozpoznać po nagłym wzroście liczby żądań do endpointów logowania, zwiększonej liczbie odpowiedzi 429, 502, 503 lub timeoutów, przeciążeniu load balancera, wydłużonym czasie odpowiedzi serwisu Auth oraz zgłoszeniach klientów o braku możliwości zalogowania.

Działania natychmiastowe. Należy aktywować ochronę anty-DDoS u dostawcy, zaostrzyć rate limiting i reguły WAF, odrzucać ruch o niskiej reputacji, monitorować obciążenie komponentów oraz w razie potrzeby przełączyć ruch na zapasową infrastrukturę. Komunikacja z klientami powinna jasno wskazywać, że problem dotyczy dostępności usługi.

Usunięcie przyczyny i przywrócenie działania. W przypadku DDoS źródła ataku zwykle nie da się usunąć po stronie banku, dlatego działania koncentrują się na filtracji, absorpcji ruchu i utrzymaniu dostępności. Po ustaniu ataku należy stopniowo przywrócić standardowe limity, sprawdzić stan komponentów i pozostawić podwyższony monitoring.

Raportowanie. Jeżeli atak spowodował znaczną niedostępność usługi bankowej, należy rozważyć raportowanie zgodnie z wymaganiami DORA oraz wytycznymi KNF dotyczącymi zarządzania IT i bezpieczeństwem teleinformatycznym [13, 5].

Działania poincydentowe. Po incydencie należy przeanalizować parametry ruchu, skuteczność filtracji, progi rate limitingu, działanie WAF i ochrony anty-DDoS, wykonać test przełączenia awaryjnego, zaktualizować plan ciągłości działania oraz ponownie ocenić ryzyko R10.

5.7 Procedura raportowania incydentów

Raportowanie incydentów w SafeBank ma trzy poziomy: raportowanie wewnętrzne, raportowanie regulacyjne oraz komunikację z klientami. Zakres raportowania zależy od krytyczności incydentu, wpływu na dane osobowe, dostępność usługi oraz obowiązków wynikających z przepisów prawnych.

Raportowanie wewnętrzne

Każdy incydent P1-P3 powinien zostać udokumentowany w wewnętrznym rejestrze incydentów. Incydenty P1 i P2 wymagają dodatkowo bieżących raportów statusowych dla kierownictwa. Raport powinien być aktualizowany po każdej istotnej zmianie stanu incydentu.

Raport wewnętrzny powinien zawierać:

- identyfikator incydentu,
- datę i godzinę wykrycia,
- datę i godzinę rozpoczęcia incydentu, jeżeli można ją ustalić,
- źródło wykrycia,
- opis zdarzenia,
- poziom krytyczności,
- dotknięte komponenty,

- dotknięte konta lub grupy użytkowników,
- ocenę wpływu na poufność, integralność i dostępność,
- działania ograniczające skutki,
- osoby odpowiedzialne,
- status incydentu,
- decyzje dotyczące raportowania zewnętrznego.

Raportowanie naruszeń danych osobowych

Jeżeli incydent może skutkować naruszeniem ochrony danych osobowych, należy przeprowadzić formalną ocenę zgodnie z RODO. Naruszenie ochrony danych osobowych może obejmować nie tylko potwierdzony wyciek danych, ale również nieuprawniony dostęp, utratę integralności, przypadkowe ujawnienie, nieautoryzowaną zmianę lub czasową niedostępność danych, jeżeli wpływa ona na prawa i wolności osób fizycznych [12].

Ocena powinna uwzględniać:

- rodzaj danych objętych incydentem,
- liczbę osób, których dane dotyczą,
- możliwość identyfikacji osób,
- potencjalne skutki dla klientów,
- czas trwania naruszenia,
- zastosowane środki minimalizujące skutki,
- prawdopodobieństwo wykorzystania danych przez osoby nieuprawnione.

Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych, należy przygotować zgłoszenie do właściwego organu nadzorczego. Jeżeli ryzyko jest wysokie, należy również poinformować osoby, których dane dotyczą. Zasady oceny i zgłaszania naruszeń powinny być zgodne z wytycznymi EROD 9/2022 [1].

Raportowanie sektorowe i regulacyjne

Jako system bankowości elektronicznej SafeBank powinien uwzględniać wymagania regulacyjne dotyczące odporności cyfrowej oraz zarządzania bezpieczeństwem teleinformatycznym. W przypadku poważnych incydentów wpływających na dostępność, integralność lub bezpieczeństwo usług finansowych należy rozważyć obowiązki wynikające z DORA oraz wytycznych KNF [13, 5]. Dotyczy to szczególnie incydentów, które:

- wpływają na znaczną liczbę klientów,

- powodują istotną niedostępność bankowości elektronicznej,
- dotyczą usług krytycznych,
- mogą prowadzić do strat finansowych,
- mają charakter powtarzalny lub systemowy,
- wskazują na niewystarczającą odporność operacyjną organizacji.

Komunikacja z klientami

Komunikacja z klientami powinna być rzeczowa, zrozumiała i ograniczona do informacji potwierdzonych. Nie należy ujawniać szczegółów technicznych, które mogłyby ułatwić dalsze ataki. Jednocześnie komunikat powinien zawierać jasne instrukcje dla klientów, jeżeli wymagane jest ich działanie, np. zmiana hasła, ponowna aktywacja MFA lub kontakt z infolinią.

Komunikat dla klientów powinien zawierać:

- opis rodzaju incydentu w zrozumiałym języku,
- informację, czy dane klienta mogły zostać naruszone,
- działania wykonane przez bank,
- zalecane działania klienta,
- kanał kontaktu w razie pytań,
- ostrzeżenie przed phishingiem wykorzystującym incydent.

5.8 Szablon raportu incydentu

Dla zachowania spójności dokumentacji każdy incydent P1-P3 powinien zostać opisany według jednolitego szablonu. Szablon może zostać wykorzystany zarówno w dokumentacji wewnętrznej, jak i jako podstawa do raportów dla kierownictwa.

Pole raportu	Opis
ID incydentu	Unikalny identyfikator incydentu.
Data i godzina wykrycia	Moment pierwszego wykrycia lub zgłoszenia.
Data i godzina rozpoczęcia	Moment rozpoczęcia incydentu, jeżeli możliwy do ustalenia.
Źródło wykrycia	SIEM, klient, administrator, dostawca, test bezpieczeństwa.
Poziom krytyczności	P1, P2, P3 lub P4.
Opis incydentu	Krótki, rzeczowy opis zdarzenia.
Dotknięte komponenty	IAM, API Gateway, baza danych, WAF, frontend, CI/CD itp.
Powiązane ryzyka	Identyfikatory z rejestru ryzyk, np. R1, R3, R8.
Wpływ na CIA	Ocena wpływu na poufność, integralność i dostępność.
Zakres klientów / danych	Liczba kont, typ danych, potencjalny zakres naruszenia.
Działania ograniczające	Blokady, wyłączenia, reset haseł, unieważnienie sesji.
Działania naprawcze	Poprawki kodu, zmiany konfiguracji, aktualizacje, rotacja sekretów.
Raportowanie zewnętrzne	Decyzja dotycząca UODO, KNF, DORA, klientów.
Przyczyna źródłowa	Techniczna lub organizacyjna przyczyna incydentu.
Wnioski i usprawnienia	Działania zapobiegające powtórzeniu incydentu.
Status	Otwarty, ograniczony, usunięty, zamknięty.

Tabela 19: Szablon raportu incydentu bezpieczeństwa

5.9 Wskaźniki skuteczności reagowania

Aby plan reagowania był mierzalny, należy zdefiniować wskaźniki skuteczności. Bez takich wskaźników organizacja może posiadać formalną procedurę, ale nie będzie wiedziała, czy procedura faktycznie działa w warunkach incydentu.

Wskaźnik	Znaczenie	Przykładowy cel
MTTD	Średni czas wykrycia incydentu od momentu jego rozpoczęcia.	Dla P1 poniżej 30 minut, dla P2 poniżej 2 godzin.
MTTA	Średni czas potwierdzenia i przypisania incydentu do osoby odpowiedzialnej.	Dla P1 poniżej 15 minut.
MTTC	Średni czas ograniczenia skutków incydentu.	Dla przejęcia konta poniżej 1 godziny od potwierdzenia.
MTTR	Średni czas przywrócenia normalnego działania.	Zgodny z wymaganiami BCP/DRP i krytycznością usługi.
Odsetek fałszywych alarmów	Liczba alertów niebędących incydentami w stosunku do wszystkich alertów.	Stałe obniżanie przez dostrajanie reguł SIEM.
Pokrycie logowania	Odsetek krytycznych komponentów przesyłających logi do SIEM.	100% dla komponentów ścieżki logowania.
Realizacja działań poincydentowych	Odsetek działań naprawczych wykonanych w terminie.	Minimum 90% działań zamkniętych w terminie.

Tabela 21: Wskaźniki skuteczności reagowania na incydenty

5.10 Działania poincydentowe i doskonalenie systemu

Zamknięcie incydentu nie kończy procesu reagowania. Najważniejszym elementem dojrzałego zarządzania incydentami jest wykorzystanie zdarzenia do poprawy bezpieczeństwa organizacji. Wnioski z incydentu powinny wpływać na rejestr ryzyk, zabezpieczenia, procedury, monitoring, szkolenia i wymagania projektowe.

Po każdym incydencie P1-P3 należy przeprowadzić spotkanie poincydentowe. Spotkanie powinno mieć charakter analityczny, a nie personalnie obciążający. Celem jest ustalenie, co zawiodło w systemie, procesie lub komunikacji, a nie wskazanie winnej osoby.

Minimalny zakres analizy poincydentowej:

- czy incydent został wykryty automatycznie, czy przez użytkownika,
- czy alerty SIEM były wystarczająco precyzyjne,
- czy klasyfikacja incydentu była prawidłowa,
- czy działania ograniczające skutki były skuteczne,
- czy procedura eskalacji zadziałała,
- czy zabezpieczono wystarczający materiał dowodowy,
- czy istniejące zabezpieczenia ograniczyły wpływ incydentu,
- jakie kontrole należy dodać lub poprawić.

Wynikiem analizy powinien być plan działań naprawczych zawierający właściciela, termin realizacji oraz sposób weryfikacji.

6 Ochrona danych osobowych i aspekty prawne

Przetwarzanie danych w ramach systemu logowania SafeBank podlega wielowarstwowym regulacjom. W przypadku banku o charakterze lokalnym, wyzwaniem jest zachowanie pełnej zgodności z restrykcyjnymi wymogami przy wykorzystaniu zasobów ograniczonych budżetowo. Poniżej przedstawiono analizę prawno-informatyczną w odniesieniu do ścieżki logowania.

6.1 Zgodność z RODO (GDPR)

System logowania realizuje kluczowe zasady ochrony danych osobowych oraz obowiązki prawne zgodnie z RODO [12] poprzez następujące mechanizmy:

- **Podstawa przetwarzania danych:** Przetwarzanie danych uwierzytelniających opiera się na niezbędności do wykonania umowy o świadczenie usług bankowości elektronicznej (art. 6 ust. 1 lit. b RODO) oraz obowiązku prawnym ciążącym na administratorze (art. 6 ust. 1 lit. c RODO) w związku z wymogami silnego uwierzytelniania.

- **Minimalizacja danych:** Gromadzone are wyłącznie poświadczenia (login) i metadane techniczne (IP, znacznik czasu) niezbędne do weryfikacji tożsamości.

- **Integralność i poufność:** Zastosowanie nieodwracalnych skrótów haseł (hashing) oraz szyfrowania TLS 1.3 eliminuje ryzyko odczytu danych przez osoby nieuprawnione.

- **Ograniczenie przechowywania (retencja):** Czas przechowywania danych jest ściśle dostosowany do ich charakteru i celów operacyjno-prawnych. Tymczasowe kody MFA w pamięci podręcznej wygasają po **15 minutach**, logi sesyjne oraz zdarzenia bezpieczeństwa w systemie SIEM są przechowywane przez **12 miesięcy** w celach audytowych i powłamaniowych, natomiast dane o historii autoryzacji klientów są retencjonowane przez okres **5 lat** od momentu zamknięcia rachunku, zgodnie z wymogami Prawa Bankowego [12].

- **Rozliczalność i obowiązki administratora:** Każda próba logowania oraz każda operacja administratora na bazie poświadczeń jest trwale rejestrowana w audytowalnych logach. Bank jako administrator realizuje również obowiązek zgłaszania naruszeń (art. 33 RODO) w oparciu o wdrożone procedury reagowania na incydenty.

6.2 Uproszczona Ocena Skutków dla Ochrony Danych (DPIA)

Zgodnie z art. 35 RODO, systematyczne przetwarzanie krytycznych danych uwierzytelniających wymaga przeprowadzenia oceny skutków dla ochrony danych (DPIA) [2]. Poniżej przedstawiono uproszczoną ocenę, stanowiącą wkład analityczny do pełnego raportu DPIA dla tego procesu:

- **Zagrożenia dla praw i wolności osób:** Materializacja zidentyfikowanych w analizie ryzyk (np. R1 – przejęcie konta klienta, R2 – nieuprawniony odczyt bazy poświadczeń) niesie za sobą bezpośrednie zagrożenie kradzieży tożsamości,

naruszenia tajemnicy bankowej oraz dotkliwych strat finansowych dla osób, których dane dotyczą.

- **Ocena ryzyka dla prywatności (Privacy Risk):** Biorąc pod uwagę dużą skalę przetwarzania oraz krytyczny charakter danych (poświadczenia, dane finansowe), wbudowane ryzyko dla prywatności ocenia się jako **Krytyczne**. Bez odpowiednich kontroli, prawdopodobieństwo skutecznego ataku (np. Credential Stuffing) i jego wpływ na jednostkę są bardzo wysokie.

- **Środki minimalizacji ryzyka:** W celu obniżenia ryzyka do poziomu akceptowalnego, wdrożono techniczne i organizacyjne środki minimalizacji opisane szczegółowo w Rozdziale 4. Obejmują one m.in. silne uwierzytelnianie klienta (MFA), szyfrowanie danych w spoczynku i w locie (TLS 1.3, nieodwracalny hashing z solą) oraz ciągłe monitorowanie anomalii przez system SIEM. Środki te redukują rezydualne ryzyko dla prywatności do poziomu akceptowalnego w sektorze bankowym.

6.3 Wymogi Sektora Finansowego (KNF i Prawo Bankowe)

Jako instytucja finansowa, bank wdraża specyficzne zabezpieczenia wynikające z przepisów krajowych i unijnych:

- **Tajemnica Bankowa (Art. 104 Prawa Bankowego):** Dane logowania są traktowane jako informacje objęte tajemnicą [15]. System zapewnia izolację tych danych od procesów niezwiązanych z autoryzacją.

- **Silne Uwierzytelnienie (SCA):** Zgodnie z dyrektywą PSD2, logowanie wymaga dwóch niezależnych składników (hasło + kod SMS/Push), co minimalizuje ryzyko przejęcia konta [3].

- **Rekomendacja D KNF:** System realizuje wytyczne dotyczące zarządzania obszarami IT, w szczególności w zakresie bezpieczeństwa kanałów elektronicznych i nienaruszalności logów zdarzeń [4].

6.4 Zarządzanie Outsourcingiem i Cyberodpornością

Specyfika banku korzystającego z rozwiązań zastanych (*on-hand*) wymaga szczególnego podejścia do usług zewnętrznych:

- **Outsourcing Bankowy (Art. 6a-6d):** Wykorzystanie zewnętrznej bramki do wysyłki kodów MFA (SMS) podlega rygorom outsourcingu wynikającym z Prawa Bankowego [15]. Dane przesyłane do operatora są pseudonimizowane (tylko nr telefonu i kod, bez danych osobowych).

- **Zgodność z DORA i KSC:** System logowania jest sklasyfikowany jako usługa kluczowa. Bank posiada procedury zgłaszania incydentów do właściwego CSIRT sektorowego oraz plany awaryjne na wypadek niedostępności serwisu autoryzacyjnego [13, 5].

6.5 Analiza luk i rekomendacje poprawy

W toku analizy zidentyfikowano następujące obszary, które wymagają wzmocnienia w celu pełnego zabezpieczenia interesów prawnych banku:

1. **Ochrona kluczy (HSM):** Brak sprzętowego modułu HSM jest punktem spornym w kontekście pełnej zgodności z Rekomendacją D [4]. Rekomenduje się wdrożenie procedury *Dual Control* przy zarządzaniu kluczami programowymi.

2. **Strategia wyjścia (Exit Strategy):** Dla rozwiązań *Open Source* (Keycloak/Nginx) należy sformalizować plany na wypadek zaprzestania wsparcia tych projektów przez społeczność, co jest wymagane przez rozporządzenie DORA [13].

3. **Audyt ciągły:** Sugeruje się wdrożenie zautomatyzowanych narzędzi do monitorowania zmian w uprawnieniach administratorów posiadających dostęp do bazy poświadczeń [5].

7 Analiza finansowa

Niniejszy rozdział przedstawia ekonomiczne uzasadnienie wdrożenia proponowanych zabezpieczeń dla ścieżki logowania systemu SafeBank. Analiza uwzględnia specyfikę banku lokalnego, opierając się na modelu maksymalnego wykorzystania zasobów własnych („on-hand") oraz technologii Open Source, co jest zgodne z wytycznymi dotyczącymi optymalizacji kosztów IT w małych instytucjach finansowych [5]. Zgodnie z przyjętą metodologią, dokonano rozróżnienia między posiadanymi aktywami a niezbędnymi nowymi inwestycjami.

7.1 Zasoby zastane i koszty bieżące (Stan obecny)

Architektura systemu opiera się na wykorzystaniu posiadanej już infrastruktury sprzętowej oraz darmowego oprogramowania, co pozwala na uniknięcie znacznych wydatków początkowych (CAPEX). Wykorzystanie rozwiązań takich jak Keycloak Community Edition wymaga jednak od zespołu IT samodzielnego zarządzania bezpieczeństwem łańcucha dostaw [16].

Kategoria	**Komponent / Zasób**	**Typ**	**Koszt dodatkowy**
Sprzęt	Serwery Dell PowerEdge (istniejąca flota)	CAPEX	0 PLN
Infrastruktura	Modernizacja serwerów (RAM, dyski SSD)	CAPEX	15 000 – 30 000 PLN
Oprogramowanie	System Linux, PostgreSQL, Keycloak CE	CAPEX	0 PLN
Utrzymanie	Wewnętrzny zespół IT (bieżąca obsługa)	OPEX	W ramach etatu
Monitoring	Rozwiązania Zabbix / Graylog	OPEX	0 PLN
Weryfikacja	Roczne testy penetracyjne [9]	OPEX	30 000 – 50 000 PLN

Tabela 23: Zestawienie zasobów zastanych wykorzystywanych w procesie logowania.

7.2 Szacunkowy koszt proponowanych usprawnień

W celu mitygacji ryzyk krytycznych, takich jak kradzież tożsamości czy ataki na API [8], niezbędne jest poniesienie nakładów na modernizację i nowe mechanizmy kontrolne.

Kategoria	**Komponent / Działanie**	**Typ**	**Szacunkowy koszt**
Bezpieczeństwo	Urządzenia brzegowe i UTM (np. FortiGate/pfsense)	CAPEX	15 000 – 30 000 PLN
Komunikacja	Bramka SMS do obsługi kodów MFA (koszt roczny)	OPEX	10 000 – 30 000 PLN

Tabela 25: Koszty nowych inwestycji w zabezpieczenia ścieżki logowania.

7.3 Optymalizacja i racjonalizacja doboru zabezpieczeń

Przyjmując perspektywę banku lokalnego, dokonano świadomej selekcji zabezpieczeń, rezygnując z rozwiązań o skrajnie wysokim koszcie wdrożenia, których brak nie uniemożliwia zachowania akceptowalnego poziomu bezpieczeństwa:

- **Rezygnacja z fizycznego modułu HSM:** Zamiast kosztownego sprzętowego modułu HSM, zdecydowano się na programową realizację operacji kryptograficznych. Mimo że Rekomendacja D sugeruje stosowanie rozwiązań sprzętowych [4], dla instytucji tej skali ryzyko uznano za akceptowalne przy zastosowaniu procedur Dual Control.
- **Priorytetyzacja MFA i WAF:** Nakłady finansowe skierowano głównie na mechanizmy silnego uwierzytelniania [3, 17] i ochronę brzegową, ponieważ to one mitygują najbardziej prawdopodobne ataki [7, 11].

7.4 Oszacowanie strat w przypadku incydentu (Model Ilościowy)

Materializacja ryzyk krytycznych, takich jak przejęcie kont klientów (R1) lub wyciek bazy poświadczeń (R2), generuje straty znacznie wykraczające poza bezpośrednie koszty techniczne. W celu obiektywizacji kosztów zastosowano standardowy model ilościowej oceny ryzyka oparty na wskaźnikach SLE (Single Loss Expectancy), ARO (Annualized Rate of Occurrence) oraz ALE (Annualized Loss Expectancy).

Wartość pojedynczej straty (SLE) w przypadku poważnego incydentu (wyciek danych logowania) oszacowano na podstawie potencjalnych kar z tytułu RODO [12], kosztów przywrócenia ciągłości działania (DRP) oraz strat wizerunkowych na kwotę ok. 2 000 000 PLN. Prawdopodobieństwo wystąpienia takiego incydentu w ciągu roku (ARO) dla niezabezpieczonego systemu (ryzyko wbudowane Krytyczne) szacuje się ostrożnie na 10%.

Oczekiwana strata roczna (ALE) przed wdrożeniem kontroli wynosi zatem:

$$ALE_{wbudowane} = SLE \times ARO$$

$$ALE_{wbudowane} = 2000000PLN \times 0.10 = 200000PLN$$

7.5 Porównanie kosztu kontroli z potencjalnymi stratami i ROSI

Wdrożenie kompleksowych zabezpieczeń (WAF, MFA, SIEM), których roczny zsumowany koszt (CAPEX zamortyzowany + OPEX) szacuje się na ok. 100 000 PLN (Koszty Kontroli), obniża prawdopodobieństwo skutecznego ataku (ARO) do poziomu 1%.

Nowa wartość oczekiwanej straty rocznej po wdrożeniu zabezpieczeń wynosi:

$$ALE_{rezydualne} = 2000000PLN \times 0.01 = 20000PLN$$

Aby ocenić opłacalność inwestycji, obliczono wskaźnik zwrotu z inwestycji w bezpieczeństwo (ROSI – Return on Security Investment), korzystając z klasycznego wzoru:

$$ROSI = \frac{ALE_{wbudowane} - ALE_{rezydualne} - KosztyKontroli}{KosztyKontroli} \times 100\%$$

$$ROSI = \frac{200000 - 20000 - 100000}{100000} \times 100\% = 80\%$$

Parametr finansowy	**Wartość szacunkowa**
Wartość pojedynczej straty (SLE)	2 000 000 PLN
Oczekiwana strata roczna przed kontrolą ($ALE_{wbudowane}$)	200 000 PLN
Roczne koszty wdrożenia i utrzymania kontroli	100 000 PLN
Oczekiwana strata roczna po wdrożeniu kontroli ($ALE_{rezydualne}$)	20 000 PLN
Szacowany wskaźnik ROSI	**80%**

Tabela 27: Kwantytatywne zestawienie redukcji ryzyka i wskaźnika ROSI.

Dodatni i wysoki wskaźnik ROSI na poziomie 80% jednoznacznie udowadnia, że proponowane w niniejszym dokumencie rozwiązania mitygujące są w pełni opłacalne biznesowo i chronią instytucję przed katastrofalnymi skutkami finansowymi.

7.6 Wskazanie poziomu ryzyka po wdrożeniu zabezpieczeń

Dzięki zastosowaniu opisanych kontroli, ogólny poziom ryzyka systemu logowania został zredukowany do poziomu akceptowalnego przez regulatora [4, 5]:

- **Ryzyka krytyczne (R1-R3):** Zredukowane z poziomu Krytycznego do Średniego/Wysokiego [14].
- **Ryzyko rezydualne:** Na poziomie wysokim pozostają zagrożenia o silnym komponencie zewnętrznym (np. phishing), wymagające ciągłej edukacji użytkowników i monitorowania anomalii [7, 13].

8 Podsumowanie i wnioski końcowe

Przeprowadzona kompleksowa analiza ryzyka oraz opracowanie planu reagowania na incydenty dla systemu bankowości elektronicznej **SafeBank** pozwoliły na dogłębną ocenę stanu bezpieczeństwa badanej organizacji. Zgodnie z przyjętymi założeniami, badanie skoncentrowano na krytycznym wycinku architektury, jakim jest ścieżka logowania i autoryzacji użytkowników. Pozwoliło to na sformułowanie precyzyjnych wniosków dotyczących zarówno technologicznej odporności „bramy wejściowej" systemu, jak i wyzwań operacyjnych stojących przed lokalną instytucją finansową.

8.1 Wnioski końcowe

Na podstawie przeprowadzonych prac analitycznych, w tym oceny podatności, klasyfikacji ryzyk oraz analizy finansowo-prawnej, sformułowano następujące wnioski końcowe:

1. **Krytyczne znaczenie ścieżki logowania:** Analiza potwierdziła, że proces uwierzytelniania jest najbardziej eksponowanym i ryzykownym elementem systemu bankowego. Zastosowanie metodyki OWASP wykazało, że błędy w tym obszarze (takie jak podatność na *Credential Stuffing* czy *Session Hijacking*) niosą za sobą najwyższy potencjał strat biznesowych i wizerunkowych, prowadząc do bezpośredniego przejęcia kont klientów.

2. **Skuteczność, ale i wyzwania modelu budżetowego:** Przyjęta przez bank architektura oparta w dużej mierze na rozwiązaniach Open Source (m.in. Keycloak, Nginx, PostgreSQL) pozwala na znaczną optymalizację kosztów inwestycyjnych (CAPEX). Jendak generuje ona podwyższone ryzyko operacyjne. Brak dedykowanego wsparcia producentów (SLA) nakłada na wewnętrzny zespół IT ogromną odpowiedzialność za monitorowanie podatności typu zero-day oraz szybkie wdrażanie poprawek.

3. **Zgodność regulacyjna a kompromisy technologiczne:** Zaproponowane zabezpieczenia pozwalają na osiągnięcie zgodności z podstawowymi wymogami RODO, dyrektywą PSD2 (w zakresie silnego uwierzytelniania – SCA) oraz wytycznymi KNF. Zidentyfikowano jednak dług technologiczny – w szczególności brak sprzętowego modułu HSM do ochrony kluczy kryptograficznych, który w przypadku rygorystycznego audytu zgodności z Rekomendacją D może zostać uznany za lukę wymagającą natychmiastowej mitygacji.

4. **Czynnik ludzki jako najsłabsze ogniwo:** Pomimo wdrożenia technicznych mechanizmów obronnych (WAF, MFA, SIEM), ryzyka o najwyższym poziomie rezydualnym pozostają ściśle powiązane z działaniami użytkowników. Phishing, socjotechnika oraz potencjalne błędy konfiguracyjne po stronie administratorów wymagają ciągłej edukacji, weryfikacji uprawnień (zasada *Least Privilege*) oraz rygorystycznego monitorowania procesów.

5. **Zasadność inwestycji w bezpieczeństwo (ROSI):** Analiza finansowa jednoznacznie wykazała, że koszty wdrożenia i utrzymania zaproponowanych mechanizmów kontrolnych są niewspółmiernie niskie w porównaniu do potencjalnych kar administracyjnych (np. z tytułu naruszenia RODO) oraz strat

wynikających z utraty płynności finansowej banku po poważnym incydencie wycieku danych poświadczeń.

8.2 Rekomendacje rozwojowe

W celu stałego podnoszenia poziomu cyfrowej odporności operacyjnej systemu SafeBank, w szczególności w kontekście nadchodzących wymogów rozporządzenia DORA, rekomenduje się podjęcie następujących działań w średnim i długim horyzoncie czasowym:

- **Ewolucja mechanizmów MFA:** Docelowe odejście od kodów jednorazowych opartych na kanale SMS, który jest podatny na ataki typu *SIM swapping*, na rzecz silniejszych metod uwierzytelniania, takich jak powiadomienia *Push* w aplikacji mobilnej wsparte biometrią lub wdrożenie standardu FIDO2 (klucze sprzętowe/Passkeys).
- **Eliminacja długu kryptograficznego:** Zaplanowanie w budżecie na kolejne lata inwestycji (CAPEX) w dedykowane, sprzętowe moduły bezpieczeństwa (HSM), co zniweluje ryzyko R7 (kompromitacja kluczy w warstwie programowej) i zapewni pełną zgodność z wytycznymi KNF.
- **Automatyzacja procesów SOC:** Rozbudowa wdrożonego systemu monitorowania (SIEM) o zaawansowane reguły korelacyjne i analizę behawioralną (UEBA), co pozwoli na drastyczne skrócenie czasu wykrycia (MTTD) zautomatyzowanych ataków na formularze logowania.
- **Cykliczna weryfikacja ofensywna:** Wdrożenie stałego harmonogramu testów penetracyjnych (minimum raz w roku) skupionych wyłącznie na ścieżce logowania, mechanizmach odzyskiwania hasła oraz zarządzaniu tokenami sesyjnymi.

Podsumowując, system **SafeBank** posiada solidne podstawy architektoniczne do bezpiecznego zarządzania tożsamością i autoryzacją użytkowników. Pełne bezpieczeństwo procesu logowania jest jednak stanem dynamicznym, wymagającym od lokalnego banku ciągłego monitorowania zagrożeń, regularnej aktualizacji rejestru ryzyk oraz ścisłego stosowania opracowanych procedur reagowania na incydenty.

Bibliografia

[1] Europejska Rada Ochrony Danych, 2023. Wytyczne 9/2022 dotyczące zgłaszania naruszeń danych. [**online**]. Dostępny na: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en [Dostęp: 5 maj. 2026].

[2] Grupa Robocza Art. 29, 2017. Wytyczne dotyczące oceny skutków dla ochrony danych DPIA. [**online**]. Dostępny na: https://ec.europa.eu/newsroom/article29/items/611236/en [Dostęp: 5 maj. 2026].

[3] Komisja Europejska, 2018. PSD2 RTS – silne uwierzytelnianie klienta i bezpieczna komunikacja. [**online**]. Dostępny na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389 [Dostęp: 5 maj. 2026].

[4] Komisja Nadzoru Finansowego, 2013. Rekomendacja D – bezpieczeństwo IT w bankach. [**online**]. Dostępny na: https://www.knf.gov.pl/knf/pl/komponenty/img/rekomendacja_d_8_01_13_uchwala_7_33016.pdf [Dostęp: 5 maj. 2026].

[5] Komisja Nadzoru Finansowego, 2025. Wytyczne KNF dotyczące zarządzania IT i bezpieczeństwem teleinformatycznym. [**online**]. Dostępny na: https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/wytyczne_dotyczace_zarzadzania_obszarami_IT [Dostęp: 5 maj. 2026].

[6] Nelson, A. i in., 2025. NIST SP 800-61 Rev. 3 – reagowanie na incydenty. [**online**]. Dostępny na: https://doi.org/10.6028/NIST.SP.800-61r3 [Dostęp: 5 maj. 2026].

[7] ORANGE, 2025. Raport CERT Orange Polska. [**online**]. Dostępny na: https://cert.orange.pl/raporty-cert-orange-polska/ [Dostęp: 26 kw. 2026].

[8] OWASP Foundation, 2023. OWASP API Security Top 10 – 2023. [**online**]. Dostępny na: https://owasp.org/API-Security/editions/2023/en/0x00-header/ [Dostęp: 5 maj. 2026].

[9] OWASP Foundation, 2025. OWASP Application Security Verification Standard. [**online**]. Dostępny na: https://owasp.org/www-project-application-security-verification-standard/ [Dostęp: 5 maj. 2026].

[10] OWASP Foundation, 2025. OWASP Risk Rating Methodology. [**online**]. Dostępny na: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology [Dostęp: 5 maj. 2026].

[11] OWASP Foundation, 2025. OWASP Top 10 List. [**online**]. Dostępny na: https://owasp.org/Top10/2025/ [Dostęp: 27 mar. 2026].

[12] Parlament Europejski i Rada Unii Europejskiej, 2016. RODO – rozporządzenie 2016/679 o ochronie danych osobowych. [**online**]. Dostępny na: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 [Dostęp: 5 maj. 2026].

[13] Parlament Europejski i Rada Unii Europejskiej, 2022. DORA – rozporządzenie 2022/2554 o odporności cyfrowej sektora finansowego. [**online**]. Dostępny na: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022R2554 [Dostęp: 5 maj. 2026].

[14] Ross, R., 2012. NIST SP 800-30 – analiza ryzyka. [**online**]. Dostępny na: https://doi.org/10.6028/NIST.SP.800-30r1 [Dostęp: 5 maj. 2026].

[15] Sejm RP. *Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe*. t.j. Dz. U. z 2023 r. poz. 2486 z późn. zm. 1997. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971400939 5 maj. 2026.

[16] Souppaya, M., Scarfone, K. i Dodson, D., 2022. NIST SP 800-218 – bezpieczne wytwarzanie oprogramowania. [**online**]. Dostępny na: https://doi.org/10.6028/NIST.SP.800-218 [Dostęp: 5 maj. 2026].

[17] Temoshok, D. i in., 2025. NIST SP 800-63B-4 – uwierzytelnianie i zarządzanie metodami uwierzytelniania. [**online**]. Dostępny na: https://doi.org/10.6028/NIST.SP.800-63B-4 [Dostęp: 5 maj. 2026].