# Ocena projektu grupy: Michał Gawron 172833, Tomasz Synak 180713

**Grupa oceniająca: Michał Negacz 179120, Piotr Wróblewski 179198**

# Identyfikacja podejść architektonicznych

|  |  |
| --- | --- |
| **Goal** | **How achieved (Tactics)** |
| Bezpieczeństwo | Autoryzacja (jest) Uwierzytelnianie (jest) Szyfrowanie wrażliwych danych użytkowników (jest) Walidacja danych otrzymanych od użytkownika (nowa) Walidacja danych zapisywanych do bazy (nowa) |
| Wydajność | Cache’owanie przetworzonych danych (prawdopodobnie jest tzn. zasobów i wyników wyszukiwania) Asynchroniczne wykonywanie czasochłonnych operacji (jest) |
| Dostępność | Wybór sprzętu odpornego na awarie (jest – zapewnienie dostępności) Wybór sprzętu wysokiej wydajności (nowe) Równoważenie obciążenia (nowe) Rozproszenie lokalnej bazy danych (nowe) Rozproszenie serwerów aplikacji IIS (nowe) |
| Pielęgnowalność | ORM i relacyjny schemat bazy danych  Wzorzec MVC |

# Drzewo użyteczności atrybutów jakości

* Użyteczność
  + Wydajność
    - Maksymalne opóźnienie
      * Maksymalne opóźnienie ładowania wynoszące 5 sekund. (H, H)
  + Modyfikowalność
    - Nowe produkty
      * Dodanie warstwy z WCF’em w mniej niż 2 osoby w tydzień(M,M)
      * Dodanie nowej relacji w bazie danych, wraz z operacjami CRUD w aplikacji w mniej niż 2 osoby w tydzień.(M,H)
    - Zmiany w bieżących funkcjonalnościach
      * Przebudowanie całego interfejsu użytkownika w mniej niż 4 osoby w tydzień(M, M)
      * Podpięcie danych od nowego operatora w mniej niż 1 osoba w 4 dni(M,M)
  + Dostępność
    - Geograficzna
      * Dostępność do serwisu w dowolnym miejscu(M, M)
    - Czasowa
      * Dostępność do serwisu o dowolnym czasie na poziomie 99% w roku(H, H)
  + Bezpieczeństwo
    - Poufność danych
      * Operacje wymagające kontroli dostępu zawsze będą wymagały wcześniejszego uwierzytelniania(jedno uwierzytelnienia dla wielu operacji).(H,M)
    - Integralność danych
      * Całkowite zabezpieczenie przed nieautoryzowanym odczytem haseł. (H, L)
      * Wykonywanie płatności w 100% gwarantuje bezpieczeństwo przed nieautoryzowanym odczytem danych transakcji bankowej.(H ,L)
    - Spójność danych
      * 100% danych w bazie danych jest zgodna z rzeczywistością (H, L)

**Analiza podejść architektonicznych**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Maksymalne opóźnienie ładowania wynoszące 5 sekund. (H, H) | | | |
| Atrybuty | Wydajność – maksymalne opóźnienie | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Dokonanie rezerwacji przez użytkownika | | | |
| Odpowiedź | Dla 1000 użytkowników jednocześnie mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Aplikacja hostowana w chmurze | S1 |  |  | NR1 |
| Mechnizmy async/await |  |  | R1 |  |
| ASP.NET Caching | S2 |  |  |  |

NR1: Zostawienie konieczności dbania o infrastrukturę specjalistom.

S1: Możliwość uzależnienia się od rozwiązań jednego dostawcy(utrudnione przeniesienie aplikacji).

R1: Mechanizmy wielowątkowe, szczególnie w aplikacjach webowych są trudne w utrzymaniu.

S2: Użycie niewłaściwego poziomu izolacji w aplikacji wielowątkowej może wpłynąć na spójność danych.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Całkowite zabezpieczenie przed nieautoryzowanym odczytem haseł. | | | |
| Atrybuty | Bezpieczeństwo – poufność danych | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Logowanie się w systemie | | | |
| Odpowiedź | Mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Autoryzacja i uwierzytelnianie realizowane przez mechanizmy MS SQL i .NET URLAuthorization |  |  |  | NR2 |
| Algorytm SHA-2 |  | T1 |  |  |

NR2: Korzystanie z istniejących i sprawdzonych rozwiązań w zakresie bezpieczeństwa jest rekomendowane przez OWASP(Open Web Application Security Project).

T1: Algorytm zmniejsza szanse nieautoryzowanego odczytu haseł kosztem wydajności systemu.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Wykonywanie płatności w 100% gwarantuje bezpieczeństwo przed nieautoryzowanym odczytem danych transakcji bankowej. | | | |
| Atrybuty | Bezpieczeństwo – poufność danych | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Płatność za imprezę turystyczną. | | | |
| Odpowiedź | Mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Zewnętrzna usługa płatności |  |  |  | NR3 |
| HTTPS |  |  |  | NR4 |

NR3: Przekazanie odpowiedzialności za kluczowe dane(numery i hasła do kont bankowych) ludziom, którzy mają w tym temacie dużo większe doświadczenie.

NR4: Uniemożliwienie podsłuchiwania w sieciach lokalnych, dzięki HTTPS.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Operacje wymagające kontroli dostępu zawsze będą wymagały wcześniejszego uwierzytelniania(jedno uwierzytelnienia dla wielu operacji).(H,M) | | | |
| Atrybuty | Bezpieczeństwo – integralność danych | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Wykonywanie operacji wymagających uprawnień | | | |
| Odpowiedź | Mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Autoryzacja i uwierzytelnianie realizowane przez mechanizmy MS SQL i .NET URLAuthorization |  |  |  | NR5 |
| Uprawnienia i konto w relacji 1 do 1 |  |  | R2 |  |

NR5: Wykorzystanie sprawdzonych zewnętrznych mechanizmów uwierzytelniania i autoryzacji.

R2: Konieczność definiowania osobnych uprawnień dla każdego konta.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | 100% danych w bazie danych jest zgodna z rzeczywistością (H, L) | | | |
| Atrybuty | Bezpieczeństwo – spójność danych | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Rezerwacja imprezy turystycznej | | | |
| Odpowiedź | Mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Jedna baza danych |  | T2 |  |  |

T2: Dzięki jednej bazie danych, łatwiej jest utrzymać spójność danych, dzieję się to jednak kosztem wydajności i skalowalności.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Dodanie nowej relacji w bazie danych, wraz z operacjami CRUD w aplikacji w mniej niż 2 osoby w tydzień.(M,H) | | | |
| Atrybuty | Modyfikowalność – nowe produkty | | | |
| Środowisko | Deweloperskie | | | |
| Bodziec | Dodanie nowe funkcjonalności | | | |
| Odpowiedź | Dwie osoby w tydzień | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Wzorzec MVC |  |  |  | NR6 |
| Relacyjna baza danych MS SQL oraz MS SQL  Entity Framework |  |  |  | NR7 |

NR6: Zastosowanie wzorca rozdziela aplikację co ułatwia wprowadzanie zmian.

NR7: Zastosowanie gotowych rozwiązań i generatorów przyśpiesza wprowadzanie zmian.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenariusz | Dostępność do serwisu o dowolnym czasie na poziomie 99% w roku(H, H) | | | |
| Atrybuty | Dostępność – czasowa | | | |
| Środowisko | Standardowa praca systemu | | | |
| Bodziec | Dokonanie rezerwacji użytkownika | | | |
| Odpowiedź | Dla 1000 użytkowników jednocześnie mniejsza niż 5s. | | | |
| Decyzje arch. | Wrażliwość | Kompromis | Ryzyko | Bez ryzyka |
| Aplikacja hostowana w chmurze | S3 |  |  | NR8 |

NR8: Deklarowana wysoka dostępność rozwiązań zlokalizowanych w chmurze.

S3: Możliwość uzależnienia się od rozwiązań jednego dostawcy (brak alternatywy w razie awarii).

**Spis**

NR1: Zostawienie konieczności dbania o infrastrukturę specjalistom.

NR2: Korzystanie z istniejących i sprawdzonych rozwiązań w zakresie bezpieczeństwa jest rekomendowane przez OWASP(Open Web Application Security Project).

NR3: Przekazanie odpowiedzialności za kluczowe dane(numery i hasła do kont bankowych) ludziom, którzy mają w tym temacie dużo większe doświadczenie.

NR4: Uniemożliwienie podsłuchiwania w sieciach lokalnych, dzięki HTTPS.

NR5: Wykorzystanie sprawdzonych zewnętrznych mechanizmów uwierzytelniania i autoryzacji.

NR6: Zastosowanie wzorca rozdziela aplikację co ułatwia wprowadzanie zmian.

NR7: Zastosowanie gotowych rozwiązań i generatorów przyśpiesza wprowadzanie zmian.

NR8: Deklarowana wysoka dostępność rozwiązań zlokalizowanych w chmurze.

R1: Mechanizmy wielowątkowe, szczególnie w aplikacjach webowych są trudne w utrzymaniu.

R2: Konieczność definiowania osobnych uprawnień dla każdego konta.

S1: Możliwość uzależnienia się od rozwiązań jednego dostawcy(utrudnione przeniesienie aplikacji).

S2: Użycie niewłaściwego poziomu izolacji w aplikacji wielowątkowej może wpłynąć na spójność danych.

S3: Możliwość uzależnienia się od rozwiązań jednego dostawcy (brak alternatywy w razie awarii).

T1: Algorytm zmniejsza szanse nieautoryzowanego odczytu haseł kosztem wydajności systemu.