System teleinformatyczny dla firmy kurierskiej

Patryk Kaniewski Jakub Kijo

Table of Contents

1. Analiza Wymagań
    1.1. Opis firmy
    1.2. Opis problemu
    1.3. Propozycja projektu
        1.3.1. Propozycja sprzętu
        1.3.2. Proponowane rozwiązanie
        1.3.3. Diagramy
2. Analiza Ryzyka
    2.1. Zagrożenia systemu
    2.2. Zagrożenia aplikacji
        2.2.1. App4
        2.2.2. App3
        2.2.3. App2
        2.2.4. App1
    2.3. Ryzyko
        2.3.1. Kryteria dla wskaźnika Z
        2.3.2. Kryteria dla wskaźnika R
        2.3.3. Kryteria dla wskaźnika W
        2.3.4. Kryterium WPR
3. Polityki bezpieczenstwa
    3.1. Definicje bezpieczenstwa
    3.2. Zabezpieczenie stacji roboczych
    3.3. Bezpieczeństwo danych
    3.4. Polityka Haseł
    3.5. Edukacja pracowników w zakresie bezpieczeństwa
    3.6. Transport danych poufnych

1. Analiza Wymagań

1.1. Opis firmy

Firma kurierska z przesyłkami na cały kraj, posiada kilka sortowni w różnych częściach kraju, oraz bardzo wielu kurierów odpowiedzialnych za transportowanie paczek między nimi, oraz bezpośrednio do odbiorców. Posiada też bazę klientów (inne firmy), którzy używają API aby tworzyć i nadawać przesyłki do indywidualnych odbiorców. Odbiorca zamówienia otrzymuję powiadomienia o stanie paczki.

1.2. Opis problemu

Kurier potrzebuję urządzenia z aplikacją umożliwiającą skanowanie paczek, które wchodzą do sortowni, wychodzą z niej. Otrzymuję od klientów lub dostarcza odbiorcą. Musi też mieć dostęp do danych adresowych klientów oraz odbiorców. Kurier nie pobiera pieniędzy od odbiorcy ze względu na to że firma kurierska nie obsługuje płatności przy odbiorze paczki. Owe urządzenie musi też mieć możliwość zabezpieczenia w przypadku kradzieży, np za pomocą hasła, by poufne dane nie dostały się w niepowołane ręce.

Każda sortownia powinna posiadać redundantne serwery, które będą odpowiedzialny z przydzielanie paczek kurierom, oraz posiadać listę paczek która aktualnie jest na sortowni.

Odbiorca powinien posiadać możliwość śledzenia przesyłki na podstawie jej numeru poprzez aplikację na urządzenie mobilne.

Klient powinien móc poprzez API zarejestrować paczkę oraz wygenerować dla niej etykietę. Najbliższa sortownia przydzieli również kuriera który w najbliższym czasie odbierze paczkę od zleceniodawcy

1.3. Propozycja projektu

Na podstawie tych informacji klarują nam się 4 aplikację:

1. Aplikację dla odbiorcy umożliwiającą śledzenie przesyłki.
2. Aplikacja dla kuriera, umożliwiająca skanowanie zarejestrowanych paczek oraz komunikująca się z sortownią która zmienia stan paczki.
3. Aplikacja dla sortowni, która odpowiada za całą logikę naszego systemu, przydziela paczki kurierom oraz wysyła jest do innych sortowni. Posiada również historię realizacja przesyłek.
4. API dla klienta, umożliwiającą generowanie etykiet oraz śledzenie przesyłki

   Dalej zwane:

   - App1
   - App2
   - App3
   - App4

Koszt (sprzętowy) rozwiązania jest wprost proporcjonalny do ilości kurierów i sortowni

1.3.1. Propozycja sprzętu

1. Serwer

   Serwer DELL PowerEdge R6515 Rack Server

Element	**Ilośc**	**Specyfikacja**
CPU	1	AMD EPYC 7313P
RAM	4	8GB RDIMM 3200MT
SSD	4	480GB SATA 2.5in Hot-plug
PSU	2	Hot-plug 550W
NIC	2	Broadcom 5720 1GbE LOM Mezz Card
OS	1	Red Hat Enterprise Linux 8.4 x64
	Koszt	14263 PLN

2. Stacja robocza

   ThinkCentre M90q Gen 2 Tiny

Element	**Ilośc**	**Specyfikacja**
CPU	1	Intel i7-11700T
RAM		16 GB DDR4 3200MT
SSD	1	512 GB SSD gen4
OS		Fedora 35 Workstation
	Koszt	3500 PLN

3. Urządzenie kuriera

   Smartphone Samsung Galaxy A32

   Koszt 1200 PLN

1.3.2. Proponowane rozwiązanie

Proponowane rozwiązanie będzie składać sie głownie z 3 elementów

1. Sortownia

    - podwójnie redundantne połaczenie do sieci (dwóch dostawców usług internetowych)
    2. pracownik sortowni

       Wydaje oraz przyjmuje paczki od kurierów, wymagane połaczenie do serwera jak i serwera do centrali

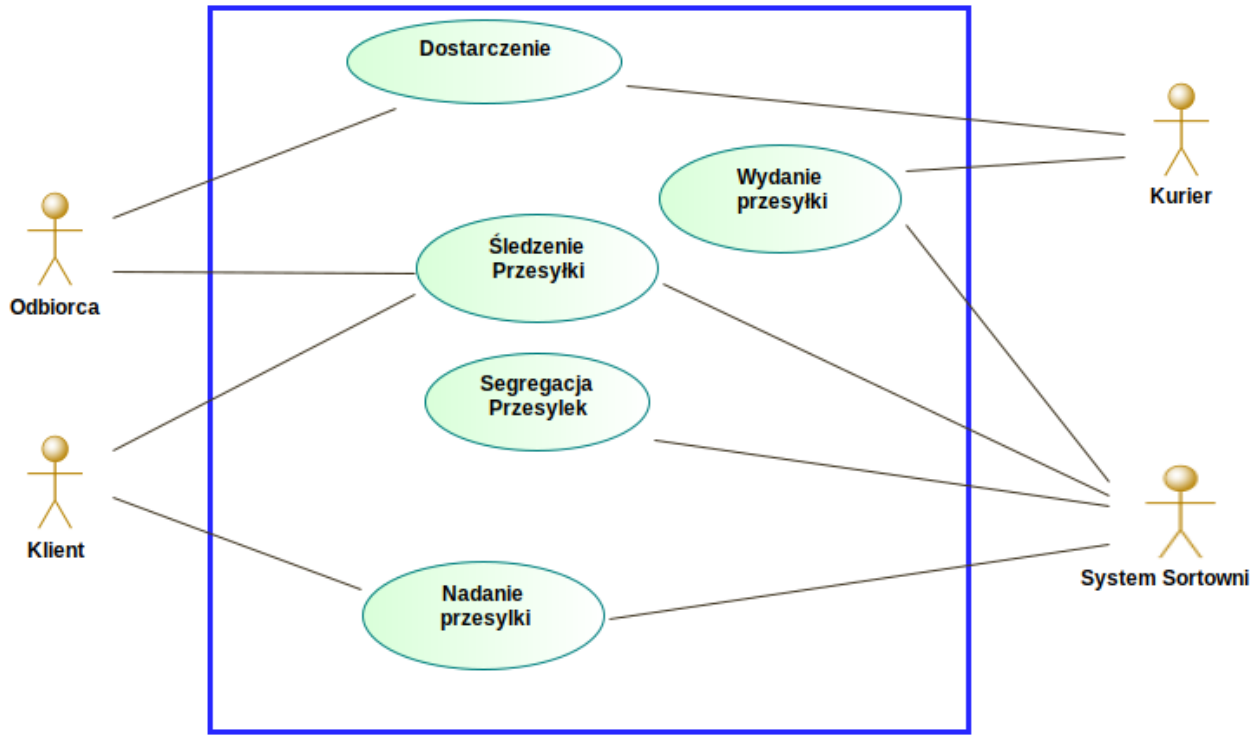
        - stacja robocza
    3. serwer1
    4. serwer2 (mirror)
2. Centrala
    1. serwer1
    2. serwer2 (mirror)
3. Kurier
    - podwójnie redundantne połaczenie do sieci (dwóch dostawców usług GSM)
    2. kurier

       Transportuje paczki pomiędzy sortowniami oraz do klienta i do odbiorcy, wymaganie połaczenie

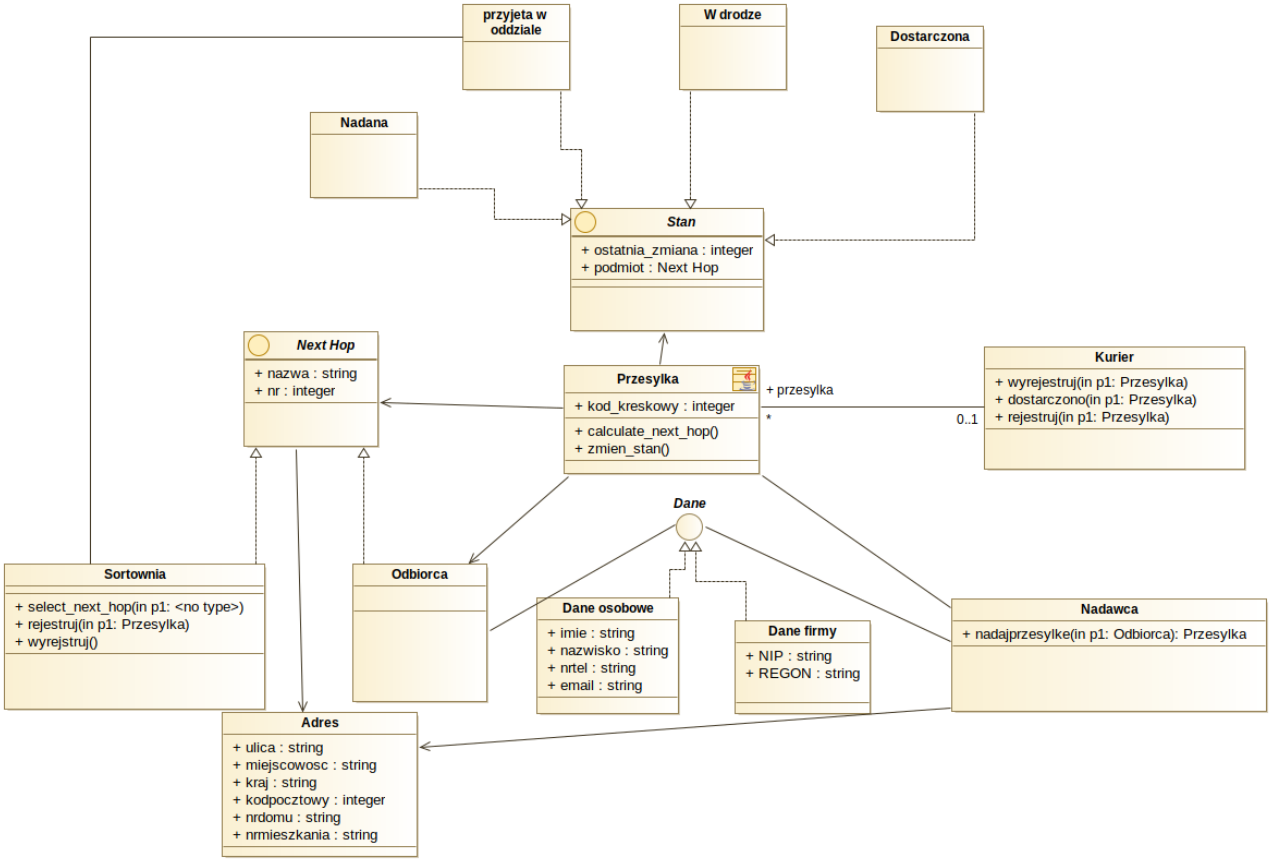
        - smartphone

1.3.3. Diagramy

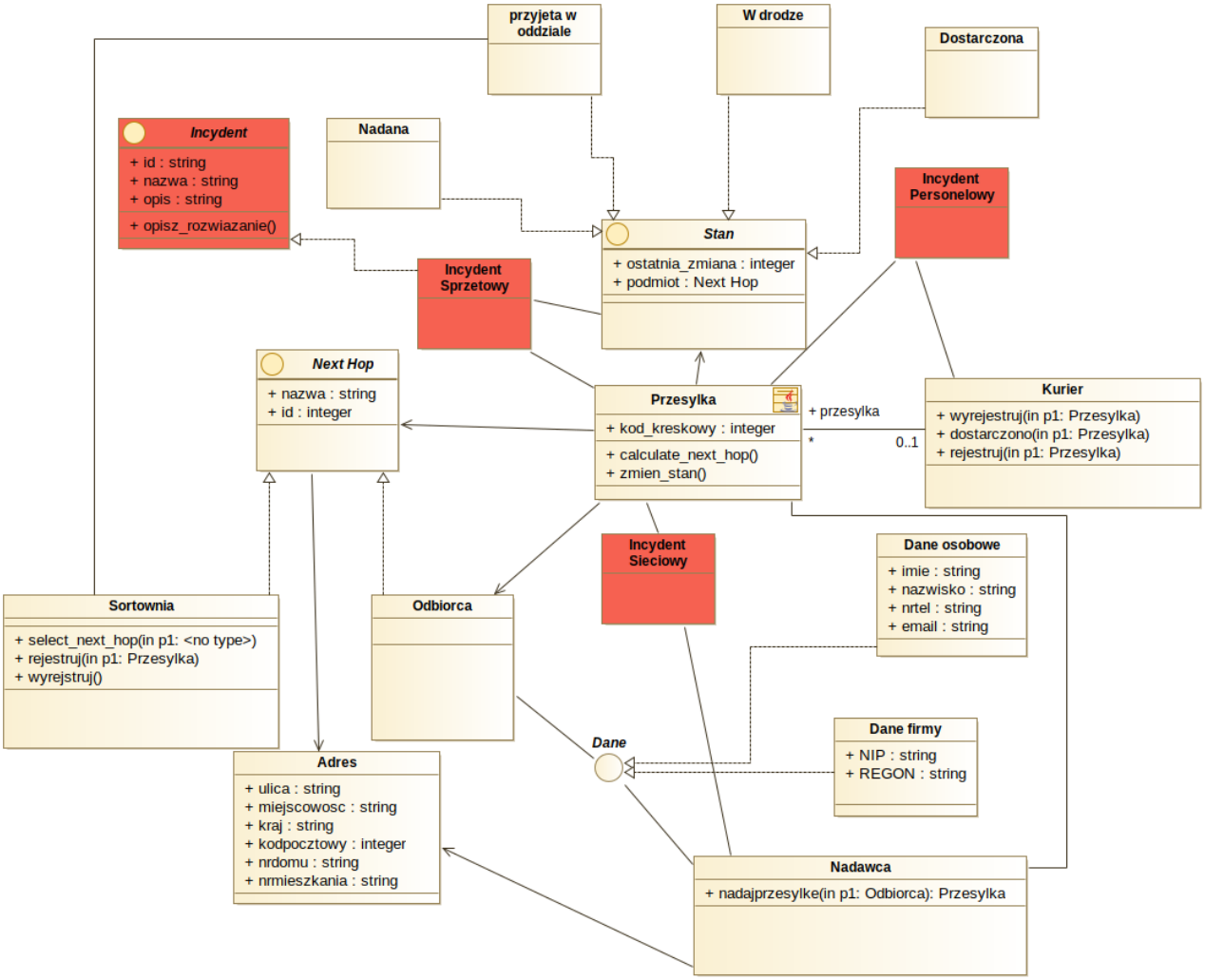
1. Diagram przypadków użycia



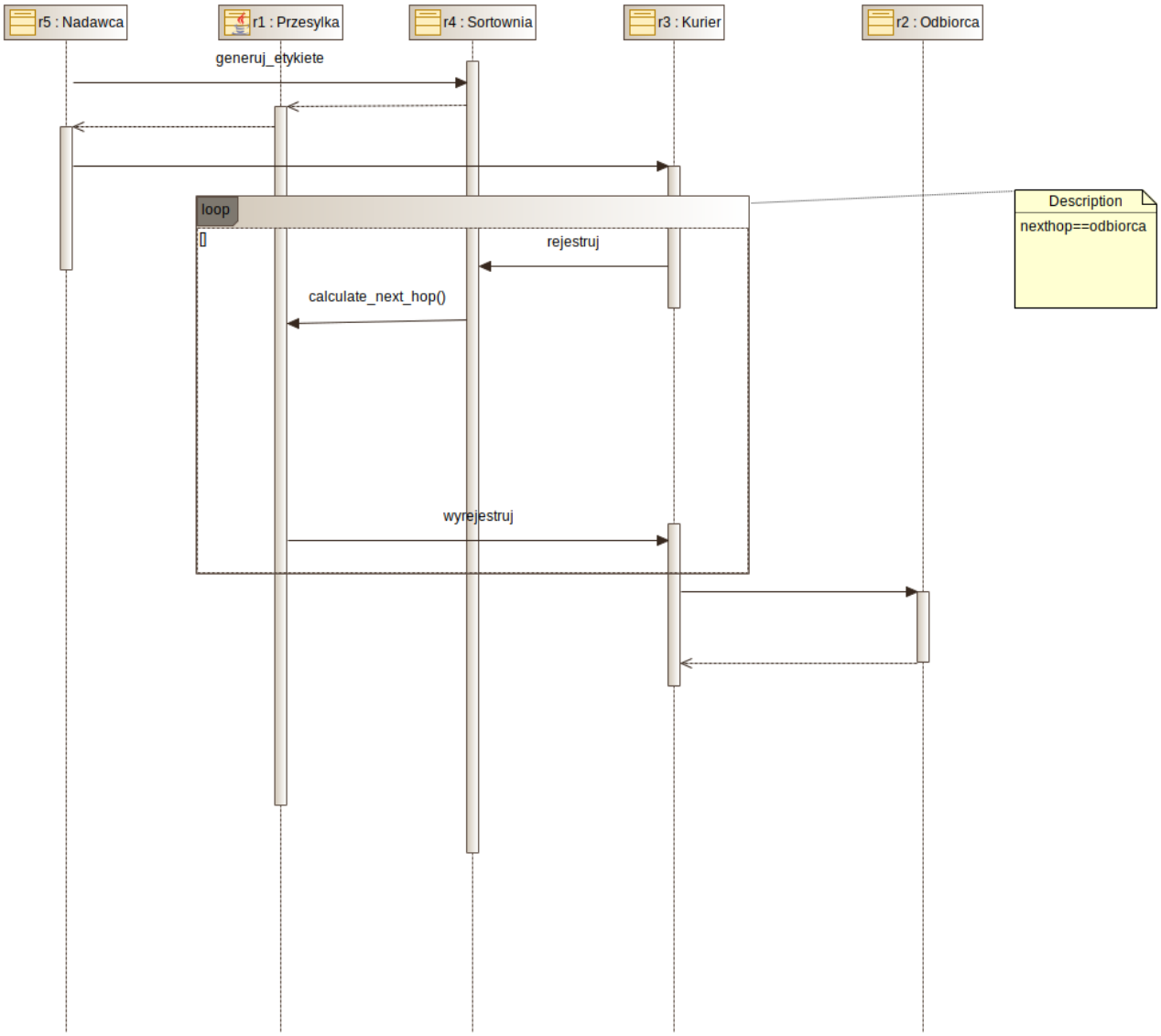
2. Diagram klas App3



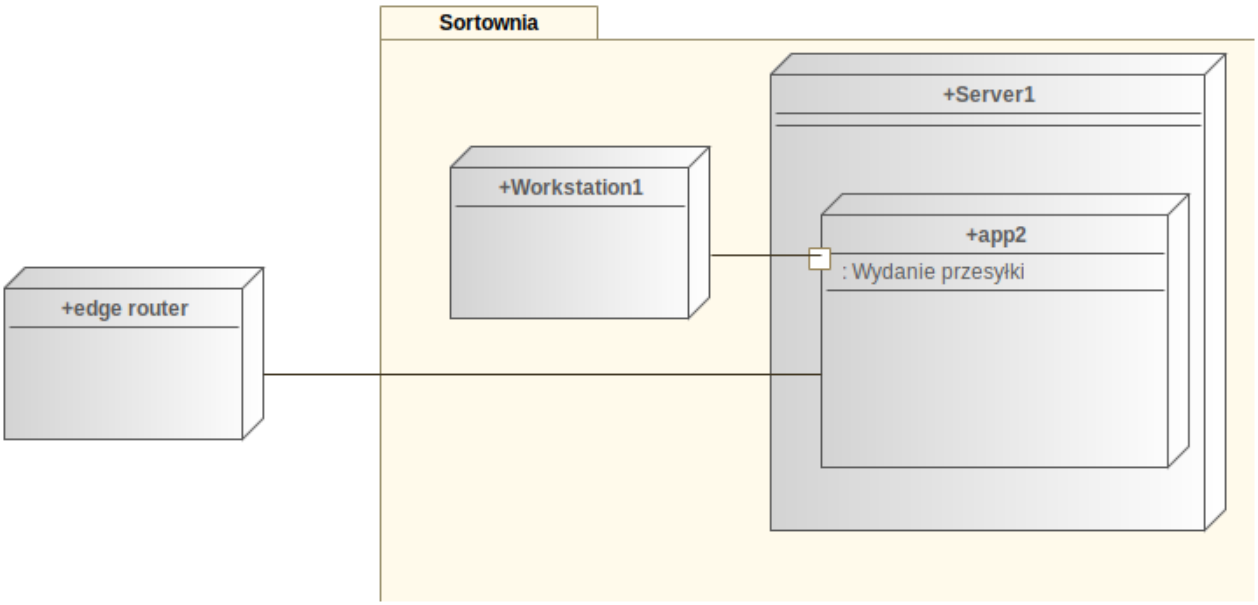
3. Diagram klas App3 z wyszczególnionymi typami zagrożeń



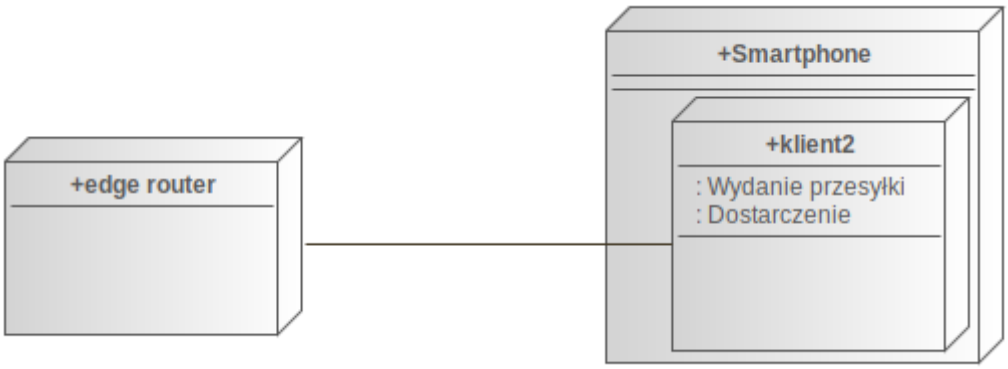
4. Diagram Sekwencji



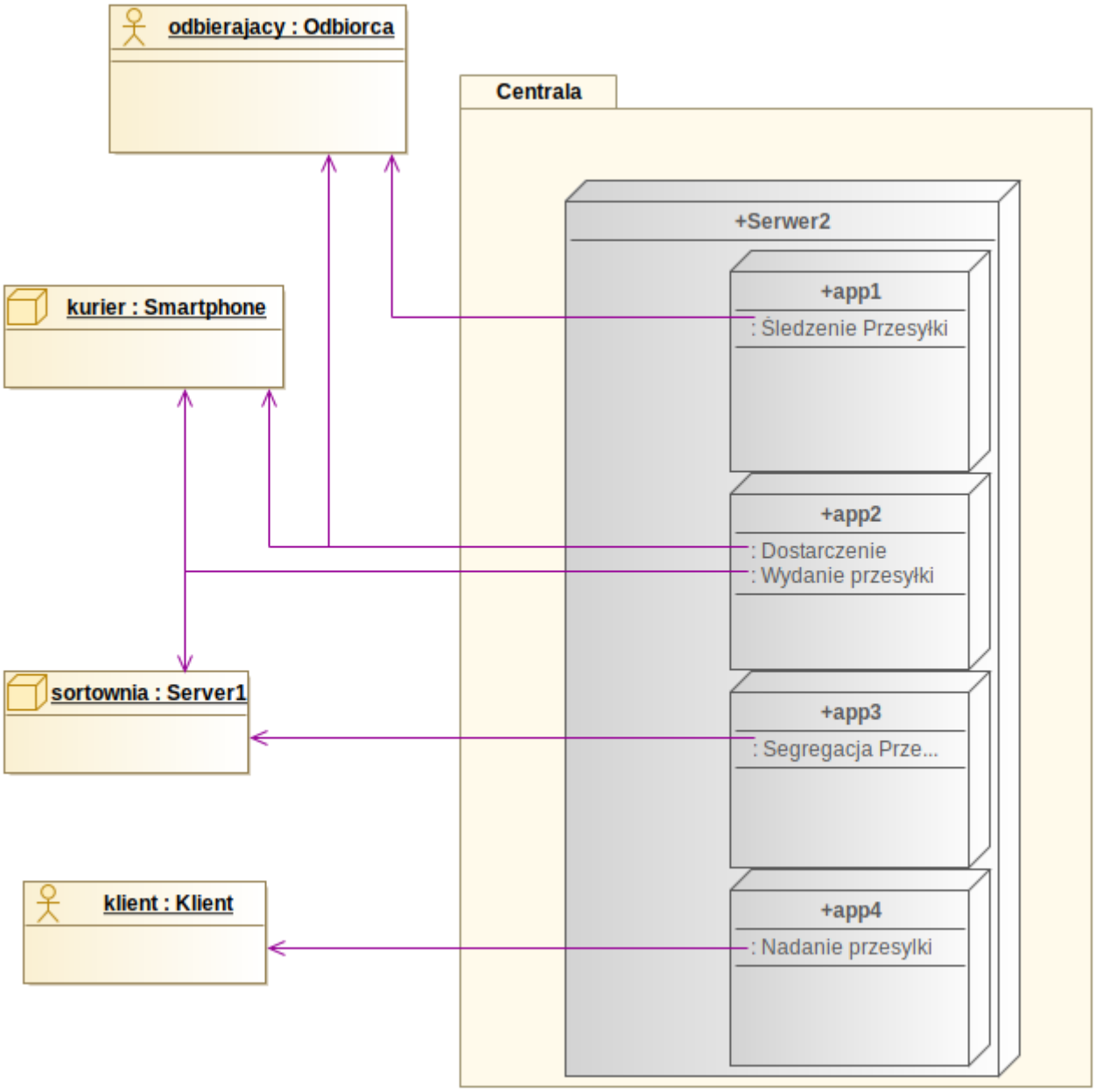
5. Diagram wdrożenia
    1. Sortownia



2. Kurier



3. Centrala



2. Analiza Ryzyka

2.1. Zagrożenia systemu

Brak prądu Kradzież Wandalizm Błąd w eksploatacji pożar Brak dostępu do sieci Siły natury

2.2. Zagrożenia aplikacji

Brak dostępu do usługi Nieprawidłowe działanie Luki bezpieczeństwa

2.2.1. App4

- Brak dostępu do usługobiorcy

- Nieprawidłowe dane
- Nieupoważniony dostęp do API
- Problemy z płatnościami

2.2.2. App3

- Kradzież paczek
- Wyciek danych o paczkach
- Wyciek danych o odbierających

2.2.3. App2

- Kradzież paczek
- Wyciek danych o paczkach
- Wyciek danych o odbierających

2.2.4. App1

- Brak dostępu do usługi
- Przechwycenie paczki

2.3. Ryzyko

Do analizy ryzyka użyto metody FMEA zgodnej ze standardem ISO 27001:2013 Ryzyko oceniamy wg. Wzoru WPR=ZxRxW gdzie:

Z - znaczenie zdarzenia R- szansa wykorzystania podatności lub prawdopodobieństwo zdarzenia W- szansa wykrycia zdarzenia

Wszystkie współczynniki określamy w pięciostopniowej skali:

Kryteria dla wskaźnika Z

OCENA	Określenie znaczenia
1	Zdarzenie nie wpływa na funkcjonowanie przedsiębiorstwa
2	Nieznaczne utrudniena dla bezpieczeństwa i brak znaczenia dla funkcjonowanie przedsiębiorstwa
3	Małe utrudnienia dla bezpieczeństwa i przedsiębiorstwa
4	Znaczne utrudnienia dla bezpieczeństwa i funkcjonowania przedsiębiorstwa
5	Niemożliwość funkcjonowanie przedsiębiorstwa

Kryteria dla wskaźnika R

OCENA	Szansa wystąpienia (w procentach na 30 dni)
1	znikome (<1%)
2	rzadkie (1% - 10 %)
3	średnie (10% - 40 %)
4	prawdopodobne (40% - 70%)
5	pewne (70%-100%)

Kryteria dla wskaźnika W

OCENA	Możliwość wykrycia
1	pewne
2	łatwe
3	średnie
4	trudne
5	prawie niemożliwe

Punkty	Kryterium WPR
<10	Nie wymaga reakcji
<15	Obserwacja
<50	Wymaga modyfikacji sposobu działania
<75	Wymaga zmiany sposobu postępowania
>75	Wyłączenie procesu lub zmiany globalne

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Brak prądu	Brak dostępu do sprzętu, brak możliwości pracy	Czynnik zewnętrzny lub wewnętrzny (np Pogoda lub zaniedbanie)	Posiadanie własnych generatorów, albo baterii na wypadek braku prądu.	4	2	1	8	Nie wymaga akcji
Kradzież	Brak dostępu do sprzętu, brak możliwości pracy	Czynnik zewnętrzny (np. osoba niepowołana)	Ograniczenie dostępu osobom niepowołanym, zainstalowanie systemu przeciw włamaniom.	2	2	1	4	Nie wymaga akcji
Wandalizm	Zniszczenie sprzętu, brak możliwości pracy	Czynnik zewnętrzny (np. osoba niepowołana)	Ograniczenie dostępu osobom niepowołanym, zainstalowanie systemu przeciw włamaniom.	2	2	2	8	Nie wymaga akcji
Błąd w eksploatacji	Zniszczenie sprzętu, brak możliwości pracy	Czynnik wewnętrzny (np. zaniedbanie)	Szkolenie, poprawnej eksploatacji sprzętu	1	3	4	12	Obserwacja
pożar	Zniszczenie sprzętu, brak możliwości pracy	Czynnik zewnętrzny lub wewnętrzny (np Pogoda lub zaniedbanie)	Dostosowanie się do norm Ppoż i instalacja takowych systemów.	4	1	1	4	Nie wymaga akcji
Brak dostępu do sieci	Brak możliwości komunikacji, brak możliwości pracy	Czynnik zewnętrzny (np Pogoda)	Posiadanie wielu źródeł dostępu do sieci	4	2	1	8	Nie wymaga akcji
Siły natury	Zniszczenie sprzętu, brak możliwości pracy	Czynnik zewnętrzny (np Pogoda)	W zależności od zagrożenia, wprowadzenie odpowiedniego systemu lub zasad postępowania.	4	1	1	4	Nie wymaga akcji

Ryzyka Aplikacji

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Brak dostępu do usługi	Brak dostępu do sprzętu, brak możliwości pracy	Atak DDos, atak mallware, atack hakerski	Nowoczesny Firewall i wdrożenie zasad polityki bezpieczeństwa	4	2	1	8	Nie wymaga akcji
Nieprawidłowe działanie	Utrudniony dostęp do sprzętu.	Czynnik zewnętrzny i wewnętrzny, zaniedbanie lub osoba błąd firmy dostarczającej oprogramowanie	Testowanie oprogramowania, oraz utworzenie programu szkoleń	3	2	2	12	Obserwacja
Luki bezpieczeństwa	Wypłynięcie danych osobowych, utrudniony dostęp do sprzętu	Czynnik zewnętrzny (np. luki w systemie zabezpieczeń)	Wdrożenie zasad polityki bezpieczeństwa, nowoczesnu Firewall.	4	2	4	32	Wymaga modyfikacji sposobu działania

Ryzyka App 4

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Brak dostępu do usługobiorcy	Usługobiorca nie może nadawać przesyłek	Problem po stronie usługobiorcy, atak na nasze serwery	Firewall, wdrożenie polityki bezpieczeństwa	4	3	1	12	Obserwacja
Nieprawidłowe dane	Kurier może mieć problem z odnalezieniem usługobiorcy	Usługobiorca podał nieprawidłowe dane	Weryfikacja danych podawanych przez usługobiorcę	2	2	2	8	Nie wymaga akcji
Nieupoważnion y dostęp do API	Dostęp do poufnych danych	Niedopatrzenie usługiobiorcy	Zabezpieczenie API hasłem	2	1	5	10	Obserwacja
Problemy z płatnościami	Brak możliwości składania nowych zamówień	Problemy z systemem płatności (Obsługuję go firma zewnętrzna)	Posiadanie wielu systemów płatności	4	1	1	4	Nie wymagania akcji

Ryzyka App 3

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Kradzież paczek	Koszty pieniężne dla firmy	Osoba niepowołana lub pracownik	System antywłamaniowy, kontrola pracowników	2	3	1	6	Nie wymaga akcji
Wyciek danych o paczkach	Koszty pieniężne i zaufania dla firmy	Atak sieciowy, luki w zabezpieczeniach	Firewall, Wdrożenie polityki bezpieczeństwa	3	1	4	12	Obserwacja
Wyciek danych o odbierających	Koszty pieniężne i zaufania dla firmy	Atak sieciowy, luki w zabezpieczeniach	Firewall, Wdrożenie polityki bezpieczeństwa	2	1	4	8	Nie wymaga akcji

Ryzyka App 2

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Kradzież paczek	Koszty pieniężne i zaufania dla firmy	Osoba niepowołana lub pracownik	System do kontroli pracowników, system zabezpieczający urządzenie	2	3	2	12	Obserwacja
Wyciek danych o paczkach	Koszty pieniężne i zaufania dla firmy	Osoba niepowołana lub pracownik	system zabezpieczający urządzenie	3	2	2	12	Obserwacja
Wyciek danych o odbierających	Koszty pieniężne i zaufania dla firmy	Osoba niepowołana lub pracownik	system zabezpieczający urządzenie	2	2	2	12	Obserwacja

Ryzyka App 1

Zdarzenie	Skutki zdarzenia	Przyczyny zdarzenia	Działania zapobiegawcze	Z	R	W	WPR	Opis
Brak dostępu do usługi	Brak większych skutków zdarzenia	Błąd programistyczny	Kontrolę działania systemu	1	2	1	2	Nie wymaga akcji
Przechwycenie paczki	Koszty pieniężne i zaufania dla firmy	Osoba niepowołana, która włamała się na konto	Zabezpieczenie konta	2	1	4	8	Nie wymaga akcji

3. Polityki bezpieczenstwa

3.1. Definicje bezpieczenstwa

1. Poufność - uniemożliwienie dostępu do danych osobom do tego szczególnie nie uprawnionym
2. Integralność - zapewnienie nienaruszalności danych przez osoby do tego nieuprawnione
3. Uwierzytalnianie
    1. Identyfikacja - deklaracja tożsamości
    2. Uwierzytalnie - weryfikacja podanej tożsamości
    3. Autoryzacja - nadanie danej tożsamości uprawnień do manipulacji i/lub odczytu danych
4. Dostępność - zapewnienie prostego i solidnego dostępu do danych
5. Anonimizacja

3.2. Zabezpieczenie stacji roboczych

1. Wymaganie wygaszania sesji po nieaktywnosci 15 minut
2. Aktualne oprogramowanie specjalistyczne i systemowe
3. Zabezpieczony dostep do stacji roboczych.
    1. Weryfikacja pierwszego etapu - Hasło
    2. Weryfikacja drugiego etapu - Klucz
4. Szyfrowanie całych woluminów

3.3. Bezpieczeństwo danych

1. Wszystkie dane muszą być przechowywane w 3 kopiach
    1. Redundacja - na systemie przechowującym dane musi być wykorzystane powielanie danych
    2. Backup - wykonywanie dziennych przyrostowych kopiach zapasowych i miesięcznych

kopiach pelnych.

3. Offsite backup - wykonanie tygodniowych kopii zapasowych do innej placówki

3.4. Polityka Haseł

1. Zmiana haseł co 2 miesiące
2. Haslo musi zawierac albo:
    1. przynajmniej 30 znaków
    2. przynajmniej 16 znaków i przynajmniej jedna litere, cyfra i znak specjalny

3.5. Edukacja pracowników w zakresie bezpieczeństwa

Okresowe szkolenia ws. bezpieczenstwa informacji

1. Szkolenie panelowe - zabezpieczenie stanowiska
2. Szkolenie panelowe - swiadomosc problemow bezpieczenstwa
3. Losowe symulowanie szkolenie z inżynierii socjalnej

3.6. Transport danych poufnych

1. Zabrania sie kopiowania, przenoszenia danych firmowych nie oznaczonych do publikacji zewnętrznej na żadne nośniki danych
2. Wymagany transport danych na nosnikach zewnętrznych wymaga szyfrowania danych za pomocą klucza publicznego podmiotu ubiegającego się o transport