Analiza ryzyka bezpieczeństwa informacji – system obsługi klientów indywidualnych

Opracowanie zgodne z metodyką podmiotów publicznych

Dominik Rolek

20.12.2024 r.

1. Wprowadzenie

Niniejszy dokument przedstawia identyfikację zagrożeń oraz plan analizy ryzyka bezpieczeństwa informacji dla systemu obsługi klientów indywidualnych firmy Krzak. Dokument zawiera również przykładowe obliczenie ryzyka końcowego (Rk) dla scenariusza, który w wyniku analizy uzyskał najwyższy poziom ryzyka pierwotnego (Rp).

Przedmiotem analizy jest system obejmujący następujące elementy i funkcje:

1. Interfejs self-care: portal dostępny dla klienta końcowego, zarówno na
    a. urządzeniu stacjonarnym – przeglądarka internetowa w komputerze stacjonarnym lub laptopie
    b. urządzeniu mobilnym – telefon i aplikacja mobilna
2. Interfejs customercare: portal dostępny dla pracowników biurowych, dostępny z sieci wewnętrznej z komputerów stacjonarnych.
3. Interfejs POS (point of sales): portal dostępny dla pracowników w rozsianych po całym kraju punktach sprzedaży (salony Krzak). Punkty te są podłączone tylko do Internetu, nie mają połączenia z siecią wewnętrzną.
4. Możliwość przechowywania dokumentów klientów związanych z usługami. Dokumenty zawierają dane bilingowe oraz dane osobowe.
5. Możliwość pobierania faktur przez wszystkie interfejsy.
6. Możliwość pobierania rachunków szczegółowych użycia usługi, m.in. połączeń telefonicznych, SMS, etc. przez wszystkie interfejsy.
7. Możliwość automatycznego wysyłania e-mail do klientów.

Analiza ryzyka została zaplanowana zgodnie z metodyka zarządzania ryzykiem dla podmiotów rządowych, opartą o podejście PN-ISO/IEC 27005, z uwzględnieniem oceny wpływu na poufność, integralność i dostępność danych.

2. Identyfikacja aktywów

2.1 Cel

Celem niniejszego rozdziału jest identyfikacja aktywów wchodzących w zakres analizowanego systemu obsługi klientów indywidualnych. Identyfikacja aktywów stanowi podstawę do dalszych etapów związanych z identyfikacją zagrożeń i przeprowadzania analizy i oceny ryzyka.

Aktywa obejmują:

- Aktywo nadrzędne – system jako całość
- Aktywa informacyjne – informacje, dane, dokumenty
- Aktywa techniczne – komponenty, interfejsy, funkcjonalności
- Aktywa organizacyjne – role, procesy, polityki, SZBI

2.2 Wykaz aktywów

Kategoria aktywa	Identyfikator	Nazwa aktywa	Opis	Obszary użycia	C/I/A(P/I/D)
Aktywo nadrzedne	A-0	System obsługi klientów indywidualnych	System obejmujący kanały self-care, customercare, POS oraz usługi wspólne (API, dane, e-mail)	Wszystkie	**P/I/D**
Aktywo informacyjne	A-1	Dane osobowe klientów	Dane identyfikacyjne, kontaktowe, umowne	Wszystkie	**P**/**I**/D
Aktywo informacyjne	A-2	Dane billingowe / rachunki	Dane o połączeniach, SMS, zużyciu usług	Wszystkie	**P**/**I**/D
Aktywo informacyjne	A-3	Faktury	Dokumenty rozliczeniowe	Wszystkie	**P**/**I**/D
Aktywo informacyjne	A-4	Repozytorium danych klientów	Dokumenty związane z usługami (np. załączynki/skany)	Wszystkie	**P**/**I**/D
Aktywo informacyjne	A-5	Repozytorium danych pracowników	Dokumenty związane z uprawnieniami i identyfikatorami pracowników.	Wszystkie	**P**/**I**/D
Aktywo techniczne	A-6	Portal self-care (WWW)	Warstwa prezentacji dla klientów w przeglądarce + mechanizmy sesji/tokenów	Internet	P/I/**D**
Aktywo techniczne	A-7	Aplikacja mobilna self-care	Warstwa prezentacji dla klientów mobilnych + mechanizmy sesji/tokenów	Internet/mobile	P/I/**D**
Aktywo techniczne	A-8	Portal customercare	Aplikacja dla pracowników biurowych	LAN	**P/I/D**
Aktywo techniczne	A-9	Portal POS	Aplikacja dla pracowników salonów	Internet	**P/I/D**

Aktywo techniczne	A-10	Backend/API	Usługi aplikacyjne obsługujące logikę biznesową	Wszystkie	**P/I/D**
Aktywo techniczne	A-11	Repozytorium dokumentów	Składowanie dokumentów, uprawnień + metadanych	Backend	**P/I/D**
Aktywo techniczne	A-12	Baza danych systemu	Dane transakcje, referencyjne	Backend	**P/I/D**
Aktywo techniczne	A-13	Kopie zapasowe/ archiwum	Backupy danych i dokumentów	Utrzymanie	P/**I/D**
Aktywo techniczne	A-14	Usługa wysyłki email	SMTP/API, szablony i kolejki wysyłek	Wszystkie	**P/I/D**
Aktywo organizacyjne	A-16	Role stron zainteresowanych	Klient/customercare/POS/administrator/ ...	Wszystkie	**P/I**/D
Aktywo organizacyjne	A-17	Procesy biznesowe	Logowanie, pobieranie faktur, billingów, obsługa informacji	Wszystkie	P/**I/D**
Aktywo organizacyjne	A-18	Zarządzanie danymi	Zasady klasyfikacji danych, minimalizacji, retencji/usuwania oraz udostępniania danych i dokumentów	Wszystkie	**P/I/D**
Aktywo organizacyjne	A-19	Zarządzanie kontami uprzywilejowanymi	Zasady użycia kont administracyjnych, separacja uprawnień, kontrola i rejestrowanie działań uprzywilejowanych	Backend, administracja	**P/I/D**

Legenda:

- Kategoria aktywa – typ aktywa
- Identyfikator – unikalny kod aktywa wykorzystywany do jednoznacznego odwołania się do aktywa w kolejnych rozdziałach
- Nazwa aktywa - Skrócony opis aktywa
- Opis - zwięzły opis zakresu aktywa (co obejmuje, czego dotyczy)
- Obszar użycia - obszar/strefa wykorzystania aktywa w architekturze i modelu dostępu. Wskazujący m. in. Ekspozycję na zagrożenia oraz kontekst użytkowników.
    - Wszystkie – aktywo jest współdzielone lub wykorzystywane przez wszystkie kanały/interfejsy systemu.
    - Internet – aktywo jest dostępne lub wykorzystywane w strefie narażonej na zagrożenia z sieci Internet (np. portal www). Oznacza zwiększoną ekspozycję na zagrożenia zewnętrzne.
    - LAN – aktywo jest dostępne w sieci wewnętrznej organizacji. Oznacza zwiększoną ekspozycję na zagrożenia wewnętrzne.

    - Backend – aktywo znajduje się w warstwie usług wspólnych/przetwarzania danych. Krytyczne dla działania wszystkich kanałów
    - Utrzymanie – aktywo wykorzystywane jest głownie w procesach administracji i utrzymania
- C/I/A(P/I/D) - Atrybuty bezpieczeństwa odpowiadające Podatności, Integralności i Dostępności

3. Identyfikacja i lista zagrożeń dla bezpieczeństwa informacji

3.1 Cel

Celem niniejszego rozdziału jest identyfikacja i wylistowanie zagrożeń dla bezpieczeństwa informacji w zakresie aktyw zidentyfikowanych w Rozdziale 2.

3.2 Bazowy katalog zagrożeń (wg metodyki - załącznik)

Poniższy katalog kategorii zagrożeń stanowi bazową listę referencyjną wykorzystywaną jako checklista w procesie identyfikacji zagrożeń dla analizowanego systemu. Katalog ten nie jest jeszcze wykazem ryzyk w rozumieniu analizy ryzyka – jego rolą jest zapewnienie, że podczas identyfikacji nie pominięto typowych klas zdarzeń zagrażających bezpieczeństwu informacji.

Identyfikator	Kategoria zagrożenia (wg metodyki)	Przykładowe podatności (wg metodyki)	Typowa strefa / kanał w naszym systemie
K-1	Wniknięcie kodu złośliwego z sieci WAN	brak/nieaktualne AV,zła konfiguracja firewall/IDS/IPS, podatność na socjotechnikę, brak monitoringu obciążenia	Internet (self-care WWW, POS, mobile), styki perymetryczne
K-2	Wprowadzenie kodu złośliwego z sieci LAN	brak/nieaktualne AV, zła konfiguracja firewall/IDS/IPS, niewłaściwa konfiguracja bezpieczeństwa w LAN	LAN (customercare), stacje robocze, sieć biurowa
K-3	Atak typu DDoS lub DoS	zła konfiguracja firewall/IDS/IPS, brak nadzoru nad ruchem (QoS); brak monitoringu obciążenia, błąd oprogramowania, utrata dostępu do usług WAN	Internet (self-care, POS) oraz zależności WAN/ISP
K-4	Nieautoryzowany dostęp do informacji	brak nadzoru nad uprawnieniami; zbyt wolne zmiany uprawnień, brak kontroli dostępu fizycznego do elementów systemu	LAN/Backend (customercare, administracja), także kanały Internet przy słabym IAM
K-5	Nieumiejętne posługiwanie się systemem przez użytkownika	brak szkoleń; brak kontroli jakości danych; podatność na socjotechnikę; odzyskanie informacji z nośników wycofanych z użycia	LAN/Internet (customercare, POS), obsługa danych i dokumentów

K-6	Przełamanie zabezpieczeń dostępu wewnątrz systemu	nieadekwatne uprawnienia, zbyt wolne zmiany uprawnień, brak nadzoru nad aktywnością, brak/źle wdrożone AV/firewall/IDS/IPS	LAN/Backend (customercare, admin), nadużycia i eskalacje uprawnień
K-7	Podsłuch danych, przechwyt danych	brak nadzoru nad ruchem (QoS), emisja ujawniająca; brak szyfrowania w łączach WAN, podsłuch w LAN; pozyskanie informacji z nośników wycofanych z użycia	Internet/WAN/LAN (POS przez Internet, kanały klientów), transmisje i endpointy
K-8	Włamanie do systemu z sieci zewnętrznej WAN (przełamanie zabezpieczeń)	brak aktualizacji oprogramowania, zła konfiguracja firewall/IDS/IPS, brak nadzoru nad ruchem, brak monitoringu obciążenia; socjotechnika	Internet => Backend (atak na portale/API/warstwę usług)
K-9	System podmiotu źródłem zakłóceń w cyberprzestrzeni	brak nadzoru nad ruchem, brak/nieaktualne AV, zła konfiguracja firewall/IDS/IPS	LAN/Backend (np. infekcje/botnet, wysyłka spamu)

3.3 Wykaz zagrożeń dla systemu

Poniżej przedstawiono wykaz zagrożeń dla analizowanego systemu w postaci scenariuszy incydentów. Scenariusze zostały opracowane na podstawie katalogu zagrożeń z pkt. 3.2 oraz w odniesieniu do aktywów zidentyfikowanych w Rozdziale 2. Identyfikacja zagrożeń obejmuje wszystkie kanały dostępu oraz kluczowe funkcje systemu. Na etapie identyfikacji zagrożeń nie dokonuje się jeszcze oszacowania prawdopodobieństwa ani skutków

Każde zagrożenie zostało zapisane jaki krótki scenariusz incydentu i powiązane z:

- Dotkniętymi aktywami;
- Obszarem użycia (Internet, LAN, Backend, utrzymanie, administracja);
- Atrybutami bezpieczeństwa CIA (P/I/D)
- Uwagami

Identyfikator	Identyfikator zagrożenia	Opis scenariusza	Dotknięte aktywa	Obszar użycia	C/I/A (P/I/D)	Uwagi
Z-1	K-1	Zainfekowanie stacji/urządzenia POS (np. złośliwy plik, link) i wykorzystanie dostępu do	A-9, A-16, A-10, A-12	Internet / backend	**P/I**/D	Zabezpieczenia

		systemu do dalszych nieautoryzowanych działań				
Z-2	K-1	Wirus szyfrujący dane na serwerach powoduje zaszyfrowanie zasobów i przestój usług.	A-10, A-11, A-12, A-13, A-1, A-2, A-3, A-4	Internet / backend / utrzymanie	P/I/**D**	Wymusza uruchomienie procedur odtwarzania danych z backupów
Z-3	K-2	Komputer pracownika customercare zostaje zainfekowany (np. po kliknięciu w fałszywy e-mail). Atakujący wykorzystuje to, żeby z tego komputera próbować dostać się dalej do systemów backendu (serwery, bazy danych, repo dokumentów).	A-8, A-16, A-10, A-12, A-12, A-1, A-2, A-3, A-4	LAN / Backend	**P/I**/D	Wektor wejścia: phishing (fałszywe e-maile), nośniki USB, infekcja komputera pracownika (endpoint)
Z-4	K-3	DDoS na portal self-care powoduje niedostępność logowania i pobierania dokumentów przez klientów	A-6, A-10, A-2, A-3, A-4	Internet	P/I/**D**	Utrata dostępności
Z-5	K-3	DDoS na API/backend powoduje niedostępność dla wszystkich kanałów (WWW/mobile/customercare/ POS)	A-10, A-6, A-7, A-8, A-9	Internet/ backend	P/I/**D**	Utrata dostępności
Z-6	K-4	Przejęcie konta klienta (phishing/credential stuffing) i pobranie faktur oraz billingów	A-6, A-7, A-10, A-1, A-2, A-3	Internet	**P/I**/D	Self-care WWW i mobile
Z-7	K-4	Nadużycie uprawnień pracownika customercare – masowy dostęp do danych klientów	A-8, A-16, A-10, A-12, A-1, A-2, A-3	LAN/ Backend/ utrzymanie	**P/I**/D	Zakres ról + monitoring działań(rozliczalność)
Z-8	K-4	Brak zgodności uprawnień z zakresem obowiązków (utrzymywanie nadmiernych uprawnień) – pracownik posiada dostęp do danych lub funkcji, do których nie powinien mieć dostępu, ponieważ uprawnienia nie zostały wykryte i skorygowane	A-13, A-12, A-11, A-19, A-16	Utrzymanie	**P/I**/D	Procedury związane z uprawnieniami

Z-9	K-5	Błąd pracownika (customercare/POS) powoduje udostępnienie danych niewłaściwemu odbiorcy lub nieuprawnioną zmianę	A-8, A-9, A-16, A-1, A-2, A-3	LAN/ Internet/ utrzymanie	**P/I**/D	Świadomość, kompetencje, procedury,
Z-10	K-5	Błędna alokacja uprawnień (nadanie nadmiernych uprawnień) – naruszenie zasady najmniejszych uprawnień.	A-11, A-16, A-18, A-19	Backend/ administracja	**P**/I/D	Świadomość, kompetencje, procedury,
Z-11	K-6	Eskalacja uprawnień do konta uprzywilejowanego i wykonanie operacji administracyjnych na danych	A-19, A-16, A-10, A-12, A-11, A-1, A-2, A-3, A-4	Backend/ administracja	**P/I/D**	Admin, narzędzia, separacja uprawnień
Z-12	K-6	Nadużycie kont uprzywilejowanych do nieautoryzowanych zmian (np. modyfikacja danych billingowych/dokumentów)	A-19, A-12, A-11, A-2, A-3	Backend / administracja	**P/I/**D	Integralność, monitorowanie, rozliczalność
Z-13	K-7	Przechwycenie danych w transmisji POS–system (np. błąd szyfrowania)	A-9, A-10, A-1, A-2, A-3	Internet	**P**/I/D	Kanał POS
Z-14	K-7	Kradzież tokenów/sesji klienta (np. na urządzeniu) i pobranie dokumentów lub operacje na koncie.	A-7, A-6, A-10, A-4	Internet/ mobile	**P**/I/D	Sesje, tokeny, mobile, zabezpieczenia
Z-15	K-7	Utrata/nieprawidłowa utylizacja nośników i odzyskanie danych klientów	A-13, A-1, A-2, A-3, A-4, A-17	Utrzymanie	**P**/I/D	Procedury
Z-16	K-8	Atak na portal self-care (WWW) wykorzystujący podatność aplikacji lub błędną konfigurację, prowadzący do uzyskania dostępu do danych klienta	A-6, A-10, A-12, A-1, A-2, A-3	Internet/ backend	**P**/I/D	Autoryzacja, sesje, zabezpieczenia
Z-17	K-8	Atak na API (np. błędy autoryzacji) umożliwia pobieranie dokumentów innych klientów	A-10, A-11, A-4, A-1, A-2, A-3	Internet/ backend	**P**/I/D	Ryzyko masowego wycieku przez API
Z-18	K-9	Komponent e-mail użyty do spamu/phishingu do klientów (nadużycie reputacji)	A-14, A-10	Internet / backend	**P/I**/D	Reputacja domeny, blokady dostawców

4. Metodyka i plan analizy ryzyka

4.1 Cel

W niniejszym rozdziale przedstawiono metodykę oraz plan przeprowadzania analizy ryzyka dla scenariuszy zagrożeń zidentyfikowanych w Rozdziale 3 w odniesieniu do aktywów opisanych w Rozdziale 2. Rozdział opisuje sposób postepowania z ryzkiem (proces), role oraz wymagane dane wejściowe.

4.2 Założenia i zakres analizy

Analiza ryzyka dotyczy systemu obsługi klientów indywidualnych (A-0) oraz wszystkich aktywów składowych. Uwzględniono wszystkie kanały dostępu wymienione w Rozdziale 1.

Podstawą analizy są zidentyfikowane zagrożenia Z-XX (Rozdział 3), które są powiązane z:

- Dotkniętymi aktywami (A-XX);
- Obszarem użycia;
- Atrybutami bezpieczeństwa informacji C/I/A(P/I/D)

4.3 Proces analizy i postępowania z ryzykiem

Proces realizowany jest iteracyjnie dla ryzyk opisanych w Rozdziale 3 w formie scenariuszy Z-xx, powiązanych z aktywami A-xx, obszarem użycia oraz atrybutami bezpieczeństwa (P/I/D).

4.3.1 Ustanowienie kontekstu

- Potwierdza się zakres analizy: aktywo nadrzędne A-0 i aktywa A-xx, kanały dostępu (self-care WWW/mobile, customercare, POS) oraz obszary (Internet/LAN/Backend/Utrzymanie).
- Określa się kryteria oceny ryzyka: skale prawdopodobieństwa materializacji zagrożenia P oraz skutków dla P/I/D, sposób wyznaczania poziomu ryzyka oraz progi kwalifikacji i akceptacji.
- Wskazuje się role i odpowiedzialności: właściciel ryzyka, właściciel aktywa, osoby dokonujące oceny, ścieżka eskalacji/akceptacji.

4.3.2 Analiza ryzyka

Dla każdego zagrożenia Z-XX przeprowadza się analizę ryzyka.

4.3.2.1 Szacowaniu prawdopodobieństwa incydentu P

Dla każdego zagrożenia Z-XX szacuje się wartość P (prawdopodobieństwo incydentu / materializacji zagrożenia) w skali 0–4:

- 0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),
- 1 – zdarzenie prawie nieprawdopodobne,
- 2 – zdarzenie mało prawdopodobne,

- 3 – zdarzenie wysoce prawdopodobne,
- 4 – zdarzenie niemal pewne.

Przy określaniu wartości prawdopodobieństwa powinny być brane pod uwagę następujące okoliczności:

- doświadczenie szacującego oraz statystyki dotyczące podobnych zdarzeń,
- w przypadku zagrożeń antropogennych atrakcyjność zasobu lub efektu skutku dla wywołującego incydent,
- dla zagrożeń o charakterze przypadkowym położenie geograficzne, warunki pogodowe itp., które mogą oddziaływać na powstawanie błędnych działań użytkowników zasobów informacyjnych lub systemów teleinformatycznych,
- rodzaje podatności,
- istniejące zabezpieczenia.

4.3.2.2 Szacowanie skutków oddzielnie dla atrybutów bezpieczeństwa

Dla każdego zagrożenia **Z-XX** szacuje się skutki oddzielnie dla atrybutów bezpieczeństwa informacji:

- Sd (dostępność)
- Si(integralność)
- Sp(poufność)

Wartości skutków (Sd/Si/Sp) przypisuje się w skali 0-4:

- 0 – zdarzenie nie powoduje skutku (brak podatności),
- 1 – zdarzenie wywołuje niewielki skutek,
- 2 – zdarzenie wywołuje znaczący skutek,
- 3 – zdarzenie wywołuje bardzo znaczący skutek,
- 4 – zdarzenie wywołuje skutek katastrofalny.

Następstwa mogą mieć charakter materialny (np. koszt odtworzenia danego zasobu lub przywrócenia jego sprawności) lub niematerialny (np. utrata wizerunku podmiotu w społeczeństwie). Wskazane jest, aby szacowanie następstw (skutków) było prowadzone w odniesieniu do określonych scenariuszy incydentów. (Źródło załącznik Metodyka_zarządzania_ryzykiem)

4.3.2.3 Wyznaczanie poziomu ryzyka pierwotnego Rp

Po oszacowaniu prawdopodobieństwa incydentu P (prawdopodobieństwo incydentu / materializacji zagrożenia) oraz skutków Sd/Si/Sp dla danego zagrożenia Z-XX wyznacza się poziom ryzyka pierwotnego Rp (ryzyko pierwotne) zgodnie ze wzorem:

$$Rp = P \times (Sd + Si + Sp)$$

4.3.3 Ocena ryzyka

Ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyka pierwotnego **Rp** z kryteriami akceptacji oraz na ustaleniu priorytetów.

- **Rp ≤ 9,6** (≤ 20% poziomu maksymalnego) – ryzyko uznaje się a priori za **szczątkowe** i nie podlega procedurze postępowania z ryzykiem,
- **Rp > 9,6** (> 20% poziomu maksymalnego) – ryzyko **podlega** procedurze postępowania z ryzykiem.

4.3.4 Postępowanie z ryzykiem

Ryzyka, które na etapie oceny nie zostały uznane za ryzyka szczątkowe, podlegają procedurze postępowania z ryzykiem. Postępowanie z ryzykiem może polegać na:

1. **mitygacji ryzyka** (zmniejszenie poziomu ryzyka poprzez zastosowanie zabezpieczeń)
2. unikaniu ryzyka,
3. przeniesieniu ryzyka,
4. akceptacji ryzyka, mimo że jego poziom przekracza poziom ryzyka szczątkowego.

4.3.4.1 Mitygacja ryzyka

Mitygacja ryzyka polega na ograniczaniu poziomu ryzyka poprzez zastosowanie zabezpieczenia (środka kontroli) dobranego adekwatnie do charakteru danego ryzyka.

Na etapie mitygacji ryzyka dokonuje się ponownego estymowania poziomu ryzyka z uwzględnieniem zastosowanych zabezpieczeń. Przeliczenie wykonywane jest według wzoru:

$$Rk = P \times \left(\frac{Sd}{Cd} + \frac{Si}{Ci} + \frac{Sp}{Cp}\right)$$

- gdzie:
  - **Rk** – końcowy poziom ryzyka (ryzyko rezydualne),
  - **P** – prawdopodobieństwo incydentu / materializacji zagrożenia,
  - **Sd/Si/Sp** – skutki dla dostępności / integralności / poufności,
  - **C** – skuteczność zabezpieczenia,
  - **Cd/Ci/Cp** ∈ {1, 2, 3, 4}.
- gdzie:
  - 1 – brak zabezpieczenia,
  - 2 – zabezpieczenie ogranicza poziom ryzyka,
  - 3 – zabezpieczenie w istotny sposób ogranicza poziom ryzyka,
  - 4 – zabezpieczenie w bardzo istotny sposób ogranicza poziom ryzyka.

Zastosowanie zabezpieczenia powinno uwzględniać wpływ na pozostałe atrybuty bezpieczeństwa (np. mitygacja ryzyka utraty poufności może powodować wzrost ryzyka utraty

dostępności). W takim przypadku wymagany jest powrót do estymacji poziomu ryzyka z uwzględnieniem zastosowanego zabezpieczenia.

4.3.4.2 Unikanie ryzyka

Unikanie ryzyka polega na rezygnacji z realizacji czynności lub funkcjonalności powodującej ryzyko (zmiana zakresu lub sposobu realizacji). W przypadku realizacji zadań publicznych unikanie ryzyka, co do zasady, nie ma zastosowania.

4.3.4.3 Przeniesienie ryzyka

Przeniesienie ryzyka polega na przekazaniu skutków ryzyka do podmiotu trzeciego. W przypadku realizacji zadań publicznych przeniesienie ryzyka, co do zasady, nie ma zastosowania. Niemniej przeniesienie ryzyka może być zasadne np. w postaci ubezpieczenia składników majątkowych systemu.

4.3.4.4 Akceptacja ryzyka

W wyniku mitygacji ryzyka i przeliczenia poziomów ryzyka uzyskuje się wartość końcową poziomu ryzyka **Rk**.

- ryzyka, dla których końcowy poziom ryzyka jest niższy lub równy **20% poziomu maksymalnego** (tj. **Rk ≤ 9,6**) podlegają automatycznej akceptacji,
- ryzyka, dla których poziom zawiera się w przedziale **9,6 < Rk ≤ 38,4** podlegają akceptacji według zasad ustalonych w podmiocie lub wymagają ponownej analizy,
  o ryzyka, dla których poziom ryzyka jest większy niż **80% poziomu maksymalnego** (tj. **Rk > 38,4**) przedstawiane są do akceptacji kierownictwa podmiotu lub wymagaja ponownej analizy.

4.3.5 Wyniki i dokumentacja procesu

Wynikiem realizacji procesu szacowania, oceny i postępowania z ryzykiem jest komplet dokumentacji stanowiącej podstawę zarządzania ryzykiem w systemie:

- Rejestr ryzyk – zestawienie scenariuszy Z-XX powiązanych z aktywami A-XX, zawierające wartości P, Sd/Si/Sp, Rp, decyzję z etapu oceny (szczątkowe / do postępowania) oraz priorytet.
- Plan mitygacji ryzyka – wykaz działań (zabezpieczeń) przypisanych do ryzyk wymagających postępowania, wraz z właścicielem działania, terminem realizacji oraz kryterium weryfikacji skuteczności.
- Karta/Deklaracja stosowania zabezpieczeń (SoA – Statement of Applicability) – wykaz zabezpieczeń rozpatrywanych w ramach mitygacji ryzyka wraz z decyzją „stosowane/niestosowane" oraz uzasadnieniem, powiązaniem z ryzykami (Z-XX) i odniesieniem do wymagań/polityk SZBI.
- Decyzje akceptacji ryzyka – udokumentowane decyzje dotyczące akceptacji ryzyk po mitygacji (Rk).

- Założenia monitorowania i przeglądu – wskazanie, jakie elementy podlegają monitoringowi (np. logi, alerty, przeglądy uprawnień, testy odtworzeń) oraz kiedy wykonywany jest przegląd ryzyk (okresowo oraz po zmianach/incydentach).

5. Pytania audytowe

5.1 Cel

Celem niniejszego rozdziału jest wskazanie zagadnień do dalszej analizy w formie checklisty pytań audytowych. Pytania te służą do zebrania danych wejściowych niezbędnych do rzetelnego oszacowania wartości P (prawdopodobieństwo) oraz skutków Sd/Si/Sp (dostępność/integralność/poufność) dla scenariuszy zagrożeń Z-XX, a także do oceny skuteczności zabezpieczeń Cd/Ci/Cp w procesie mitygacji ryzyka.

5.2 Wykaz pytań audytowych

Obszar	Pytanie audytowe (kluczowe)	Po co to pytanie (co zasila w analizie)	Przykładowy dowód / źródło
Architektura i strefy	Jak wygląda podział na strefy (Internet/LAN/Backend/Utrzymanie) oraz przepływy danych między kanałami (WWW/mobile/customercare/POS) a backendem (A-10) i bazą danych (A-12)?	Uzasadnienie **P** (ekspozycja), oraz skutków **Sd/Sp** (wpływ i rozległość)	Diagramy architektury, schematy sieci, opis przepływów danych, CMDB
Tożsamość i uprawnienia	Jak realizowane są uwierzytelnianie i autoryzacja użytkowników (klient/customercare/POS/admin), w tym MFA, model ról (A-16) oraz proces nadawania/odbierania uprawnień (w tym kont uprzywilejowanych A-19)?	Uzasadnienie **P** (przejęcie/nadużycia), wpływ na **Sp/Si**, podstawa do oceny mitygacji (**Cp/Ci**)	Konfiguracje IAM/PAM, macierz ról, procedury dostępowe, logi uprawnień
Ochrona danych i dokumentów	Jak chronione są dane i dokumenty (A-1…A-4, A-11) w spoczynku i w transmisji (szyfrowanie, kontrola dostępu) oraz jakie są zasady klasyfikacji i retencji/usuwania (A-18)?	Uzasadnienie skutków **Sp/Si**, ograniczenie skutków (mitygacja **Cp/Ci**)	Polityka klasyfikacji/retencji, konfiguracje szyfrowania (KMS/TLS), ACL/role, procedury usuwania
Logowanie i monitoring	Jakie zdarzenia są logowane i monitorowane (w szczególności pobieranie faktur/billingów/dokumentów), czy istnieje detekcja anomalii oraz jak wygląda obsługa incydentów?	Uzasadnienie **P** (wykrywalność/reakcja), wsad do decyzji o mitygacji i monitoringu	SIEM/logi aplikacyjne, reguły alertów, playbook IR, raporty incydentów
Ciągłość działania i odtwarzanie	Jakie są wymagania dostępności (RTO/RPO) dla kanałów i backendu oraz jak realizowane są kopie zapasowe (A-13) i testy odtwarzania?	Uzasadnienie skutków **Sd**, ocena mitygacji **Cd**	SLA/SLO, polityka backup, harmonogramy, raporty testów odtwarzania/DR

6. Obliczenie ryzyka według metodyki (przykład dla najwyższego ryzyka)

6.1 Cel i założenia

Celem niniejszego rozdziału jest przedstawienie sposobu obliczenia poziomu ryzyka pierwotnego Rp oraz poziomu ryzyka końcowego Rk dla wszystkich scenariuszy zagrożeń Z-XX z Rozdziału 3, z wykorzystaniem arkusza kalkulacyjnego (Excel). Wyniki obliczeń służą do ustalenia priorytetów ryzyk oraz wskazania scenariusza o najwyższym poziomie ryzyka.

Obliczenia wykonywane są dla każdego scenariusza **Z-XX** zgodnie z rozdziałem 4.

Na potrzeby demonstracji metodyki dopuszcza się wypełnienie wartości **P, Sd, Si, Sp** (oraz **Cd, Ci, Cp**) danymi przykładowymi/testowymi. W takim przypadku wyniki stanowią ilustrację działania metodyki oraz sposobu wyznaczenia scenariusza o najwyższym ryzyku, a nie wynik analizy opartej o dowody audytowe. **Zasady punktacji oraz interpretacja skal P, Sd/Si/Sp i Cd/Ci/Cp zostały przedstawione w Rozdziale 4. W przypadku przeprowadzania rzeczywistego szacowania ryzyka należy stosować te zasady oraz opierać przypisania wartości na zebranych danych i dowodach (w tym odpowiedziach na pytania audytowe).**

6.2 Kontekst i dane wejściowe

Symulacja obliczeń ryzyka wykonywana jest dla scenariuszy zagrożeń **Z-XX** zidentyfikowanych w Rozdziale 3 i powiązanych z aktywami **A-XX** z Rozdziału 2.

6.3 Tabela 1 – wyznaczenie poziomu ryzyka pierwotnego Rp oraz kwalifikacja ryzyk szczątkowych

Formuły i obliczenia na podstawie danych z rozdziału 4.

Z_ID	K_ID	Atrybuty (P/I/D)	P (0-4)	Sd (0-4)	Si (0-4)	Sp (0-4)	Rp	Kwalifikacja_Rp	Do_mitygacji
Z-1	K-1	P/I/D	3	3	3	4	30,0	Do mitygacji	TAK
Z-2	K-1	P/I/D	3	2	3	1	18,0	Do mitygacji	TAK
Z-3	K-2	P/I/D	2	1	1	0	4,0	Szczątkowe	NIE
Z-4	K-3	P/I/D	2	3	3	0	12,0	Do mitygacji	TAK

Z-5	K-3	P/I/D	2	4	3	4	22,0	Do mitygacji	TAK
Z-6	K-4	P/I/D	3	1	2	0	9,0	Szczątkowe	NIE
Z-7	K-4	P/I/D	3	0	4	3	21,0	Do mitygacji	TAK
Z-8	K-4	P/I/D	2	3	1	4	16,0	Do mitygacji	TAK
Z-9	K-5	P/I/D	0	4	2	1	0,0	Szczątkowe	NIE
Z-10	K-5	P/I/D	3	2	4	1	21,0	Do mitygacji	TAK
Z-11	K-6	P/I/D	2	1	1	2	8,0	Szczątkowe	NIE
Z-12	K-6	P/I/D	2	1	0	2	6,0	Szczątkowe	NIE
Z-13	K-7	P/I/D	4	2	0	2	16,0	Do mitygacji	TAK
Z-14	K-7	P/I/D	0	4	4	1	0,0	Szczątkowe	NIE
Z-15	K-7	P/I/D	3	4	2	4	30,0	Do mitygacji	TAK
Z-16	K-8	P/I/D	4	3	2	4	36,0	Do mitygacji	TAK
Z-17	K-8	P/I/D	3	4	2	1	21,0	Do mitygacji	TAK
Z-18	K-9	P/I/D	1	0	0	4	4,0	Szczątkowe	NIE

Scenariusz **Z-16** („Atak na portal self-care (WWW) wykorzystujący podatność aplikacji lub błędną konfigurację, prowadzący do uzyskania dostępu do danych klienta") uzyskał **najwyższą wartość ryzyka pierwotnego Rp = 36** w zestawieniu scenariuszy. W związku z tym scenariusz Z-16 został wybrany jako przykład do przedstawienia kolejnego etapu procesu, tj. **mitygacji ryzyka** oraz wyznaczenia wartości **Rk**.

6.4 Mitygacja ryzyka (przykład Z-16)

Celem mitygacji ryzyka jest obniżenie poziomu ryzyka dla scenariusza **Z-16** poprzez dobór środków kontrolnych oraz ocenę ich skuteczności. Zgodnie z metodyką, na etapie mitygacji **nie zmienia się wartości skutków Sd/Si/Sp** przypisanych do scenariusza. Wpływ zabezpieczeń na ryzyko odzwierciedla się poprzez współczynniki skuteczności **Cd/Ci/Cp** (dla dostępności/integralności/poufności), na podstawie których wyznacza się wartość ryzyka końcowego **Rk**.

Dobór zabezpieczeń wykonano w sposób minimalny i przejrzysty – **po jednym środku kontrolnym dla każdego atrybutu P/I/D**, aby jednoznacznie powiązać mitygację z oceną skuteczności **Cp/Ci/Cd**.

Z_ID	Z-16
K_ID	K-8
Opis scenariusza	Atak na portal self-care (WWW) wykorzystujący podatność aplikacji lub błędną konfigurację, prowadzący do uzyskania dostępu do danych klienta
Dotknięte aktywa	A-6, A-10, A-12, A-1, A-2, A-3
Obszar użycia	Internet / backend
Atrybuty	**P**/I/D
Wybrane zabezpieczenia (katalog)	**P– Cp** PROXY/WAF + listy blokad URL/IP (katalog: WAN – poz. 6) **I– Ci** Rozproszenie uprawnień / zasada „czterech par oczu” dla operacji wrażliwych (katalog: Nieautoryzowany dostęp – poz. 4) **D – Cd** Procedury reagowania na wykryte incydenty (katalog: WAN – poz. 9)

Uzasadnienie doboru	• **P (poufność) / Cp:** PROXY/WAF ogranicza możliwość skutecznego wykorzystania podatności aplikacyjnych i utrudnia nieautoryzowane pobieranie danych (blokowanie wzorców ataku, filtrowanie, reguły). • **I (integralność) / Ci:** zasada „4-eyes" (rozproszenie uprawnień) ogranicza możliwość wykonania nieautoryzowanych zmian w danych lub dokumentach – nawet jeśli nastąpi przełamanie warstwy aplikacji. • **D (dostępność) / Cd:** procedury reagowania na incydenty skracają czas identyfikacji, izolacji i przywrócenia usługi po incydencie, co ogranicza wpływ na dostępność (organizacyjna zdolność odtworzenia/ustabilizowania usługi).
P	4
Sd	3
Si	2
Sp	4
Rp	36,0
Cd	1
Ci	2
Cp	2
Rk	24,0
Decyzja	Ponowna analiza
Komentarz	Ryzyko po mitygacji pozostaje > 9,6 (nie jest szczątkowe) – wymaga ponownej analizy.

Na podstawie przyjętych wartości **Cd/Ci/Cp** obliczono ryzyko końcowe **Rk**. Po mitygacji poziom ryzyka pozostaje powyżej progu ryzyka szczątkowego. Oznacza to, że ryzyko nie może zostać uznane za szczątkowe i wymaga ponownej analizy.

6.5 Wniosek oraz kwalifikacja do ponownej analizy

Na podstawie przyjętych wartości Cd/Ci/Cp wyznaczono ryzyko końcowe Rk dla scenariusza Z-16. Po zastosowaniu mitygacji poziom ryzyka pozostaje powyżej progu ryzyka szczątkowego, co oznacza, że ryzyko nie może zostać uznane za szczątkowe i wymaga dalszego postępowania.

W ramach dalszego postępowania:

- ryzyko kieruje się do ponownej analizy, w szczególności w zakresie doboru dodatkowych środków kontrolnych lub zwiększenia skuteczności mitygacji (Cd/Ci/Cp),
- po ponownej analizie wykonywane jest ponowne przeliczenie Rk oraz decyzja akceptacyjna zgodnie z progami i zasadami podmiotu (akceptacja wg zasad / eskalacja do kierownictwa).

Z_ID	Z-16
K_ID	K-8
Opis scenariusza	Atak na portal self-care (WWW) wykorzystujący podatność aplikacji lub błędną konfigurację, prowadzący do uzyskania dostępu do danych klienta
Dotknięte aktywa	A-6, A-10, A-12, A-1, A-2, A-3
Obszar użycia	Internet / backend
Atrybuty	P/I/D
Wybrane zabezpieczenia (katalog)	P – Cp PROXY/WAF + listy blokad URL/IP (katalog: WAN – poz. 6) I – Ci Rozproszenie uprawnień / zasada „czterech par oczu” dla operacji wrażliwych (katalog: Nieautoryzowany dostęp – poz. 4) D – Cd Procedury reagowania na wykryte incydenty (katalog: WAN – poz. 9)

Uzasadnienie doboru	• P (poufność) / Cp: PROXY/WAF ogranicza możliwość skutecznego wykorzystania podatności aplikacyjnych i utrudnia nieautoryzowane pobieranie danych (blokowanie wzorców ataku, filtrowanie, reguły). • I (integralność) / Ci: zasada „4-eyes" (rozproszenie uprawnień) ogranicza możliwość wykonania nieautoryzowanych zmian w danych lub dokumentach, nawet jeśli nastąpi przełamanie warstwy aplikacji. • D (dostępność) / Cd: procedury reagowania na incydenty skracają czas identyfikacji, izolacji i przywrócenia usługi po incydencie, ograniczając wpływ na dostępność.
P	4
Sd	3
Si	2
Sp	4
Rp	36,0
Cd	4
Ci	4
Cp	4
Rk	9,0
Decyzja	Akceptacja
Komentarz	Ryzyko po mitygacji ≤ 9,6 (szczątkowe) – podlega akceptacji.

Na podstawie przyjętych wartości skuteczności mitygacji **Cd/Ci/Cp** wyznaczono ryzyko końcowe **Rk** dla scenariusza **Z-16.** Uzyskany poziom ryzyka końcowego spełnia kryterium ryzyka szczątkowego (tj. **Rk ≤ 9,6**), co oznacza, że ryzyko może zostać uznane za akceptowalne w ramach bieżącej iteracji analizy.

W konsekwencji:

- ryzyko **Z-16** kwalifikuje się do **akceptacji**,
- scenariusz pozostaje ujęty w **rejestrze ryzyk** jako ryzyko nadzorowane (monitorowane),
- utrzymuje się wymaganie **weryfikacji skuteczności** wdrożonych zabezpieczeń w ramach przeglądów okresowych oraz po incydentach lub zmianach w systemie.

6.6 Dalsze postępowanie i podsumowanie

Wyniki przeprowadzonej analizy oraz mitygacji dla scenariusza **Z-16** wymagają odzwierciedlenia w dokumentacji wskazanej w pkt. **4.3.5 Wyniki i dokumentacja procesu**. W szczególności należy:

- **Zaktualizować Rejestr ryzyk** – uzupełnić wpis dla Z-16 o wartości zastosowane zabezpieczenia, wartości skuteczności **Cd/Ci/Cp**, wynik **Rk** oraz decyzję o **akceptacji** i status „monitorowane".
- **Zaktualizować Plan mitygacji ryzyka** – wykazać działania/zabezpieczenia przypisane do Z-16 (właściciel działania, termin, sposób weryfikacji skuteczności), a następnie oznaczyć je jako wdrożone lub zaplanowane.
- **Uzupełnić Kartę/Deklarację stosowania (SoA – Statement of Applicability)** – wskazać zabezpieczenia przyjęte dla Z-16 jako „stosowane" (lub „planowane"), podać uzasadnienie ich wyboru oraz powiązać je z ryzykiem (Z-16) i wymaganiami/politykami SZBI.
- **Udokumentować decyzję akceptacji ryzyka** – zapisać decyzję dotyczącą akceptacji ryzyka po mitygacji (**Rk**) wraz z zakresem, datą, właścicielem ryzyka oraz warunkami (np. wymagany monitoring, przegląd okresowy).
- **Określić monitoring i przegląd** – wskazać, jakie elementy podlegają monitorowaniu (np. zdarzenia , logi dostępu, alerty bezpieczeństwa, przeglądy uprawnień) oraz kiedy wykonywany jest przegląd ryzyk (okresowo oraz po zmianach/incydentach).

8. Podsumowanie

W ramach niniejszego opracowania przeprowadzono identyfikację aktywów systemu obsługi klientów indywidualnych oraz zidentyfikowano zagrożenia w formie scenariuszy incydentów dla wszystkich kanałów dostępu (self-care WWW/mobile, customercare, POS). Następnie zastosowano metodykę szacowania i oceny ryzyka zgodnie z Rozdziałem 4, wyznaczając poziomy ryzyka pierwotnego **Rp** oraz – dla scenariuszy wymagających postępowania – ryzyko końcowe **Rk** po mitygacji.