AZALIZA ZAGROŻEŃ I RYZYKA

Spis treści znajduje się na ostatnie stornie

# IDENTYFIKACJA POTENCJALNYCH ZAGROŻEŃ

W tej sekcji przedstawione zostaną największe według naszego zespołu zagrożenia jakie mogą wpłynąć negatywnie na sukces naszego projektu.

1. **Ataki hackerskie**: Nasza platforma może być podatna na ataki hackerskie, polegające na kradzieży danych osobowych czy blokowaniu strony oraz żądaniu okupu w zamian za wznowienie działania
2. **Oszustwa transakcyjne:** Użytkownicy sprzedający swoje towary mogą chcieć oszukiwać kupujących oraz na odwrót tzn. kupujący będą chcieć oszukać sprzedawców
3. **Problemy techniczne**: Przerwy techniczne oraz błędy w działaniu strony takie jak problemy z serwerem, problemy z wydajnością strony internetowej przy dużych obciążeniach itp., mogą prowadzić do utraty klientów i spadku zainteresowania stroną.
4. **Problemami związanymi z ocenami i opiniami:** Nasza platforma może spotkać się z nieuczciwymi za graniami ze strony konkurencji, która będzie chciała naruszyć opinie o „Ollegro”. Może to wpłynąć negatywnie na poziom zainteresowania i zaufania w stosunku do naszej platformy.

# OCENA RYZYKA

## Atak Hackerski

**Prawdopodobieństwo**: Wysokie  
**uzasadnienie:** można obserwować ataki na inne strony tego typu. Przykładem może tu być Allegro, które niedawno (5/3/2023)1 zostało zaatakowane. Hackerzy chcieli wykraść informacje za pomocą phishing’u. Wysokie prawdopodobieństwo wynika z zysków jakie wynikają z tego typu sytuacji.

**Wpływ:** Wysoki  
**Uzasadnienie:** Uzyskanie przez osoby niepożądane dostępu do danych osobowych naszych klientów może mieć ogromny wpływ na zaufanie jakim darzą naszą stronę. Może spowodować to spadek obrotów oraz problemy prawne.

## Oszustwa transakcyjne

**Prawdopodobieństwo:** Wysokie   
**uzasadnienie:** wyłudzenia oraz oszustwa to popularna plaga jaka dotyka sklepów internetowych. Przykładem może tu być portal OLX. W tym przypadku policja2 zamieszcza informacje o nowych metodach jakie stosują oszuści.

**Wpływ:** średni   
**uzasadnienie:** Oszustwa mogą zmniejszyć zaufanie do naszego portalu. W pesymistycznym przypadku, gdy oszustów będzie odpowiednio dużo wtedy może dojść do całkowitej utraty zainteresowania naszym projektem przez użytkowników. W tej sytuacji dochodzi do rozmycia odpowiedzialności pomiędzy serwis, bank oraz samego użytkownika. Wina w zależności od przypadku może leżeć po której ze stron, nie można jednak zakładać że za wszystkie przypadki nadużyć odpowiedzialna będzie nasza witryna.

## Problemy techniczne

**Prawdopodobieństwo:** Średnie   
**Uzasadnienie:** W przypadku platform e-commerce, problemy techniczne, takie jak przerwy, błędy w działaniu strony lub problemy z wydajnością, mogą występować, ale nie zawsze są tak powszechne. Mogą być wynikiem sporadycznych incydentów technicznych lub nieprzewidzianych czynników. Częstym problemem w przerwie w działaniu strony jest przeciążenie serwerów.

**Wpływ:** Średni   
**Uzasadnienie:** Przerwy w działaniu strony mogą frustrować użytkowników oraz zniechęcać ich do korzystania ze strony. Problemy techniczne, w naszym rozumieniu są to przerwy w działaniu strony, nie skutkują konsekwencjami prawnymi w przeciwieństwie do wycieków danych osobowych.

## Problemami związanymi z ocenami i opiniami

**Prawdopodobieństwo:** Średnie  
**uzasadnienie:** Inne platformy mogą chcieć zmniejszyć zainteresowanie naszym sklepem. Istnieje jednak prawdopodobieństwo powiązania negatywnych opinii z nieuczciwą konkurencją, co może spowodować odwrotny efekt od zamierzonego (z perspektywy konkurencji)

**Wpływ:** Średni   
**uzasadnienie:** Nieuczciwe oceny i opinie mogą wprowadzić dezinformację, utracić zaufanie klientów oraz wpływać negatywnie na decyzje zakupowe. Mogą skutkować spadkiem zainteresowania i reputacji naszej platformy, ale możliwość naprawienia tego wpływu istnieje poprzez monitorowanie i zarządzanie ocenami i opiniami.

# STRATEGIE ZARZĄDZANIA RYZYKIEM

Ataki hackerskie:   
1. Bezpieczeństwo systemu i oprogramowania:

* + Regularne aktualizacje: Zapewnienie, że nasz system i oprogramowanie są regularnie aktualizowane z najnowszymi poprawkami i łatkami bezpieczeństwa. To pomoże w minimalizacji luk i podatności na ataki.

1. Ochrona danych osobowych:
   * Szyfrowanie danych: Wdrażanie protokołów szyfrowania danych, takich jak protokół SSL/TLS, aby chronić poufność i integralność danych osobowych klientów w czasie przesyłania.
   * Bezpieczne przechowywanie danych: Zapewnienie bezpiecznego przechowywania danych osobowych klientów poprzez zastosowanie odpowiednich metod i standardów bezpieczeństwa.
2. Monitorowanie i wykrywanie zagrożeń:
   * System monitoringu: Wdrożenie systemu monitorowania, który będzie analizować i wykrywać potencjalne zagrożenia oraz ataki na naszą platformę.
   * Wykrywanie anomalii: Stosowanie technik wykrywania anomalii, które pomogą w identyfikacji podejrzanej aktywności, takiej jak nieautoryzowane próby logowania czy niezwykłe zachowanie użytkowników.
3. Świadomość i szkolenia pracowników:
   * Szkolenia z cyberbezpieczeństwa: Zapewnienie odpowiednich szkoleń dla pracowników w zakresie cyberbezpieczeństwa, aby zwiększyć ich świadomość i umiejętności w rozpoznawaniu potencjalnych zagrożeń.
   * Polityka bezpieczeństwa: Opracowanie i wprowadzenie polityki bezpieczeństwa, która określi zasady i procedury dotyczące ochrony danych oraz postępowania w przypadku podejrzenia naruszenia bezpieczeństwa.
4. Reagowanie na incydenty:
   * Plan reagowania na incydenty: Opracowanie planu reagowania na incydenty, który zawiera procedury i odpowiedzialności w przypadku ataku hackerskiego. W tym planie należy uwzględnić szybką reakcję, powiadomienie odpowiednich organów i klientów, jak również analizę incydentu i wdrażanie działań naprawczych.
5. Audyt bezpieczeństwa:
   * Regularne audyty bezpieczeństwa: Przeprowadzanie regularnych audytów bezpieczeństwa, aby ocenić skuteczność środków ochronnych, identyfikować ewentualne luki i wprowadzać ulepszenia w systemie ochrony.

## Oszustwa transakcyjne:

1. Edukacja klientów:
   * Szkolenia i informacje: Zapewnienie klientom informacji i szkoleń na temat bezpiecznych praktyk transakcyjnych oraz świadomości zagrożeń związanych z oszustwami. Można opracować materiały edukacyjne, poradniki i wskazówki, które pomogą klientom unikać pułapek oszustów.
2. Weryfikacja sprzedawców:
   * System weryfikacji: Wdrożenie systemu weryfikacji sprzedawców, który sprawdza ich wiarygodność i historię transakcji. Można wykorzystać różne metody weryfikacji, takie jak weryfikacja danych kontaktowych, opinie od innych klientów itp.
3. Bezpieczne płatności:
   * Bezpieczne bramki płatności: Wprowadzenie zaufanych i bezpiecznych bramek płatności, które zapewniają ochronę danych finansowych klientów i minimalizują ryzyko oszustw związanych z płatnościami.
4. System monitoringu:
   * Monitorowanie aktywności: Wdrożenie systemu monitorowania aktywności transakcyjnej, który analizuje zachowanie klientów i identyfikuje potencjalne nieprawidłowości. Może to obejmować wykrywanie niezwykłych wzorców zachowań, dużej liczby reklamacji czy nieautoryzowanych działań.
5. Polityka zwrotów i reklamacji:
   * Jasne zasady: Ustanowienie jasnych zasad dotyczących zwrotów i reklamacji, które zapewniają ochronę klientów w przypadku nieuczciwych transakcji. Wspieranie uczciwych i szybkich rozwiązań reklamacji, aby utrzymać zaufanie klientów.
6. Komunikacja i wsparcie klientów:
   * Otwarta komunikacja: Zapewnienie łatwego dostępu do kontaktu z obsługą klienta, aby klienci mogli zgłaszać potencjalne oszustwa lub problemy z transakcjami. Wysoka jakość obsługi klienta pomoże w rozwiązaniu problemów i przywróceniu zaufania.
7. Analiza danych i monitorowanie trendów:
   * Analiza danych: Regularna analiza danych transakcyjnych, opinii i innych informacji, aby identyfikować trendy i wzorce związane z oszustwami transakcyjnymi. To pomoże w doskonaleniu strategii i dostosowaniu działań zapobiegawczych.

Problemy techniczne*:*

1. Monitorowanie i zapobieganie przerwom technicznym:
   * Skalowalność infrastruktury: Upewnienie się, że nasza infrastruktura jest skalowalna i elastyczna, aby móc obsłużyć większe obciążenia i minimalizować ryzyko przerw technicznych w przypadku wzrostu ruchu na stronie.
2. Testowanie i utrzymanie systemu:
   * Testy wydajności: Przeprowadzanie regularnych testów wydajności, aby zidentyfikować ewentualne wąskie gardła i problemy z wydajnością strony. To pomoże nam zoptymalizować naszą infrastrukturę i uniknąć przeciążeń.
   * Regularne aktualizacje: Zapewnienie regularnych aktualizacji i utrzymania naszego systemu, oprogramowania oraz zabezpieczeń. Aktualizacje mogą zawierać łatki naprawiające błędy i podatności, które mogą prowadzić do problemów technicznych.
3. Plan awaryjny i przywracanie systemu:
   * Plan awaryjny: Opracowanie planu awaryjnego, który określa procedury i odpowiedzialności w przypadku przerw technicznych. Powinien obejmować szybkie przywracanie działania strony, zapewnienie wsparcia technicznego dla klientów oraz minimalizację wpływu przerw na biznes.
   * Regularne kopie zapasowe: Wykonywanie regularnych kopii zapasowych danych, aby w razie przerw technicznych móc przywrócić działanie strony do ostatniej sprawnej wersji.
4. Komunikacja z klientami:
   * Otwarta komunikacja: Informowanie klientów o problemach technicznych, przerwach lub planowanych pracach konserwacyjnych. Ważne jest utrzymanie otwartej linii komunikacji, aby zachować zaufanie klientów i dostarczyć im aktualnych informacji.
5. Świadomość i szkolenia pracowników:
   * Szkolenia techniczne: Zapewnienie szkoleń dla pracowników związanych z obsługą systemu, rozwiązywaniem problemów technicznych oraz procedurami awaryjnymi. Wysoka kompetencja pracowników przyczyni się do szybkiego rozwiązania problemów i minimalizacji wpływu przerw technicznych.

## Problemy związane z ocenami i opiniami:

1. Weryfikacja ocen i opinii:
   * System weryfikacji: Wdrożenie systemu weryfikacji ocen i opinii, który sprawdza ich autentyczność i wiarygodność. Można stosować różne metody weryfikacji, takie jak weryfikacja użytkowników, sprawdzanie treści czy analiza wzorców i anomalii.
2. Monitorowanie i reagowanie:
   * System monitorowania: Wdrożenie systemu monitorowania ocen i opinii, który analizuje i śledzi wpływające informacje. W przypadku wykrycia podejrzanych lub nieuczciwych ocen, podejmowanie szybkich działań w celu ich zbadania i rozwiązania.
3. Otwarta komunikacja z klientami:
   * Odpowiedzi na opinie: Regularne monitorowanie i odpowiadanie na opinie klientów, zarówno pozytywne, jak i negatywne. Ważne jest, aby być otwartym na feedback klientów i podejmować działania w celu rozwiązania problemów zgłaszanych przez nich.
4. Polityka usuwania nieuczciwych ocen:
   * Procedury usuwania: Opracowanie jasnych procedur i polityki usuwania nieuczciwych, obraźliwych lub spamowych ocen. Wdrażanie takich procedur pozwoli utrzymać jakość i wiarygodność ocen i opinii na platformie.
5. Zwiększenie zaufania i angażowania klientów:
   * System nagradzania: Wprowadzenie systemu nagradzania klientów za uczciwe i wartościowe opinie, co zachęci do wystawiania wiarygodnych ocen.
   * Uwzględnianie opinii: Aktywne uwzględnianie opinii klientów i wprowadzanie ulepszeń na podstawie ich feedbacku. Pokazanie klientom, że ich opinie są ważne i mają wpływ na rozwój naszego sklepu.
6. Monitorowanie konkurencji:
   * Analiza rynku: Regularna analiza rynku i monitorowanie działań konkurencji w celu identyfikacji potencjalnych prób manipulacji ocenami i opiniami. Może to pomóc w szybkim reagowaniu i ograniczaniu wpływu negatywnych działań konkurencji.
7. Edukacja klientów:
   * Szkolenia i informacje: Zapewnienie klientom informacji na temat procesu oceniania i składania opinii. Można opracować wytyczne i poradniki, które pomogą klientom wystawiać uczciwe i wartościowe oceny.

Rozwiązania przedstawione w ten sekcji są jedynie celami do jakich należy dążyć, w obecnej demonstracyjnej wersji strony nie została wdrożona większość z przedstawionych rozwiązań.

# PODSUMOWANIE

Analiza zagrożeń i ryzyka przeprowadzona dla naszego sklepu e-commerce "Ollegro" identyfikuje kilka istotnych obszarów, które wymagają uwagi i odpowiednich strategii zarządzania ryzykiem. Wysokie prawdopodobieństwo ataków hackerskich, oszustw transakcyjnych, problemów technicznych oraz nieuczciwych ocen i opinii może mieć negatywny wpływ na reputację naszej platformy, zaufanie klientów oraz obroty.

W odpowiedzi na te zagrożenia, proponujemy następujące strategie zarządzania ryzykiem:

1. Ataki hackerskie: Wdrożenie środków bezpieczeństwa cybernetycznego, takich jak silne zabezpieczenia, monitorowanie systemu, regularne aktualizacje oprogramowania i świadomość pracowników w zakresie cyberbezpieczeństwa.
2. Oszustwa transakcyjne: Weryfikacja klientów, monitorowanie transakcji, edukacja klientów w zakresie bezpieczeństwa, a także współpraca z odpowiednimi organami ścigania w przypadku wykrycia oszustw.
3. Problemy techniczne: Monitoring systemu, testy wydajności, utrzymanie infrastruktury, plan awaryjny, regularne kopie zapasowe danych oraz skuteczna komunikacja z klientami w przypadku przerw technicznych.
4. Nieuczciwe oceny i opinie: Weryfikacja ocen, monitorowanie i reagowanie na nieuczciwe opinie, otwarta komunikacja z klientami, polityka usuwania nieuczciwych ocen, nagradzanie klientów za wartościowe opinie i uwzględnianie ich feedbacku.

Wdrożenie tych strategii pomoże nam minimalizować ryzyko związane z wymienionymi zagrożeniami oraz utrzymać zaufanie klientów, reputację naszego sklepu i stabilność biznesową. Będziemy nadal monitorować i aktualizować nasze środki zarządzania ryzykiem, aby dostosować się do zmieniającego się środowiska i nowych zagrożeń.

Spis treści

[IDENTYFIKACJA POTENCJALNYCH ZAGROŻEŃ 2](#_Toc137292063)

[OCENA RYZYKA 2](#_Toc137292064)

[Atak Hackerski 2](#_Toc137292065)

[Oszustwa transakcyjne 2](#_Toc137292066)

[Problemy techniczne 3](#_Toc137292067)

[Problemami związanymi z ocenami i opiniami 3](#_Toc137292068)

[STRATEGIE ZARZĄDZANIA RYZYKIEM 4](#_Toc137292069)

[Ataki hackerskie: 4](#_Toc137292070)

[Oszustwa transakcyjne: 5](#_Toc137292071)

[Problemy techniczne 6](#_Toc137292072)

[Problemy związane z ocenami i opiniami: 7](#_Toc137292073)

[PODSUMOWANIE 8](#_Toc137292074)