PolishAPI

Rekomendacje dotyczące obszaru bezpieczeństwa dla podmiotów korzystających ze standardu

Dokument opracowany przez Grupę Projektową ds. PolishAPI

4 września 2019
Wersja 1.0

1 Spis treści

2 Wstęp

2.1 Kontekst

Nowa dyrektywa w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD2) wprowadza ramy prawne dla oferowania nowych usług płatniczych – usługi dostępu do informacji o rachunku, usługi inicjowania płatności oraz usługi potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej. Zarówno banki, jak i spółdzielcze kasy oszczędnościowo-kredytowe czy oddziały instytucji kredytowych, a także tzw. podmioty trzecie (TPP), będą mogły świadczyć nowe usługi w oparciu o przepisy PSD2 uzyskując dostęp do rachunków płatniczych prowadzonych on-line przez uprawnione do tego podmioty (ASPSP).

Świadczenie nowych usług płatniczych i udzielanie ich dostawcom dostępu do rachunków płatniczych wymaga jednakże zastosowania najwyższych środków bezpieczeństwa, które umożliwią w maksymalnym zakresie ograniczenie ryzyka ujawnienia poufnych danych osobom nieuprawnionym czy powstania innych incydentów bezpieczeństwa.

W tym celu został opracowany wspólny, uniwersalny standard API (dla którego używana jest nazwa PolishAPI) dla wszystkich podmiotów biorących udział w komunikacji w ramach świadczenia nowych usług, tj. TPP i ASPSP. Zgodnie z zapisami rozdziału 6 dokumentacji standardu PolishAPI (Bezpieczeństwo informacji), Grupa Projektowa PolishAPI została zobowiązana do opracowania dodatkowego szczegółowego dokumentu, obejmującego m.in. kwestie bezpieczeństwa implementacji, operacji i utrzymania systemów opartych na PolishAPI. Niniejszy dokument stanowi wypełnienie tego zobowiązania.

W dokumencie uwzględniono zapisy następujących regulacji oraz wytycznych:

1) Dyrektywy 2007/64/WE Parlamentu Europejskiego i Rady 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (znowelizowana dyrektywa w sprawie usług płatniczych, PSD2),
2) Rozporządzenia Delegowanego w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (RTS), opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 13 marca 2018 roku,
3) Wytycznych w sprawie wymogów zgłaszania nadużyć finansowych na podstawie art. 96 ust. 6 drugiej dyrektywy w sprawie usług płatniczych (PSD2),
4) Wytycznych dotyczących zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2),
5) Wytycznych w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (PSD2),
6) Opinia Europejskiego Nadzoru Bankowego w sprawie wykorzystania certyfikatów eIDAS w ramach RTS dla SCA oraz CSC.

2.2 Struktura dokumentu

Dokument składa się z czterech części dotyczących następujących obszarów:

1) Obszar 1: Wymagania organizacyjne i procesowe
2) Obszar 2: Wymagania dla infrastruktury systemu
3) Obszar 3: Wymagania dla interfejsu PolishAPI
4) Obszar 4: Przeciwdziałanie nadużyciom i atakom.

2.3 Zastosowanie dokumentu

Wszystkie wymagania przedstawione w niniejszym dokumencie dotyczą wyłącznie elementów związanych z funkcjonalnością interfejsu PolishAPI o ile szczegółowe zapisy nie mówią inaczej.

Niniejszy dokument ma zastosowanie do dostawców usług płatniczych wykorzystujących standard PolishAPI, tj. zarówno TPP jak i ASPSP (łącznie jako "PSP").

2.4 Założenia

1) PSP mogą, wedle własnego uznania i przeprowadzonej oceny ryzyka oraz na własną odpowiedzialność, podjąć decyzję o zastosowaniu się do przedstawionych tutaj rekomendacji i wymagań, w całości lub części.
2) Niniejszy dokument nie stanowi także opinii prawnej.

3 Definicje

Access token – ciąg znaków, stanowiący techniczną reprezentację sesji komunikacyjnej, o ustalonym czasie ważności, nawiązanej pomiędzy TPP i ASPSP w kontekście ściśle określonego PSU i dla ściśle określonego zakresu usług i zasobów po stronie ASPSP, do których TPP uzyskał dostęp.

Aktywa – wszystko, co ma wartość dla organizacji [ISO/IEC 13335- 1:2004]. Można wyróżnić dwa rodzaje aktywów:

- Aktywa podstawowe:
  - Procesy i działania biznesowe
  - Informacje
- Aktywa wspierające (wszystkich rodzajów):
  - Sprzęt
  - Oprogramowanie
  - Sieć
  - Personel
  - Siedziba
  - Struktura organizacyjna

Bezpieczny kanał komunikacyjny – mechanizm komunikacji zapewniający poufność, integralność oraz dostępność danych.

Dane Chronione – zbiory wrażliwych informacji, mogących stanowić szczególnie chronione informacje obejmujące:

- dane uwierzytelniające i autoryzacyjne,
- dane transakcyjne (informacje o transakcjach finansowych wykonanych w ramach interfejsu PolishAPI: kwoty, opisy oraz nazwy stron transakcji),
- dane bankowe (informacje o rachunkach bankowych i ich saldach),
- dane osobowe (dane identyfikujące osoby zgodnie z ustawą o ochronie danych osobowych),
- klucze kryptograficzne (np. wszelkie klucze prywatne występujące w środowisku oraz klucz publiczny do certyfikatu TLS w przypadku użycia obustronnego uwierzytelnienia w tym protokole - w zakresie jego integralności)
- informacje o wewnętrznej strukturze systemu (architektura wewnętrznych baz danych po stronie serwerowej, format komunikatów przesyłanych pomiędzy systemami wewnętrznymi oraz nazwy obiektów wewnętrznych).

EAT (External Authorization Tool) – zewnętrzne narzędzie autoryzacyjne, będące systemem zapewniającym procedurę SCA czyli silnego uwierzytelnienia PSU.

Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria zdarzeń nieplanowanych przez dostawcę usług płatniczych, które mają lub prawdopodobnie będą mieć niekorzystny wpływ na integralność, dostępność, poufność, autentyczność, uwierzytelnienie i/lub ciągłość świadczenia usług płatniczych [ISO/IEC TR 18044:2004].

Media Chronione – fizyczne nośniki informacji zawierające Dane Chronione.

OAuth2 – otwarty standard autoryzacji. Pozwala dzielić zasoby przechowywane w jednej aplikacji z inną aplikacją bez konieczności zagłębiania się w obsługę ich poświadczeń. W wyniku autoryzacji w standardzie OAuth2 zapewniany jest dostęp do zasobów pomiędzy aplikacjami.

Serwery frontend – część infrastruktury PolishAPI dostępna w publicznej sieci.

Serwery backend – część infrastruktury PolishAPI niedostępna w sieci publicznej.

SCA (Strong Customer Authentication, silne uwierzytelnienie klienta) – uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów (składników) należących do co najmniej dwóch różnych kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Standard – standard PolishAPI.

Środowisko Danych – środowisko zawierające Dane Chronione.

TS 119 495 – specyfikacja techniczna normy odnoszącej się do profilu certyfikatów kwalifikowanych na potrzeby dyrektywy w sprawie usług płatniczych (*Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU*).

Użytkownik – użytkownik rachunku płatniczego, którego dotyczą transakcje realizowane za pośrednictwem PolishAPI (tzw. PSU – Payment Service User).

Wrażliwe obszary – obszary zawierające Dane Chronione, wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji, np. data center.

XS2A (Access to Account) – interfejs pomiędzy TPP a ASPSP umożliwiający dostęp do rachunków płatniczych i wykorzystywany do wykonywania usług realizowanych w ramach PolishAPI.

Zdarzenie operacyjne – jest określoną zmianą stanu systemu, usługi lub sieci, która wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem [ISO/IEC TR 18044:2004]

3.1 Określenia używane do ustalenia priorytetu wymagań:

Pisane wielkimi literami słowa kluczowe „MUSI", „MOŻE", „POWINNO" i ich warianty, odmiana oraz formy zaprzeczone, mają być interpretowane tak jak opisano poniżej:

- MUSI, WYMAGANE, NIE WOLNO, NIE MOŻE: Te słowa kluczowe oznaczają bezwzględne wymaganie. Takie wymaganie musi być zaimplementowane we wszystkich systemach, które obejmuje standard.
- POWINNO, REKOMENDOWANE, NIE POWINNO, NIEREKOMENDOWANE: Te słowa oznaczają mocną rekomendację. Brak spełnienia wymagania opatrzonego zwrotem „POWINEN" dopuszczalny jest tylko w jawnie opisanych i uzasadnionych przypadkach. Konieczne jest przeprowadzenie analizy skutków niewypełnienia zalecenia i związanych z tym ryzyk.
- MOŻE, OPCJONALNIE, NIE MUSI, NIEWYMAGANE: Te słowa kluczowe oznaczają możliwość opcjonalnego wdrożenia zalecenia. Ponadto niewdrożenie takich zaleceń nie musi być uzasadniane ani dokumentowane.

4 Obszar 1: Wymagania organizacyjne i procesowe

4.1 Polityka bezpieczeństwa informacji

Cel: Podmiot korzystający z PolishAPI MUSI mieć zatwierdzoną przez najwyższe kierownictwo organizacji, wprowadzoną i regularnie aktualizowaną politykę bezpieczeństwa informacji, która definiuje wszystkie obowiązki w zakresie bezpieczeństwa informacji oraz jednoznacznie przypisuje te obowiązki wyznaczonym komórkom/jednostkom.

Podmiot korzystający z PolishAPI MUSI:

1. Posiadać zdefiniowane, opublikowane wobec swoich pracowników i współpracowników oraz współpracujących firm zewnętrznych, zatwierdzone przez najwyższe kierownictwo, utrzymywane i rozpowszechniane polityki bezpieczeństwa.
2. Zadbać o przestrzeganie w organizacji i w podmiotach współpracujących procedur w zakresie zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa, w tym bezpieczeństwa teleinformatycznego, a także o skuteczne wdrożenie mechanizmów kontroli i bieżącej oceny środków ograniczających ryzyko operacyjne i ryzyko naruszenia bezpieczeństwa w zakresie świadczenia usług płatniczych.
3. Dokonywać regularnych przeglądów procedur i polityk bezpieczeństwa oraz aktualizować je w związku ze zmianami istotnymi z punktu widzenia organizacji.

4.2 Organizacja bezpieczeństwa informacji

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone polityki dotyczące zarządzaniem bezpieczeństwem informacji wewnątrz organizacji oraz wymiany informacji z podmiotami zewnętrznymi.

Podmiot korzystający z PolishAPI MUSI:

1. Przypisać obowiązki i role zarządzania bezpieczeństwem informacji wyznaczonym komórkom/jednostkom organizacji, w szczególności:
   - Zdefiniowanie, udokumentowanie, zatwierdzanie i rozpowszechnianie polityk i procedur bezpieczeństwa;
   - Monitorowanie i analiza alarmów bezpieczeństwa i informacji oraz rozpowszechnianie do odpowiednich komórek/jednostek organizacji;
   - Zdefiniowanie, udokumentowanie i rozpowszechnianie procedury reakcji na zdarzenia operacyjne i incydenty bezpieczeństwa w celu zapewnienia niezwłocznego i efektywnego postępowania;
   - Zarządzanie kontami użytkowników, w tym dodawanie, modyfikowanie i usuwanie;
   - Monitorowanie i kontrola dostępu do danych;
   - Utrzymywanie należytego kontaktu z odpowiednimi organami, w tym w szczególności Komisją Nadzoru Finansowego.
2. Zdefiniować i wdrożyć proces autoryzacji nowych środków przetwarzania informacji wprowadzanych do użycia, w szczególności systemów informatycznych i elementów sieci informatycznej.
3. Definiować wymogi dotyczące umów o zachowaniu poufności i dokonywać regularnie ich przeglądów pod kątem zapewniania ochrony informacji adekwatnej do aktualnych potrzeb organizacji.

4. Definiować wymogi bezpieczeństwa dotyczące umów ze stronami trzecimi (w tym dostawcami systemów IT), w szczególności dotyczącymi dostępu, przetwarzania lub zarządzania informacjami organizacji w sieciach i systemach informatycznych.
5. Dokonywać regularnych niezależnych przeglądów systemu bezpieczeństwa.

4.3 Zarządzanie usługami dostarczanymi przez zewnętrznych dostawców

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożoną politykę i procedury zarządzania dostawcami usług, które będą pozwalały oszacować oraz ograniczać ryzyko związane z użyciem usług firm zewnętrznych.

Podmiot korzystający z PolishAPI MUSI:

1. Utrzymać i wdrażać polityki i procedury zarządzania dostawcami usług (w tym w szczególności w ramach outsourcingu), którzy mają wpływ na bezpieczeństwo Danych Chronionych, zgodnie z poniższymi wymaganiami:
   - Stworzenie i aktualizacja listy dostawców usług;
   - Weryfikacja przed nawiązaniem współpracy z dostawcami usług, czy spełniają oni wymagania Standardu;
   - Zapewnienie w umowach z podmiotami trzecimi zobowiązania do spełnienia przez te podmioty wymagań Standardu adekwatnie do zakresu świadczonych usług.
   - Realizacja programu przynajmniej corocznego monitorowania zgodności dostawcy usług z wymaganiami Standardu, adekwatnie do zakresu świadczonej usługi.

4.4 Zarządzanie aktywami (z punktu widzenia bezpieczeństwa informacji)

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone procesy związane z zarządzaniem aktywami (z punktu widzenia bezpieczeństwa informacji) obejmujące: inwentaryzację aktywów, określenie ich własności oraz ustalenie zasad akceptowalnego użycia, a także zasady klasyfikacji informacji, komponentów systemu oraz zarządzania nośnikami danych.

Przystępujący do korzystania z interfejsu PolishAPI, ASPSP MUSI, a TPP POWINIEN zapewnić:

1. Okresową inwentaryzację aktywów i jej dokumentację.
2. Przypisywanie i dokumentowanie własności aktywów dedykowanym pracownikom organizacji lub uprawnionym osobom z firm zewnętrznych.
3. Definiowanie i dokumentowanie zasady akceptowalnego użycia aktywów.
4. Wdrożenie i aktualizację dokumentacji czynności związanych z inwentaryzacją, przypisywaniem własności i określaniem zasad akceptowalnego użycia aktywów zgodnie z wewnętrznymi regulacjami organizacji.
5. Fizyczne zabezpieczenie wszystkich Mediów Chronionych (m.in urządzeń z pamięcią masową, nośników danych, drukowanych dokumentów itp.). Przechowywanie kopii zapasowych Mediów Chronionych w bezpiecznych lokalizacjach, preferencyjnie w miejscu zlokalizowanym poza siedzibą organizacji, w której fizycznie znajdują się te Media Chronione.
6. Utrzymanie ścisłej kontroli nad używaniem i dystrybuowaniem Mediów Chronionych zarówno wewnątrz jak i poza organizacją zgodnie z wdrożonymi w organizacji regulacjami, w tym:
   - Przesyłanie Mediów Chronionych bezpieczną metodą, w szczególności pozwalającą na dokładne śledzenie przesyłki;
7. Niszczenie Mediów Chronionych, które nie są już potrzebne do celów biznesowych czy z powodów prawnych. Niszczenie fizycznych nośników informacji (wydruki, płyty itp.) przy wykorzystaniu niszczarki, metod spalania czy innych metod mechanicznych/sprzętowych w

celu uniemożliwienia odtworzenia Danych Chronionych. Zabezpieczenie pojemników do przechowywania materiałów przeznaczonych do zniszczenia.

8. Udokumentowanie i wykorzystywanie polityk i procedur dotyczących ograniczenia fizycznego dostępu do Danych Chronionych.

4.5 Bezpieczeństwo fizyczne i środowiskowe

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone skuteczne zabezpieczenia przed nieautoryzowanym dostępem fizycznym do pomieszczeń, w których przetwarzane są Dane Chronione. MUSZĄ zostać zapewnione środki bezpieczeństwa środowiskowego dla systemu.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Wykorzystanie odpowiednich środków kontroli dostępu w celu ograniczenia i monitorowania fizycznego dostępu do systemów w Środowisku Danych:
   - Wykorzystanie kamer wideo i/lub mechanizmów kontroli dostępu w celu monitorowania fizycznego dostępu do Wrażliwych obszarów. Wymagane jest przechowywanie nagrań przynajmniej przez 3 miesiące, chyba że prawo nakazuje inaczej.
   - Gromadzenie logów z systemu kontroli dostępu oraz przechowywanie ich minimum przez okres 1 roku.
   - Wdrożenie fizycznych i/lub logicznych mechanizmów kontroli w celu ograniczenia dostępu do ogólnodostępnych gniazdek sieciowych.
   - Ograniczenie fizycznego dostępu do bezprzewodowych punktów dostępu, bram sieciowych, urządzeń przenośnych, sprzętu sieciowego i łączności, linii telekomunikacyjnych.
2. Ustanowienie procedur w celu ułatwienia rozróżniania gości od personelu:
   - Identyfikacja gości (np. plakietki, identyfikatory).
   - Unieważnienie dostępu byłym pracownikom lub dla nieważnych identyfikatorów gości.
   - Zapisy regulujące zmiany w wymaganiach dostępu dla gości.
3. Kontrolę fizycznego dostępu pracowników do wrażliwych lokalizacji poprzez:
   - Upoważnienie na dostęp zgodnie z obowiązkami wykonywanymi przez danego pracownika.
   - Bezzwłoczne unieważnienie dostępu pracownikom z chwilą zakończenia stosunku pracy oraz bezzwłoczny zwrot urządzeń/przedmiotów wykorzystywanych do kontroli dostępu (np. klucze, karty magnetyczne, identyfikatory, itp.).
4. Wdrożenie procedur identyfikacji gości i upoważnienia na ich dostęp:
   - Upoważnienie do dostępu gości przed wstępem, eskortowanie gości w czasie przebywania na obszarach, gdzie Dane Chronione są przetwarzane lub przechowywane.
   - Identyfikacja gości na podstawie plakietek lub innych identyfikatorów, które z czasem wygasają i pozwalają na wizualne odróżnienie od personelu.
   - Zwrot plakietek lub innych identyfikatorów przed opuszczeniem placówki lub w dniu wygaśnięcia.
   - Wykorzystywanie księgi gości lub rejestru elektronicznego do ewidencji gości uzyskujących dostęp do placówki, w której przechowywane są Dane Chronione. Konieczne jest udokumentowanie m.in.: imienia i nazwiska gościa, reprezentowanej firmy oraz nazwisko osoby upoważniającej do wstępu. Przechowywanie księgi przez minimum trzy miesiące chyba, że prawo stanowi inaczej.
5. Wdrożenie procedur ochrony przed zagrożeniami typu: powódź, zalanie, pożar, przegrzanie oraz innych form katastrof naturalnych lub spowodowanych przez człowieka.

4.6 Bezpieczna eksploatacja oraz zarządzanie zmianami

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone procedury bezpiecznej eksploatacji należących do niej komponentów interfejsu PolishAPI oraz zasady zarządzania zmianami w tych komponentach.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Separację środowisk służących do tworzenia/testowania oprogramowania od środowiska produkcyjnego oraz wykorzystanie kontroli dostępu użytkowników i innych systemów organizacji do tych środowisk.
2. Separację obowiązków osób biorących udział przy tworzeniu/testowaniu oprogramowania oraz zarządzających środowiskiem produkcyjnym, adekwatnie do aktualnie obowiązujących polityk bezpieczeństwa informacji w organizacji.
3. Ograniczenie wykorzystywania danych produkcyjnych do testów czy przy tworzeniu oprogramowania, a przy uzasadnionej konieczności takiego użycia, opracowanie i zastosowanie procedury przygotowania danych produkcyjnych do zastosowań testowych (np. anonimizacja danych, selekcja danych, dostęp do danych wyłącznie dla upoważnionych osób).
4. Usunięcie danych oraz kont testowych przed uruchomieniem produkcyjnym.
5. Usunięcie lub wyłączenie zbędnych usług, procesów, trasowań, połączeń sieciowych (tzw. hardening) na wszystkich komponentach systemu.
6. Procedury zarządzania zmianą dotyczące wdrożenia poprawek bezpieczeństwa oraz modyfikacji oprogramowania, które w zastosowaniu spowodują:
   - Wytworzenie udokumentowanej zmiany, zaakceptowanej przez upoważniony personel;
   - Wykonanie i udokumentowanie testów w celu weryfikacji, czy zmiana nie wpływa niekorzystnie na bezpieczeństwo systemu;
   - Wytworzenie procedury cofnięcia dokonanych zmian.

4.7 Kontrola dostępu

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone procedury zapewniające ograniczenie dostępu do danych chronionych wyłącznie do minimum wymaganego przez realizowane procesy biznesowe.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Ograniczenie dostępu do komponentów systemu i Danych Chronionych do grona osób, których zadania służbowe wymagają takiego dostępu:
   - Zdefiniowanie potrzeb dostępu dla każdej roli:
     a) Określenie komponentów systemu i źródeł danych, do których dostęp dla danej roli jest niezbędny,
     b) Wymagany do dostępu do źródeł poziom uprawnień (np. użytkownik, administrator itp.).
   - Ograniczenie użytkownikom posiadanych uprawnień do minimalnych, koniecznych do wykonywania powierzonych obowiązków służbowych zgodnie z zasadą *least privileges*.
   - Przyznawanie dostępu na podstawie indywidualnej klasyfikacji zadań i funkcji personelu
   - Wymaganie udokumentowanej (pisemnej lub elektronicznej) zgody autoryzowanego podmiotu na przyznanie uprawnień. Przydzielanie pracownikom danych uwierzytelniających (tzw. *credentiali*):
     a) przez zastosowanie formalnie ustanowionej i udokumentowanej procedury bezpieczeństwa.

b) z zachowaniem poufności, przy uprzedniej identyfikacji pracowników.
   - Użytkowanie przez pracowników danych uwierzytelniających (tzw. *credentiali*) w sposób ograniczający możliwość uzyskania do nich dostępu przez osoby nieupoważnione.
   - Zdefiniowanie, udokumentowanie, stosowanie i okresowy przegląd minimalnych wymagań wobec metod uwierzytelniania i danych uwierzytelniających, jakie organizacja może stosować w systemie (w szczególności tzw. polityki haseł).
2. Wykorzystanie systemu kontroli dostępu do komponentów systemu, który ogranicza dostęp na zasadzie "*need to know*" z domyślnym ustawieniem "*deny all*". System kontroli dostępu MUSI dostarczać:
   - Pokrycie wszystkich komponentów systemu, w tym sieci informatycznej i urządzeń sieciowych.
   - Przyznawanie dostępu poszczególnym osobom lub grupom osób na podstawie zadań i funkcji.
3. Udokumentowanie, wykorzystywanie i udostępnienie użytkownikom polityk i procedur bezpieczeństwa dotyczących ograniczenia dostępu do Danych Chronionych.
4. Poddawanie cyklicznym przeglądom polityk i procedur bezpieczeństwa dotyczących ograniczenia dostępu do Danych Chronionych.
5. Ustanowienie, udokumentowanie i realizację procesu regularnych przeglądów praw dostępu użytkowników do wszystkich komponentów interfejsu PolishAPI, pozostających w bezpośrednim zarzadzaniu organizacji.
6. Ustanowienie, udokumentowanie i realizację „polityki czystego biurka” i „polityki czystego ekranu” uwzględniających:
   - Konieczność przechowywania w poufności dokumentów papierowych, nośników danych, dokumentów elektronicznych wobec stron nieautoryzowanych (w tym nieautoryzowanych pracowników organizacji).
   - Konieczność bezzwłocznego niszczenia dokumentów papierowych, nośników danych, dokumentów elektronicznych, które nie wymagają dalszego przetwarzania w ramach systemu i które nie podlegają obowiązkowi przechowywania na podstawie obowiązujących przepisów prawa państwowego lub przepisów wewnętrznych organizacji.

4.8 Zapewnienie bezpieczeństwa w całym cyklu życia systemów informacyjnych

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone procedury zapewniające bezpieczeństwo informacji w całym cyklu życia systemów informacyjnych będących komponentami interfejsu PolishAPI, czyli na etapach pozyskiwania, rozwoju, utrzymania i wycofania z użycia tych systemów.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Aby wymagania biznesowe dotyczące nowych systemów informatycznych wchodzących w skład interfejsu PolishAPI lub jego rozszerzenia zawierały wymagania dotyczące bezpieczeństwa informacji i bezpieczeństwa IT.
2. Zabezpieczenie interfejsu PolishAPI przed nadużyciami związanymi z błędami w komponentach tego systemu, utratą i nieuprawnioną modyfikacją danych wejściowych i wyjściowych w nim przetwarzanych, w szczególności poprzez wieloetapowe testy i formalne odbiory poszczególnych funkcjonalności systemu.
3. Ochronę przed nieautoryzowanym dostępem oraz wersjonowanie kodu źródłowego komponentów systemu.
4. Ochronę poufności i integralności Danych Chronionych wraz z rozpoczęciem produkcyjnego użytkowania nowych komponentów systemu lub komponentów rozwijanych.

5. Nadzór nad pracami rozwojowymi interfejsu PolishAPI, powierzonymi firmie zewnętrznej.
6. Ustanowienie, udokumentowanie i realizację procesu zarządzania podatnościami komponentów interfejsu PolishAPI, w celu bezzwłocznej likwidacji tych podatności i ochrony przed narażeniem systemu na utratę dostępności, poufności lub integralności danych.
7. Bezpieczne tworzenie aplikacji (w tym dostęp administracyjny do aplikacji przez sieć):
   - Zgodnie ze Standardem (np. bezpieczne uwierzytelnianie i autoryzacja),
   - W oparciu o standardy branżowe oraz najlepsze praktyki,
   - Z wykorzystaniem technik bezpieczeństwa informacji w całym cyklu tworzenia oprogramowania.
8. Ocenę modyfikacji kodu przed instalacją produkcyjną lub przed przekazaniem użytkownikowi w celu zidentyfikowania potencjalnych luk (przy pomocy ręcznego lub automatycznego procesu) przynajmniej z uwzględnieniem czy:
   - Oceny modyfikacji kodu są przeprowadzane przez inne osoby niż te, które są ich twórcami, posiadające odpowiednią wiedzę na temat technik oceny kodu i praktyk bezpiecznego programowania,
   - Osoby oceniające zapewniają, że kod jest napisany zgodnie z wytycznymi bezpiecznego programowania, w szczególności z uwzględnieniem pkt. 4,
   - Wymagane poprawki są nanoszone przed udostępnieniem aplikacji,
   - Wyniki oceny kodu podlegają weryfikacji i akceptacji osób do tego uprawnionych przed udostępnieniem aplikacji.
9. Usuwanie często spotykanych błędów programistycznych zgodnie z zapisami aktualnej, publicznie dostępnej listy „OWASP TOP 10”, w tym:
   - Brak walidacji danych wejściowych i wyjściowych aplikacji, w szczególności podatność na ataki typu *injection*, np. SQL injection, code injection, OS injection.
   - Przepełnienie bufora.
   - Błędy szyfrowania danych.
   - Niezabezpieczona komunikacja danych.
   - Nieodpowiednie zarządzanie błędami.
   - Podatność na atak Cross-site scripting (XSS, skrypty międzyserwisowe)
   - Nieodpowiednia kontrola dostępu (np. niezabezpieczone bezpośrednie odwołania do obiektów, nieograniczony dostęp URL, nieograniczony dostęp użytkowników do funkcji).
   - Podatność na ataki Cross-site request forgery.
   - Niepoprawna obsługa uwierzytelniania i sesji.
10. Usuwanie wszystkich podatności krytycznego i wysokiego ryzyka zidentyfikowanych w procesie identyfikacji luk bezpieczeństwa.
11. Usunięcie kont programistów, testerów oraz pozostałych ID użytkowników i haseł zanim system zostanie uruchomiony w środowisku produkcyjnym.
12. Zminimalizowanie błędów poprzez zapewnienie szkolenia programistów w zakresie:
    a. bezpieczeństwa tworzonego oprogramowania,
    b. unikania powszechnych luk bezpieczeństwa,
    c. zrozumienia, jak wrażliwe dane są przetwarzane w pamięci.
13. Ciągła ochrona oraz identyfikowanie luk bezpieczeństwa aplikacji:
    - Ocena bezpieczeństwa aplikacji przy pomocy ręcznych przeglądów lub automatycznych narzędzi do oceny bezpieczeństwa, przynajmniej raz na rok,
    - Błędy uznane za krytyczne zgodnie z klasyfikacją stosowaną w organizacji MUSZĄ być usuwane niezwłocznie.
14. Oprogramowanie PolishAPI MUSI korzystać wyłącznie z bibliotek, które nie zawierają publicznie opublikowanych, istotnych podatności bezpieczeństwa. Wydawca oprogramowania PolishAPI MUSI na bieżąco monitorować publikowane informacje o podatnościach w bibliotekach, z jakich korzysta jego oprogramowanie. Czas pomiędzy opublikowaniem informacji o istotnej podatności bezpieczeństwa w takiej bibliotece, a wdrożeniem poprawki

w oprogramowaniu PolishAPI MUSI wynikać z analizy ryzyka i nie może przekraczać 3 miesięcy dla podatności wysokich.

4.9 Obsługa Zdarzeń operacyjnych i Incydentów bezpieczeństwa, w tym o charakterze teleinformatycznym

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone stosowne procedury zapewniające szybką, skuteczną i uporządkowaną reakcję na incydenty związane z bezpieczeństwem informacji w celu zminimalizowania szkód finansowych i reputacyjnych.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Stworzenie oraz skuteczne wdrożenie planu reakcji na Zdarzenie operacyjne i Incydent bezpieczeństwa dotyczący usług powiązanych z interfejsem PolishAPI – zapewniającego natychmiastowe działania w celu minimalizacji zasięgu i skutków Zdarzenia operacyjnego lub Incydentu bezpieczeństwa, zebrania materiału dowodowego oraz wyciągnięcia stosownych wniosków i wdrożenia adekwatnych zabezpieczeń. Plan POWINIEN przynajmniej:
   - Opisywać role, odpowiedzialności i strategię komunikacji i kontaktu na wypadek wystąpienia Zdarzenia operacyjnego oraz Incydentu bezpieczeństwa lub nawet jego podejrzenia,
   - Podawać szczegóły i czasy reakcji na każdy rodzaj Zdarzenia operacyjnego oraz Incydentu bezpieczeństwa,
   - Zawierać procedury odtworzenia/zapewnienia ciągłości biznesowej,
   - Definiować sposób raportowania działań podjętych podczas obsługi Zdarzenia operacyjnego oraz Incydentu bezpieczeństwa, w tym zewnętrznego raportowania poważnych Incydentów bezpieczeństwa,
   - Obejmować wszystkie komponenty systemu,
2. Cykliczne przeprowadzenie testu, weryfikacji i/lub aktualizacji planu reakcji.
3. Przypisanie personelu w celu reakcji i obsługi Zdarzeń operacyjnych i Incydentów bezpieczeństwa oraz zapewnienie jego dostępności na poziomie adekwatnym do skali i powagi odnotowanego Zdarzenia operacyjnego lub Incydentu bezpieczeństwa.
4. Zapewnienie odpowiednich szkoleń osobom odpowiedzialnym za reakcję na Zdarzenie operacyjne lub Incydent bezpieczeństwa.
5. Zdefiniowanie procesu modyfikacji i udoskonalania planu reakcji na Incydent bezpieczeństwa, mającego na celu uwzględnienie doświadczeń organizacji oraz postępu w branży.
6. Gromadzenie, przechowywanie i udostępnianie materiału dowodowego zgodnie z zasadami materiału dowodowego obowiązującymi w odpowiednim prawodawstwie (prawodawstwach).

4.10 Zarządzanie ciągłością działania

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone i regularnie testowane plany utrzymania ciągłości działania oraz odtwarzania działalności w zakresie funkcjonowania interfejsu PolishAPI

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Opracowanie i wdrożenie planów ciągłości na podstawie wyników analizy wpływu na biznes (Business Impact Analysis) oraz szacowania ryzyka.
2. Zachowanie jednolitej struktury planów, aby plany były ze sobą spójne.
3. Cyklicznie sprawdzanie skuteczności planu ciągłości działania.
4. Utrzymanie i testowanie planu ciągłości działania oraz, w razie konieczności, jego korektę i ponowną ocenę.

5. Utrzymywanie i aktualizację listy krytycznych dla organizacji procesów.
6. Zawarcie w planie ciągłości działania przynajmniej:
   - Listy procesów krytycznych wraz z przypisanymi priorytetami oraz czasami RTO/RPO,
   - Sposobu funkcjonowania organizacji w trakcie trwania sytuacji kryzysowej i po jej zakończeniu,
   - Struktury zarządzania kryzysowego wraz z określeniem ról i odpowiedzialności,
   - Komunikacji i współdziałania z podmiotami zewnętrznymi.
   - Powrotu do normalnej działalności

4.11 Polityki bezpiecznego użytkowania przez pracowników

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone polityki bezpiecznego użytkowania dla istotnych z punktu widzenia bezpieczeństwa technologii przez jej pracowników (np. zdalny dostęp, użycie urządzeń przenośnych, użycie sieci bezprzewodowych, itp.). Wprowadzenie nowych technologii w organizacji MUSI wymagać przeprowadzenia formalnego procesu (w szczególności poprzez proces zarządzania zmianami).

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Opracowanie i wdrożenie polityk wprowadzania nowych technologii wraz z definicjami poprawnego korzystania z tych technologii np. technologie zdalnego i bezprzewodowego dostępu, laptopy, tablety, inne przenośne urządzenia elektroniczne (np. pendrive), wykorzystanie e-maila i Internetu. Polityki wprowadzania nowych technologii MUSZĄ opisywać następujące obszary:
   - Zgoda autoryzowanego podmiotu
   - Zapewnienie uwierzytelnienia przy korzystaniu nowych technologii tam gdzie jest to zasadne
   - Zapewnienie mechanizmów kontroli dostępu do zasobów infrastruktury organizacji
   - Metoda szybkiej identyfikacji użytkownika wykorzystującego elementy infrastruktury organizacji
   - Dopuszczalne sposoby wykorzystania technologii
   - Lista technologii dopuszczonych do użytku
2. Zakaz kopiowania, przenoszenia i przechowywania Danych Chronionych na urządzenia przenośne bez mechanizmów zapewniających zachowanie poufności.

4.12 Bezpieczeństwo zasobów ludzkich

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone polityki związane z bezpieczeństwem zasobów ludzkich minimalizujące ryzyka dla bezpieczeństwa informacji wynikające z rekrutacji nowych pracowników, wykonywania przez nich obowiązków służbowych oraz związane z zakończeniem przez nich pracy lub zmianą stanowiska.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Wdrożenie formalnego programu budowania świadomości personelu nt. bezpieczeństwa informacji, mającego na celu uświadomienie ważności bezpieczeństwa Danych Chronionych. Proces ten MUSI uwzględniać:
   a. Dokonywanie szczegółowej weryfikacji kandydatów na pracowników organizacji, z zachowaniem należytej staranności przed ich zatrudnieniem, zgodnie z obowiązującym prawem w celu minimalizacji ryzyka.
   b. Szkolenie personelu po zatrudnieniu i przynajmniej raz w roku, odpowiednio do powierzonych obowiązków służbowych i poziomu uprawnień dostępu.

c. Potwierdzanie przez personel zapoznania się i rozumienia procedur i polityk bezpieczeństwa organizacji.

4.13 Zarządzanie ryzykiem oraz testy bezpieczeństwa

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożony proces regularnego przeprowadzania analizy, ograniczania i akceptowania ryzyka oraz testowania bezpieczeństwa należących do niej komponentów interfejsu PolishAPI.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Wdrożenie procesu identyfikacji luk bezpieczeństwa przy wykorzystaniu rzetelnych źródeł informacji oraz stworzenie klasyfikacji poziomu ryzyk w celu opisywania nowo odkrytych luk.
2. Ochronę wszystkich komponentów systemu przed znanymi zagrożeniami bezpieczeństwa poprzez instalowanie odpowiednich poprawek dostawcy w terminie wynikającym z klasyfikacji aplikacji pod względem poziomu ryzyka biznesowego oraz zidentyfikowanej luki.
3. Wdrożenie cyklicznego procesu sprawdzania obecności nieautoryzowanych urządzeń w sieci wewnętrznej, w tym bezprzewodowych punktów dostępu (802.11).
4. Uruchomienie wewnętrznych i zewnętrznych (z Internetu) skanów infrastruktury organizacji („*vulnerability scan*") przynajmniej raz na rok i po wszystkich istotnych zmianach w sieci (np. instalacji nowych elementów systemu, zmian w topologii sieci, aktualizacji produktów) wraz z korektami i niezbędnymi powtórzeniami, aż wszystkie problemy wysokiego i krytycznego ryzyka będą rozwiązane.
5. Realizację testów penetracyjnych komponentów interfejsu PolishAPI w oparciu o zalecenia OWASP (lub wypracowane własne podejście do testów) i/lub branżowe metodyki testowania bezpieczeństwa przynajmniej raz w roku oraz po każdej znaczącej modyfikacji lub aktualizacji infrastruktury lub aplikacji.
6. Wykonywanie testów penetracyjnych przynajmniej raz w roku oraz każdorazowo po istotnej zmianie w infrastrukturze PolishAPI mającej wpływ na mechanizmy segmentacji lub separacji na poziomie sieci w celu weryfikacji, czy Środowisko Danych jest skutecznie odizolowane od innych sieci.
7. Wykorzystanie technik wykrywania włamań i/lub technik zapobiegania włamaniom (systemy IDS/IPS). Monitorowanie całego ruchu na obrzeżach Środowiska Danych i alarmowanie personelu w przypadku podejrzenia kompromitacji. Aktualizowanie wszystkich silników wykrywania i zapobiegania włamaniom w krótkim czasie po ukazaniu się aktualizacji.
8. Udokumentowanie, wykorzystywanie, uaktualnianie polityk i procedur monitorowania i testów bezpieczeństwa

4.14 Przeciwdziałanie praniu pieniędzy

Cel: Podmiot korzystający z PolishAPI MUSI mieć wdrożone polityki związane z przeciwdziałaniem praniu pieniędzy.

Podmiot korzystający z PolishAPI MUSI przestrzegać zapisów Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 2018.03.01 (Dz. U. 2018 poz. 723 z późn. zm.), w zakresie wymaganym przez tę Ustawę.

4.15 Informowanie Użytkowników o zasadach bezpieczeństwa

Cel: Podmiot korzystający z PolishAPI MUSI informować swoich klientów o zasadach bezpiecznego użytkowania interfejsu PolishAPI oraz uświadamiać klientów o istniejących zagrożeniach w tym zakresie.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Udostępnienie klientom przynajmniej jednego Bezpiecznego kanału komunikacyjnego (np. dedykowana strona www) do celów komunikacji związanej z prawidłowym i bezpiecznym wykorzystywaniu interfejsu PolishAPI, a w tym kanale Klient POWINIEN zostać powiadomiony o następujących kwestiach:
   - Że każdy inny sposób komunikacji może wiązać się z próbą oszustwa,
   - Przebieg procesu zgłaszania przez klienta podejrzanych transakcji (fraudów), podejrzanych zdarzeń lub anomalii w czasie sesji usługi płatności czy podejrzenia o stosowanie metod socjotechniki,
   - Przebieg odpowiedzi na zgłoszenie klienta,
   - Przebieg procesu powiadamiania klienta o potencjalnych fraudach i ostrzeganiu o atakach.
2. Informowanie klienta o aktualizacjach procedur bezpieczeństwa poprzez Bezpieczny kanał komunikacyjny, podobnie jak powiadomienia o nowych zagrożeniach (np. informacja o próbach wyłudzenia informacji).
3. Udostępnienie wsparcia klienta w przypadku pytań, skarg i reklamacji, zgłoszeń nieautoryzowanych transakcji płatniczych, potrzeby uzyskania pomocy technicznej, powiadomień o nietypowych sytuacjach, potrzeby zgłaszania incydentów związanych z usługami płatniczymi i usług powiązanych.
4. Udostępnienie klientowi niżej wymienionych informacji związanych z płatnościami:
   - Wymagania dotyczące oprogramowania i innych niezbędnych narzędzi (np. oprogramowanie antywirusowe, firewall),
   - Wskazówki dotyczące prawidłowego i bezpiecznego korzystania z poświadczeń służących uwierzytelnianiu,
   - Szczegółowy opis kolejnych kroków procedury wykonania i autoryzowania transakcji płatniczej oraz uzyskania informacji, w tym konsekwencje każdej czynności,
   - Wskazówki dotyczące prawidłowego i bezpiecznego korzystania ze sprzętu i oprogramowania dostarczonego klientowi,
   - Procedura postępowania na wypadek kradzieży lub zagubienia poświadczeń służących uwierzytelnianiu, sprzętu lub oprogramowania, służących do logowania się i przeprowadzania transakcji,
   - Procedura postępowania w przypadku, gdy klient wykryje lub podejrzewa incydent bezpieczeństwa lub incydent operacyjny,
   - Opis odpowiedzialności stron w kontekście korzystania z usług realizowanych poprzez interfejs PolishAPI.
   - W przypadku TPP – opis kroków, jakie należy podjąć celem zainicjowania przez samego klienta procesu wyłączenia usług.
   - Opis warunków blokowania transakcji klienta, powiadamiania go o tym fakcie i sposobu jej wyłączenia.
5. Poinformowanie Użytkownika o tym, że w sytuacjach zagrożenia bezpieczeństwa transakcji, pojedyncze transakcje lub usługa płatności mogą być blokowane. Jednocześnie MUSI zostać określona metoda i warunki powiadamiania klienta o blokadzie i sposobie jej wyłączenia.

6. Prowadzenie programu edukacji i poprawy świadomości Użytkowników na temat bezpieczeństwa, mającego na celu pomoc w zrozumieniu potrzeb dotyczących:
   - Ochrony danych uwierzytelniających oraz wszelkich poufnych danych,
   - Zarządzania bezpieczeństwem oprogramowania poprzez instalowanie i aktualizacje komponentów bezpieczeństwa (np. antywirusów, poprawek bezpieczeństwa itp.),
   - Unikania zagrożeń związanych z pobieraniem i instalowaniem oprogramowania pochodzącego z niezaufanych źródeł.

5 Obszar 2: Wymagania dla infrastruktury systemu

5.1 Konfiguracja sieciowa

Cel: Podmiot korzystający z PolishAPI MUSI izolować Serwery backend systemu od sieci publicznych, oraz MUSI zapewniać użycie sieciowych systemów wykrywania lub przeciwdziałania włamaniom.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Zastosowanie konfiguracji sieciowej ograniczającej połączenia pomiędzy niezaufanymi (znajdującymi się poza kontrolą organizacji) sieciami a Środowiskiem Danych
   - Ograniczenie ruchu przychodzącego i wychodzącego, niezbędnego dla Środowiska Danych, w szczególności zablokowanie wszelkiego nieuzasadnionego potrzebami biznesowymi ruchu sieciowego.
   - Zabezpieczenie plików konfiguracji urządzeń sieciowych.
2. Zabezpieczenie przed nieautoryzowanym dostępem do Środowiska Danych z sieci bezprzewodowych np. poprzez
   - blokowanie ruchu sieciowego z sieci bezprzewodowych do Środowiska Danych, poza tym, który jest niezbędny z punktu widzenia wymagań biznesowych
   - silne uwierzytelnianie dostępu (dwuskładnikowe) do sieci bezprzewodowych
   - fizyczne ograniczenie dystrybucji sygnału sieci bezprzewodowych
   - wykorzystanie systemów kontroli dostępu do sieci (Network Access Control)
3. Uniemożliwienie bezpośredniego połączenia pomiędzy Internetem a każdym komponentem systemu w Środowisku Danych, z wyłączeniem urządzeń infrastruktury brzegowej (na styku z Internetem), dedykowanej do tego celu:
   - Zastosowanie stref zdemilitaryzowanych (DMZ), w szczególności w celu ograniczenia ruchu przychodzącego tylko do tych niezbędnych komponentów i usług systemu, które zostały zatwierdzone do udostępnienia.
   - Uniemożliwienie bezpośrednich połączeń przychodzących i wychodzących dla ruchu pomiędzy Internetem a Środowiskiem Danych.
   - Wykorzystanie technik anty-spoofingowych w celu wykrycia i zablokowania sfałszowanych źródłowych adresów IP.
   - Zablokowanie nieautoryzowanego ruchu wychodzącego ze Środowiska Danych do Internetu.
   - Wykorzystanie dynamicznego filtrowania pakietów (SPI - *Stateful Packet Inspection*: tylko już "ustanowione" połączenia są wpuszczane do sieci)
   - Umieszczenie komponentów systemu przechowujących Dane Chronione (takich jak bazy danych) w strefie sieci wewnętrznej, odseparowanej od niezaufanych sieci, w szczególności sieci, z których i do których ruch z Internetu przychodzi bezpośrednio.
   - Dodatkowo komponenty systemu POWINNY być separowane wewnątrz sieci na zasadzie minimalnego dostępu, wymaganego do realizacji potrzeb biznesowych.
   - Utrzymanie w tajemnicy przed nieuprawnionymi osobami prywatnych adresów IP oraz informacji o routingu.

5.2 Konfiguracja serwerów, urządzeń oraz oprogramowania

Cel: Podmiot korzystający z PolishAPI MUSI zapewniać aktualność oprogramowania, minimalizować ryzyko związane ze złośliwym oprogramowaniem i nieautoryzowanym dostępem, zapewniać monitorowanie zdarzeń oraz uwzględniać rozdzielność środowisk produkcyjnych od testowych.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Zmianę domyślnych ustawień dostępowych zawartych w konfiguracji dostawcy oraz usunięcie lub dezaktywację zbędnych kont domyślnych przed instalacją systemu w sieci. Dotyczy to wszystkich domyślnych haseł m.in. do systemów operacyjnych, oprogramowania dostarczającego usługi bezpieczeństwa, aplikacji i kont systemowych, terminali POS, SNMP community strings itd.
2. Dla środowisk bezprzewodowych podłączonych do Środowiska Danych lub przesyłających Dane Autoryzacyjne, zmiana wszystkich domyślnych ustawień przy instalacji m.in. domyślnych kluczy kryptograficznych, haseł, haseł SNMP (community strings)
3. Ustanowienie standardu konfiguracji dla wszystkich komponentów systemu z uwzględnieniem znanych luk bezpieczeństwa oraz zgodności z uznanymi w branży standardami hardeningu systemu, np. Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST).
   - Wdrożenie tylko jednej głównej funkcji na pojedynczej instancji systemu operacyjnego w celu zapobiegania współistnienia funkcji wymagających wykorzystania różnych poziomów bezpieczeństwa (np. serwisy bazodanowe, webowe, DNS wdrożone na osobnych serwerach)
   - Uruchomienie tylko niezbędnych dla funkcjonowania systemu usług, protokołów, demonów itp.
   - Rozdział komponentów interfejsu PolishAPI na warstwę danych, warstwę kontrolera oraz warstwę prezentacyjną.
   - Wdrożenie dodatkowych zabezpieczeń dla wszystkich niezbędnych usług, protokołów i demonów uważanych za niezabezpieczone, np. wykorzystanie technologii gwarantujących poufność i integralność, jak SSH, SFTP, TLS czy IPSec w celu ochrony niezabezpieczonych usług jak np. NetBIOS, Telnet, FTP itp.
   - Konfiguracja parametrów bezpieczeństwa systemu zapobiegająca błędnemu użyciu.
   - Usunięcie lub zablokowanie wszystkich zbędnych funkcjonalności takich jak: skrypty, sterowniki, dodatki, podsystemu, serwery plików, zbędne serwery webowe.
4. Szyfrowanie wszelkiego zdalnego dostępu administracyjnego z wykorzystaniem silnej kryptografii. Wykorzystanie technologii takich jak SSH, VPN czy TLS do zarządzania z poziomu sieci web czy innego typu zdalnego dostępu.
5. Utrzymanie aktualnej dokumentacji architektury komponentów i powiązań systemów podlegających pod interfejs PolishAPI.
6. Udokumentowanie, wykorzystywanie i udostępnienie zainteresowanym stronom polityk i procedur, parametrów bezpieczeństwa służącym zarządzaniu i implementowaniu rozwiązań informatycznych
7. Oprogramowanie antywirusowe zainstalowane na wszystkich systemach narażonych na złośliwe oprogramowanie, w szczególności komputerach osobistych i serwerach.
   - Oprogramowanie antywirusowe MUSI być zdolne do wykrywania, usuwania złośliwego oprogramowania.
   - Dla systemów, na których stosowanie systemów antywirusowych jest z obiektywnych przyczyn niemożliwe lub bezzasadne, przeprowadzenie cyklicznej oceny celem identyfikacji i oceny ryzyka pod kątem potwierdzenia czy te systemy nadal nie wymagają stosowania oprogramowania antywirusowego
8. Mechanizmy antywirusowe:
   - Są aktualne,
   - Wykonują okresowe skanowanie w poszukiwaniu złośliwego oprogramowania,
   - Generują logi do celów audytowych.
9. Mechanizmy antywirusowe działają w sposób ciągły i nie mogą zostać zdezaktywowane przez użytkowników.

10. Udokumentowanie, wykorzystywanie i udostępnienie zainteresowanym stronom polityk i procedur bezpieczeństwa dotyczących ochrony systemów przed złośliwym oprogramowaniem.

5.3 Kontrola dostępu logicznego

Cel: System MUSI zapewniać identyfikację użytkowników i rozliczalność działań oraz zarządzanie użytkownikami i uprawnieniami zgodnie z zasadami minimalnego dostępu.

Podmiot korzystający z PolishAPI MUSI:

1. Zapewnić ograniczenie dostępu do komponentów interfejsu PolishAPI i Danych Autoryzacyjnych do grona osób, których zadania służbowe wymagają takiego dostępu.
2. Zdefiniować wymogi dostępu dla każdej roli:
   - Określić komponenty systemu i źródeł danych, do których dostęp dla danej roli jest niezbędny.
   - Określić wymagany do dostępu do źródeł danych poziom uprawnień (np. użytkownik, administrator itp.).
   - Uprawnienia użytkowników ograniczyć do minimalnego zakresu niezbędnego do wykonywania obowiązków służbowych.
   - Przyznawać dostęp na podstawie indywidualnej klasyfikacji zadań i funkcji personelu.
   - Wymagać udokumentowanej (pisemnej lub elektronicznej) zgody autoryzowanego podmiotu na przyznanie uprawnień.
   - Stosować zasadę separacji „*Segregation Of Duties*”.
3. Wykorzystywać system kontroli dostępu do komponentów systemu, który ogranicza dostęp na zasadzie "*need to know*" z domyślnym ustawieniem "*deny all*".
   System kontroli dostępu MUSI zawierać:
   - Pokrycie wszystkich komponentów systemu
   - Przyznawanie dostępu poszczególnym osobom na podstawie zadań i funkcji
   - Domyślne ustawienie "*deny all*"
4. Udokumentować, wykorzystywać i udostępniać zainteresowanym stronom polityki i procedury bezpieczeństwa dotyczących ograniczenia dostępu do Danych Autoryzacyjnych

5.4 Przetwarzanie Danych Chronionych po stronie serwerowej

Cel: Dane chronione MUSZĄ być zabezpieczone zgodnie z przyjętą krytycznością w obszarze integralności i poufności w trakcie przechowywania, transportu, modyfikacji, usuwania.

Podmiot korzystający z PolishAPI MUSI zapewnić:

1. Zapewnienie integralności i poufności Danych Chronionych na całej drodze ich przesyłania.
2. Dostęp do Danych Chronionych jest logowany, w sposób zapewniający ślad audytowy, przynajmniej w zakresie umożliwiającym możliwość identyfikacji uzyskującego dostęp personelu lub elementu infrastruktury informatycznej.
3. Modyfikacja Danych Chronionych jest możliwa jedynie przez uprzednio uwierzytelniony i autoryzowany personel.
4. Usuwanie danych z nośników realizowane w sposób uniemożliwiający ich odtworzenie.
5. Dane Autoryzacyjne mogą być przechowywane przez Podmiot korzystający z PolishAPI jedynie przez czas niezbędnie wymagany do obsługi procesu płatności i reklamacji.

Podmiot korzystający z PolishAPI MUSI dołożyć wszelkich starań, aby zagwarantować integralność oraz poufność Danych Chronionych przetwarzanych w infrastrukturze.

5.5 Zarządzanie kluczami kryptograficznymi

Cel: System MUSI zapewniać bezpieczeństwo kluczy kryptograficznych w całym ich cyklu życia.

Podmiot korzystający z PolishAPI MUSI:

1. Wdrożyć zasady korzystania z zabezpieczeń kryptograficznych.
2. Wdrożyć zasady zarządzania kluczami, które umożliwią korzystanie z technik kryptograficznych, zawierające przynajmniej:
    - Generowanie klucza.
    - Przechowywanie oraz kopie zapasowe kluczy.
    - Cel użycia klucza.
    - Długość klucza.
    - Czas życia klucza.
    - Dystrybucja klucza.
    - Wymiana klucza.
    - Usuwanie i archiwizacja klucza.

5.6 Zapewnienie wysokiej dostępności usług

Cel: System MUSI zapewniać wysoką dostępność usług zgodnie z przyjętą klasyfikacją krytyczności, w szczególności poprzez redundancję komponentów, wykonywanie kopii zapasowych danych i oprogramowania oraz automatyczne podtrzymywanie ciągłości pracy systemu.

Podmiot korzystający z PolishAPI MUSI:

1. Zapewnić dostępność usług systemu zgodnie przyjętymi warunkami SLA zawartymi w umowach oraz wynikami analizy ryzyk przeprowadzonej przez Podmiotu korzystającego z PolishAPI.

6 Obszar 3: Wymagania dla interfejsu PolishAPI

6.1 Uwierzytelnienie i autoryzacja w ramach PolishAPI

Cel: Dostęp do usług interfejsu PolishAPI MUSI być możliwy jedynie dla uprawnionego Podmiotu korzystającego z PolishAPI oraz Użytkownika. Sposób uwierzytelnienia Podmiotu korzystającego z PolishAPI i Użytkownika oraz autoryzacji ich działań MUSI zapewniać minimalizację ryzyka nieautoryzowanego dostępu.

1. Podmioty korzystające z PolishAPI MUSZĄ zostać poprawnie uwierzytelnione przed udzieleniem im dostępu do interfejsu XS2A. Błędy uwierzytelnienia MUSZĄ skutkować odmową dostępu do interfejsu XS2A.
2. Uwierzytelnienie MUSI nastąpić w oparciu o certyfikaty klucza publicznego w procesie wzajemnego uwierzytelnienia („*Mutual authentication*") za pomocą protokołu TLS 1.2+.
3. Podmioty korzystające z PolishAPI MUSZĄ posiadać ważny certyfikat, służący do wzajemnej identyfikacji w interfejsie XS2A, otrzymany od kwalifikowanego dostawcy usług zaufania, spełniającego wymogi regulacyjne w obszarze usług zaufania oraz identyfikacji elektronicznej. Certyfikat ten MUSI spełniać wymagania zdefiniowane w RTS oraz specyfikacji technicznej ETSI (TS 119 495). Podmioty korzystające z PolishAPI MUSZĄ każdorazowo w ramach procesu uwierzytelnienia zweryfikować ważność (przy wykorzystaniu protokołu OCSP lub listy CRL) wszystkich certyfikatów znajdujących się na ścieżce certyfikacji.
4. TPP MUSI być zarejestrowane w przynajmniej jednym rejestrze w kraju członkowskim Unii Europejskiej w roli, w której chce występować podczas realizacji komunikacji opartej na standardzie PolishAPI. ASPSP POWINNO zweryfikować status rejestracji TPP w ramach procedury uwierzytelnienia.
5. Autoryzacja TPP MUSI być oparta na modelu RBAC (*Role Based Access Control*), w którym poziom i zakres dostępu do poszczególnych zasobów API zależy od roli Podmiotu korzystającego z PolishAPI.
6. Użycie poszczególnych metod w ramach interfejsu PolishAPI MUSI być autoryzowane w taki sposób, aby uprawnienia były zależne od roli Podmiotu korzystającego z PolishAPI i zakresu udzielonych mu przez Użytkownika zgód. W szczególności, poziom i zakres autoryzacji POWINIEN być różny dla TPP w zależności od zakresu ich uprawnień.
7. Użytkownik (PSU) MUSI zostać uwierzytelniony po stronie ASPSP lub w zewnętrznym narzędziu autoryzacyjnym (EAT).
8. Uwierzytelnienie Użytkownika (PSU) MUSI zostać przeprowadzone z wykorzystaniem procedury SCA we wszystkich przypadkach wymaganych przez dyrektywę PSD2. W przypadku możliwości zwolnienia transakcji z obowiązku realizacji procedury SCA, decyzja taka pozostaje w gestii ASPSP.
9. Uwierzytelnienie po stronie ASPSP MUSI nastąpić po przekierowaniu na stronę ASPSP, przez co dane uwierzytelniające i autoryzacyjne PSU MUSZĄ być przekazywane wyłącznie ASPSP.
10. W przypadku aplikacji mobilnych, przekierowanie na stronę ASPSP i z powrotem na stronę TPP MUSI odbywać się w przeglądarce systemowej (nie są dopuszczone przeglądarki inne niż systemowa, nie jest dopuszczone stosowanie WebView), a nie w samej aplikacji mobilnej. TPP może zarejestrować odpowiedni URL w systemie operacyjnym urządzenia, aby po przekierowaniu do TPP automatycznie wznowić aplikację mobilną.
11. Uwierzytelnianie PSU w zewnętrznym narzędziu autoryzacyjnym (EAT) MUSI spełniać następujące warunki:
    - EAT MUSI zapewniać funkcjonalność silnego uwierzytelnienia PSU – SCA, w rozumieniu technicznych wymogów dyrektywy PSD2;
    - PSU MUSI uprzednio pomyślnie aktywować dostęp do narzędzia EAT zgodnie z procedurą opracowaną i wymaganą przez każdego z ASPSP;

- ASPSP przygotowuje komunikat zawierający podstawowe informacje o transakcji wyświetlane w EAT przed jej potwierdzeniem;
- Wynik przeprowadzonej procedury SCA w narzędziu EAT MUSI zostać w bezpieczny sposób przekazany powiadomieniem do właściwego ASPSP.

12. Dane uwierzytelniające użytkownika oraz sesje, a także tokeny do autoryzowania operacji NIE MOGĄ być przekazywane w postaci parametrów URI.
13. Niezależnie od zastosowanego mechanizmu uwierzytelniania PSU, proces pomyślnego uwierzytelnienia MUSI zakończyć się wydaniem przez ASPSP A*ccess tokenu*. Zlecanie operacji przez TPP MUSI odbywać się z wykorzystaniem ważnego *Access tokenu*. *Access token* może być wykorzystywany jednokrotnie lub wielokrotnie, zanim ulegnie on unieważnieniu przez ASPSP, co będzie się wiązało z koniecznością ponownego przeprowadzenia procedury SCA dla PSU.
14. Kod *authorization code* oraz *Access token* MUSZĄ zapewniać zgodność z zapisami aktualnych, publicznie dostępnych zaleceń OWASP w zakresie zarządzania sesją, w szczególności w zakresie długości, entropii oraz czasu ważności.
15. Po maksymalnie 5 kolejnych nieudanych próbach uwierzytelnienia użytkownika (podczas logowania lub podczas autoryzacji transakcji), jego konto MUSI zostać zablokowane przez ASPSP. Odblokowanie konta MUSI zostać przeprowadzone zgodnie z procedurami ASPSP.
16. Po przekroczeniu limitu nieaktywności Użytkownika *Access token* MUSI zostać unieważniony przez ASPSP.
17. Po przekroczeniu limitu długości aktywnej sesji Użytkownika *Access token* MUSI zostać unieważniony przez ASPSP. Limit długości aktywnej sesji jest ustalany indywidualnie przez każdego z Podmiot korzystającego zów PolishAPI.
18. Transakcje o wyższym poziomie ryzyka (np. o wyższych kwotach lub do osób, z którymi tego typu transakcje nie były wcześniej wykonywane) POWINNY być dodatkowo autoryzowane przez ASPSP.
19. System płatności MUSI umożliwiać ograniczenie liczby lub wartości kwot transakcji wykonywanych przez określonego Użytkownika systemu w ustalonych przedziałach czasu (np. 1 godzina, 1 dzień, 1 miesiąc). MUSZĄ również zostać ustalone domyślne ograniczenia (obowiązujące Użytkownika systemu od razu po aktywacji usług).

6.2 Mechanizmy kryptograficznego zabezpieczenia danych

Cel: Całość Danych Chronionych przesyłanych pomiędzy Podmiotem korzystającym z PolishAPI oraz pomiędzy Użytkownikiem a Podmiotem korzystającym z PolishAPI MUSI być zabezpieczona przed ujawnieniem, modyfikacją oraz podszyciem się pod jedną ze stron komunikacji.

1. Komunikacja przez PolishAPI MUSI być zabezpieczona kryptograficznie na dwóch poziomach:
   - Na poziomie transportu MUSI być stosowany protokół TLS. Renegocjacja parametrów połączenia TLS MUSI być wykonywana bezpiecznie, zgodnie ze standardem RFC 5746.
   - Na poziomie komunikatu, dla zapewniania niezaprzeczalności, MUSI być stosowany podpis JSON Web Signature, zgodnie ze standardem RFC 7515. Sygnatura podpisu MUSI być umieszczana w każdym żądaniu w nagłówku o nazwie X-JWS-SIGNATURE.
2. Uczestnicy PolishAPI POWINNI stosować najbardziej bezpieczne wersje rozwiązań w zakresie kryptograficznej ochrony danych. Minimalne wymagania dla algorytmów oraz parametrów kluczy szyfrujących MUSZĄ być nie gorsze niż rekomendowane przez uznane instytucje np. NIST.
3. Każda ze stron komunikacji (TPP, ASPSP) MUSI posiadać własne unikatowe dwie pary kluczy (do transmisji i podpisu).
4. Do zabezpieczania transmisji na poziomie HTTPS oraz podpisu JWS-SIGNATURE MUSZĄ być zastosowane odrębne certyfikaty. Dla HTTPS certyfikat MUSI posiadać rozszerzone użycie klucza (Client Authentication) dla podpisu (Digital signature).

5. Certyfikaty użyte do zestawienia transmisji oraz podpisu MUSZĄ zostać walidowane pod względem:
    - Ważności (daty ważności certyfikatu od i do)
    - Braku odwołania (CRL lub OCSP)
    - Weryfikacji ścieżki (RFC 4158)
6. Certyfikaty MUSZĄ być wydawane z uwzględnieniem specyfikacji ETSI TS 119 495.
7. Wszystkie żądania i odpowiedzi MUSZĄ być podpisywane zgodnie ze standardem JWS-SIGNATURE, w ramach interfejsu XS2A (po stronie ASPSP) oraz interfejsu wywołań zwrotnych (po stronie TPP).
8. W ramach nagłówka podpisu JWS-SIGNATURE MUSZĄ być spełnione następujące warunki:
    - użycie parametru nagłówka o nazwie „kid" jest wymagane (rozszerzenie punktu 4.1.4 RFC 7515),
    - użycie parametru nagłówka o nazwie „x5t#S256" jest wymagane (rozszerzenie punktu 4.1.8 RFC 7515).

    Dzięki temu możliwe jest jednoznaczne zidentyfikowanie certyfikatu, po stronie odczytującej, odnalezienie go w wewnętrznej infrastrukturze kryptograficznej i użycie do odczytania treści podpisu oraz pominięcie konieczności uzgodnienia certyfikatu przy każdym wysłanym i odebranym komunikacie poprzez interfejsy XS2A oraz wywołań zwrotnych.
9. Uczestnicy komunikacji MUSZĄ jednorazowo uzgodnić certyfikat, np. poprzez:
    - użycie parametru nagłówka podpisu JWS-SIGNATURE o nazwie „x5u" (punkt 4.1.5 RFC 7515); co pozwala na przekazanie URL do zasobu będącego publicznym kluczem certyfikatu X.509, w tym samym komunikacie, w którym podpis JWS-SIGNATURE został zbudowany po raz pierwszy przy użyciu tego certyfikatu;
    - zastosowanie procedury w oparciu o protokół „OAuth 2.0 Dynamic Client Registration" (RFC 7591), pozwalającej na wcześniejsze (w stosunku do faktycznej komunikacji przy użyciu interfejsu XS2A lub wywołań zwrotnych) uzgodnienie certyfikatu pomiędzy stronami.

6.3 Walidacja danych

Cel: Dane wejściowe pochodzące z niezaufanych źródeł NIE MOGĄ zostać przetworzone przez oprogramowanie interfejsu PolishAPI w taki sposób, który umożliwiałby przeprowadzenie ataków na system lub jego użytkowników (np. poprzez wywołanie ataków Cross-Site Scripting, SQL Injection, XML Injection, Directory Traversal).

1. Oprogramowanie PolishAPI MUSI sprawdzać poprawność danych uzyskanych z niezaufanych źródeł danych przed ich użyciem za pomocą pozytywnej walidacji – czyli dla każdego typu danych wejściowych MUSZĄ istnieć zasady ich poprawności, które będą możliwie jak najbardziej restrykcyjne. Jeśli dane wejściowe mogą zawierać znaki specjalne, to MUSZĄ one zostać poprawnie zakodowane, za pomocą dedykowanych funkcji.
2. Jeśli dane uzyskane z niezaufanych źródeł są wyświetlane na ekranie, to wszelkie znaki specjalne w tym kontekście (czyli np. tagi HTML jeśli użyty do wyświetlania komponent je obsługuje) MUSZĄ zostać usunięte z danych wejściowych lub odpowiednio zakodowane za pomocą dedykowanego mechanizmu.
3. Jeśli oprogramowanie PolishAPI używa wbudowanych komponentów przeglądarki WWW, to MUSI blokować elementy aktywne tej przeglądarki (np. obsługę skryptów Javascript oraz ładowanie rozszerzeń zewnętrznych typu plugins) lub umożliwiać korzystanie z tych komponentów pobierając elementy aktywne z zaufanych źródeł lub zapewniając właściwą walidację danych pochodzących z niezaufanych źródeł.

4. Jeśli dane uzyskane z niezaufanych źródeł są używane przez oprogramowanie PolishAPI MUSZĄ zostać spełnione wymagania weryfikacji dla obsługi złośliwych danych wejściowych zgodnie z aktualnym standardem OWASP Application Security Verification Standard.
5. Ustrukturyzowane dane JSON MUSZĄ być weryfikowane zgodnie z formalnymi procedurami walidacyjnymi z zastosowaniem podejścia opartego na listach dopuszczalnych wartości (*white list*). Walidacji MUSZĄ być także poddane nagłówki Content-type i Accept (application/json) na zgodność wartości nagłówka z rzeczywistą treścią komunikatu HTTP.
6. Podczas walidacji MUSI być zweryfikowany podpis cyfrowy w nagłówku (X-JWS-SIGNATURE) w kontekście danych przekazywanych zarówno w żądaniach jak i odpowiedziach protokołu HTTP, wymienianych w komunikacji na linii ASPSP-TPP (również w przypadku komunikacji inicjowanej przez ASPSP).
7. Błędy walidacji danych wejściowych MUSZĄ być rejestrowane w logach.
8. Błędy walidacji MUSZĄ być sygnalizowane komunikatem HTTP 400 (Bad Request) i dane MUSZĄ być odrzucane. Dotyczy to również negatywnej walidacji podpisu JWS-SIGNATURE.
9. W razie błędów walidacji treści Content-type i Accept POWINIEN zostać zwrócony komunikat HTTP numer 406 (Not Acceptable).

6.4 Rozliczalność zdarzeń

Cel: System MUSI zapewniać rozliczalność i niezaprzeczalność działań użytkowników systemu, przy jednoczesnym zapewnieniu poufności Danych Chronionych oraz prywatności użytkowników.

1. Oprogramowanie PolishAPI MUSI rejestrować wszystkie kluczowe operacje oraz udane i nieudane próby uwierzytelnienia i autoryzacji.
2. Czas retencji logów MUSI być zgodny z obowiązującym prawem oraz POWINIEN być możliwie jak najdłuższy.
3. Źródła czasu wszystkich podmiotów korzystających z PolishAPI POWINNY być synchronizowane z zaufanym źródłem czasu (maksimum stratum 3), aby zapewnić, że wpisy w logach mają poprawny czas.
4. Logowanie kluczowych operacji biznesowych MUSI zapewniać niezaprzeczalność i integralność wpisów, co POWINNO być realizowane przez wykorzystanie danych z podpisu JWS Signature.
5. Log POWINIEN zawierać niezbędne informacje, które pozwolą na precyzyjną analizę czasową w przypadku wystąpienia zdarzenia pozwalającą na złączenie poszczególnych wpisów w jedną transakcję. Elementem łączącym poszczególne wpisy może być np. skrót z tokenu autoryzacyjnego.
6. Informacje szczególnie wrażliwe, w tym poświadczenia tożsamości oraz klucze autoryzacyjne NIE MOGĄ podlegać buforowaniu oraz zapisywaniu w logach.
7. Każde żądanie wysyłane przez TPP do interfejsu XS2A po stronie ASPSP MUSI zawierać unikalny identyfikator (parametr o nazwie requestId w strukturze nagłówkowej przekazywanej w ciele każdego żądania oraz w nagłówku o nazwie X-REQUEST-ID). Unikalność tego identyfikatora MUSI być zachowana w skali wszystkich żądań wysyłanych przez wszystkie TPP do wybranego ASPSP. Formatem identyfikatora żądania MUSI być UUID (ang. *Universally Unique Identifier*), który jest standardem opisanym w dokumencie RFC 4122. Identyfikator żądania MUSI być generowany w wariancie numer 1 (patrz punkt 4.1.1 RFC 4122) oraz wersji nr 1 (patrz punkt 4.1.3 RFC 4122), co zapewnia uwzględnienie w wartości identyfikatora składnika monotonicznego opartego o czas wysłania żądania oraz informację identyfikującą podmiot wysyłający żądanie (TPP).
8. Ze względu na mogące wystąpić w trakcie przetwarzania żądania HTTP zdarzenia typu *timeout*, ASPSP MUSI zapewnić weryfikację unikalności na poziomie id wywołania (requestId). Po stwierdzeniu braku unikalności wywołania ASPSP MUSI zwrócić błąd 400.1 (Powtórzone wywołanie).

9. Limit czasu przetwarzania żądania (*timeout*) MUSI być określony i nie dłuższy niż 5 minut, a po przekroczeniu limitu żądanie MUSI być unieważnione.

7 Obszar 4: Przeciwdziałanie nadużyciom i atakom

7.1 Monitorowanie zdarzeń

Cel: System MUSI rejestrować działania użytkowników oraz informacje niezbędne do wykrywania prób ataku na system, przy jednoczesnym zapewnieniu poufności danych chronionych oraz prywatności użytkowników.

1. Podmiot korzystający z PolishAPI MUSI zapewnić przeprowadzenie analizy ryzyka oraz na jej podstawie podjęcie decyzji o wdrożeniu i wykorzystywaniu adekwatnego do ryzyka systemu wykrywania i zapobiegania fraudom w celu identyfikacji podejrzanych transakcji, preferowanie przed ich autoryzacją oraz w celu monitorowania działań płatników i akceptantów
2. Podmiot korzystający z PolishAPI POWINNIEN zapewniać:
   - Możliwość wykonania kompleksowej procedury kontroli i oceny transakcji w akceptowalnym czasie;
   - Odrzucanie potencjalnie oszukańczych transakcji płatniczych.

7.2 Reguły wykrywania nadużyć

Cel: System monitorowania POWINIEN analizować działanie systemu płatności korzystając ze wszystkich dostępnych w ramach tego systemu źródeł informacji – między innymi o anomaliach i błędach w działaniu różnych komponentów. Efektem działania systemu monitorowania POWINNY być informacje o przeprowadzanych atakach na system, ich skali oraz metodach używanych przez atakujących. POWINNO to prowadzić do blokowania działań atakujących na jak najwcześniejszym etapie ataku (np. w czasie rekonesansu) i minimalizować ryzyko nadużyć prowadzących do strat finansowych lub reputacyjnych.

1. W ramach interfejsu PolishAPI POWINNY zostać wdrożone mechanizmy wykrywające i blokujące podejrzane transakcje.
2. Podmiot korzystający z PolishAPI POWINIEN wymieniać informacje w zakresie podejrzeń nieautoryzowanych transakcji/skompromitowanych IP, itp.

7.3 Ochrona systemu przed atakami odmowy dostępu

Cel: Interfejs PolishAPI MUSI zostać zabezpieczony przed możliwością przeprowadzenia ataku odmowy dostępu (ang. Denial Of Service), którego celem będzie jeden lub kilka z podmiotów uczestniczących w procesie realizacji płatności.

1. Dostępne publicznie komponenty interfejsu PolishAPI MUSZĄ być chronione w taki sposób, aby minimalizowały ryzyko związanie z atakami odmowy usługi (Denial of Service). W szczególności operacje dostępne dla użytkowników niezalogowanych (np. rejestracja nowego użytkownika) MUSZĄ być zabezpieczone przed tego typu atakami.
2. W ramach interfejsu PolishAPI MUSZĄ zostać zaimplementowane mechanizmy ochrony przed atakami typu odmowa usługi poprzez zliczanie liczby transakcji i wymuszanie maksymalnych limitów, których przekroczenie będzie powodowało blokady, np.:
   - liczby transakcji inicjowanych przez TPP wraz z uwzględnieniem do kogo są adresowane i na jakie kwoty opiewają.

- liczby transakcji inicjowanych przez wybranego użytkownika.
- łącznej liczby transakcji z możliwością ich ręcznego lub automatycznego odcięcia.
- liczby zapytań dla każdego mechanizmu (funkcji, serwisu) dostępnego dla TPP w określonym przedziale czasu.

3. Wartości limitów POWINNY być ustalane na podstawie rozpoznania konkretnych warunków operacyjnych. Limity tego rodzaju POWINNY podlegać parametryzacji. Mierzenie liczby żądań dostępu do zasobów POWINNO bazować na zastosowaniu jednoznacznie identyfikującego danego TPP klucza oraz liczników zaimplementowanych per TPP po stronie serwera. Przekroczenie limitów MUSI być sygnalizowane komunikatem HTTP numer 429 (Too Many Requests).