KOMISJA
EUROPEJSKA

Bruksela, dnia 20.3.2024 r.
COM(2024) 125 final

ANNEX

ZAŁĄCZNIK

do

wniosku w sprawie decyzji Rady

w sprawie stanowiska, jakie ma być zajęte w imieniu Unii Europejskiej w ramach Wspólnego Komitetu ustanowionego na mocy Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych, w odniesieniu do zmiany załącznika II do umowy, wspólnych procedur operacyjnych i norm technicznych powiązania

DECYZJA NR 1/2024 WSPÓLNEGO KOMITETU USTANOWIONEGO NA MOCY UMOWY MIĘDZY UNIĄ EUROPEJSKĄ A KONFEDERACJĄ SZWAJCARSKĄ W SPRAWIE POWIĄZANIA ICH SYSTEMÓW HANDLU UPRAWNIENIAMI DO EMISJI GAZÓW CIEPLARNIANYCH

z dnia ...

w odniesieniu do zmiany załącznika II do umowy, wspólnych procedur operacyjnych i norm technicznych powiązania

WSPÓLNY KOMITET,

uwzględniając Umowę między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych[1] (zwaną dalej „umową"), w szczególności jej art. 9 i art. 13 ust. 2,

a także mając na uwadze, co następuje:

(1) W decyzji Wspólnego Komitetu nr 2/2019[2] przewidziano tymczasowe rozwiązanie umożliwiające uruchomienie powiązania między EU ETS a ETS Szwajcarii.

(2) Na swoim trzecim posiedzeniu Wspólny Komitet zgodził się co do potrzeby przeanalizowania opłacalności stałego powiązania między rejestrem Unii a rejestrem Szwajcarii.

(3) Na swoim piątym posiedzeniu Wspólny Komitet uzgodnił sprawozdanie przedłożone przez grupę roboczą ustanowioną na mocy decyzji Wspólnego Komitetu nr 1/2020[3] i 2/2020[4], w którym grupa ta przeanalizowała i zaleciła podejście do wdrożenia stałego powiązania między rejestrem Unii a rejestrem Szwajcarii.

(4) Aby odzwierciedlić wymogi techniczne stałego powiązania między rejestrem Unii a rejestrem Szwajcarii, a także aby dostosować przepisy załącznika II do umowy w świetle rozwoju technologicznego, należy zmienić załącznik II do umowy.

(5) Aby zapewnić spójność wspólnych procedur operacyjnych i norm technicznych powiązania z załącznikiem II do umowy, dokumenty te również należy zmienić,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Załącznik II do umowy zastępuje się tekstem załącznika I do niniejszej decyzji.

2. Wspólne procedury operacyjne, o których mowa w art. 3 ust. 6 umowy, określono w załączniku II do niniejszej decyzji.

3. Normy techniczne powiązania, o których mowa w art. 3 ust. 7 umowy, określono w załączniku III do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w [Brukseli][Bernie] w języku angielskim dnia [xx 2024] r.

---

1 Dz.U. L 322 z 7.12.2017, s. 3.
2 Dz.U. L 314 z 29.9.2020, s. 68.
3 Dz.U. L 226 z 25.6.2021, s. 2.
4 Dz.U. L 226 z 25.6.2021, s. 16.

W imieniu Wspólnego Komitetu

Sekretarz ze strony Unii Europejskiej	*Przewodniczący*	*Sekretarz ze strony Szwajcarii*

ZAŁĄCZNIK I

„ZAŁĄCZNIK II

NORMY TECHNICZNE POWIĄZANIA

W celu uruchomienia powiązania między EU ETS i ETS Szwajcarii w 2020 r. wdrożono tymczasowe rozwiązanie. Od 2023 r. powiązanie rejestrów między dwoma systemami handlu uprawnieniami do emisji będzie stopniowo przekształcane w stałe powiązanie rejestrów, które ma zostać wdrożone nie później niż w 2024 r., co umożliwi funkcjonowanie powiązanych rynków w odniesieniu do korzyści płynących z płynności rynku i realizację transakcji między dwoma powiązanymi systemami w sposób równoważny jednemu rynkowi składającemu się z dwóch systemów i który umożliwia uczestnikom rynku działanie tak, jakby byli na jednym rynku, z zastrzeżeniem jedynie indywidualnych przepisów wykonawczych stron. W normach technicznych powiązania określa się:

– architekturę łącza komunikacyjnego,

– komunikację między SSTL a EUTL,

– bezpieczeństwo przesyłania danych,

– wykaz funkcji (transakcje, uzgodnienia itp.),

– definicję warstwy transportowej,

– wymogi rejestracji danych,

– ustalenia operacyjne (centrum informacyjne, wsparcie),

– plan aktywacji komunikacji i procedurę testowania,

– procedurę testowania bezpieczeństwa.

W normach technicznych powiązania określa się, że administratorzy podejmują wszystkie rozsądne kroki w celu zapewnienia, aby SSTL, EUTL oraz łącze funkcjonowały 24 godziny na dobę, oraz 7 dni w tygodniu, a wszelkie zakłócenia w funkcjonowaniu SSTL, EUTL oraz łącza były ograniczone do minimum.

W normach technicznych powiązania określa się dodatkowe wymogi bezpieczeństwa dla rejestru Szwajcarii, SSTL, rejestru Unii oraz EUTL, a same normy techniczne powiązania odnotowuje się w „planie zarządzania bezpieczeństwem”. W szczególności w normach technicznych powiązania określa się, że:

– jeżeli istnieje podejrzenie, że bezpieczeństwo rejestru Szwajcarii, SSTL, rejestru Unii lub EUTL zostało naruszone, obie strony natychmiast przekazują sobie te informacje oraz zawieszają powiązanie między SSTL i EUTL,

– w przypadku naruszenia bezpieczeństwa strony zobowiązują się do natychmiastowej wymiany informacji na ten temat. W takim zakresie, w jakim dostępne są szczegóły techniczne, w ciągu 24 godzin od uznania incydentu związanego z bezpieczeństwem za naruszenie bezpieczeństwa, sprawozdanie, w którym opisano incydent (datę, przyczynę, skutek, środki zaradcze), udostępnia się administratorowi rejestru Szwajcarii oraz centralnemu administratorowi Unii.

Procedura testowania bezpieczeństwa określona w normach technicznych powiązania musi zakończyć się przed ustanowieniem łącza komunikacyjnego między SSTL a EUTL oraz w każdym przypadku, gdy wymagana jest nowa wersja lub nowe wydanie SSTL lub EUTL.

Normy techniczne powiązania zapewniają, oprócz środowiska produkcyjnego, dwa dodatkowe środowiska testowe: środowisko testowe dla twórców oprogramowania i środowisko akceptacyjne.

Za pośrednictwem administratora rejestru Szwajcarii i centralnego administratora Unii strony przedstawiają dowody na to, że w ciągu ostatnich dwunastu miesięcy przeprowadzono niezależną ocenę ich systemów zgodnie z wymogami bezpieczeństwa określonymi w normach technicznych powiązania. Testowanie bezpieczeństwa, w szczególności testy penetracyjne, przeprowadza się na wszystkich głównych nowo wydanych wersjach oprogramowania zgodnie z wymogami bezpieczeństwa określonymi w normach technicznych powiązania. Testów penetracyjnych nie może przeprowadzić twórca oprogramowania ani podwykonawca twórcy oprogramowania.”.

ZAŁĄCZNIK II

WSPÓLNE PROCEDURY OPERACYJNE

na podstawie art. 3 ust. 6 Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych

Procedury stałego powiązania rejestrów

Spis treści

1. Glosariusz 8
2. Wprowadzenie 10
2.1. Zakres 10
2.2. Adresaci 11
3. Podejście i normy 11
4. Zarządzanie incydentami 12
4.1. Wykrywanie i rejestracja incydentów 12
4.2. Klasyfikacja i wstępne wsparcie 12
4.3. Badanie i diagnoza 13
4.4. Rozwiązanie i przywrócenie do stanu używalności 13
4.5. Zamknięcie incydentu 14
5. Zarządzanie problemami 15
5.1. Identyfikacja i rejestracja problemu 15
5.2. Określanie priorytetu problemów 15
5.3. Badanie i diagnoza problemu 15
5.4. Rozwiązanie 15
5.5. Zamknięcie problemu 15
6. Realizacja wniosków 16
6.1. Wszczęcie procedury dotyczącej wniosku 16
6.2. Rejestracja i analiza wniosku 16
6.3. Zatwierdzenie wniosku 16
6.4. Realizacja wniosków 16
6.5. Przekazanie wniosku 16
6.6. Przegląd realizacji wniosku 17
6.7. Zamknięcie wniosku 17
7. Zarządzanie zmianą 18
7.1. Wniosek o zmianę 18

7.2. Ocena i planowanie zmiany 18
7.3. Zatwierdzanie zmiany 18
7.4. Wdrożenie zmiany 18
8. Zarządzanie wersjami 19
8.1. Planowanie wersji 19
8.2. Tworzenie i testowanie pakietu wersji 19
8.3. Przygotowanie wdrożenia 20
8.4. Cofnięcie wersji 20
8.5. Przegląd i zamknięcie wersji 20
9. Zarządzanie incydentami związanymi z bezpieczeństwem informacji 21
9.1. Kategoryzacja incydentów związanych z bezpieczeństwem informacji 21
9.2. Postępowanie z incydentami związanymi z bezpieczeństwem informacji 21
9.3. Identyfikacja incydentów związanych z bezpieczeństwem informacji 21
9.4. Analiza incydentów związanych z bezpieczeństwem informacji 22
9.5. Ocena wagi incydentu związanego z bezpieczeństwem informacji, przekazywanie go i związana z nim sprawozdawczość 22
9.6. Sprawozdawczość dotycząca reakcji na incydent związany z bezpieczeństwem informacji 22
9.7. Monitorowanie, budowanie zdolności i stałe dążenie do doskonałości 22
10. Zarządzanie bezpieczeństwem informacji 23
10.1. Identyfikacja danych szczególnie chronionych 23
10.2. Poziomy wrażliwości zasobów informacyjnych 23
10.3. Przypisywanie zasobów informacyjnych do właściciela 23
10.4. Rejestracja danych szczególnie chronionych 24
10.5. Postępowanie z danymi szczególnie chronionymi 24
10.6. Zarządzanie dostępem 24
10.7. Zarządzanie certyfikatami/kluczami 25

1. GLOSARIUSZ

Tabela 1–1 Akronimy i definicje

Akronim/termin	Definicja
Centrum certyfikacji	Podmiot, który wydaje certyfikaty elektroniczne

CH	Konfederacja Szwajcarska
ETS	System uprawnieniami do emisji
UE	Unia Europejska
IMT	Zespół ds. zarządzania incydentami
Zasób informacyjny	Informacja, która ma wartość dla przedsiębiorstwa lub organizacji
IT	Technologia informacyjna
ITIL	*Information Technology Infrastructure Library* – Biblioteka dokumentów dotyczących zarządzania infrastrukturą IT
ITSM	Zarządzanie usługami informatycznymi
LTS	Normy techniczne powiązania
Rejestr	System rejestracji uprawnień przyznanych na podstawie ETS służący do śledzenia własności uprawnień utrzymywanych na kontach elektronicznych
RFC	Wniosek o zmianę
SIL	Wykaz danych szczególnie chronionych
SR	Wniosek o usługę
Wiki	Strona internetowa umożliwiająca użytkownikom wymianę informacji i wiedzy w drodze dodawania lub dostosowywania treści bezpośrednio przez przeglądarkę internetową

2. WPROWADZENIE

Umowa między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych z dnia 23 listopada 2017 r. („umowa") przewiduje wzajemne uznawanie uprawnień do emisji, które można wykorzystać na potrzeby dostosowania się do wymogów systemu handlu uprawnieniami do emisji Unii Europejskiej („EU ETS") lub systemu handlu uprawnieniami do emisji Szwajcarii („ETS Szwajcarii"). W celu uruchomienia powiązania między EU ETS a ETS Szwajcarii ustanowione zostanie bezpośrednie powiązanie między dziennikiem transakcji Unii Europejskiej (EUTL) rejestru Unii a dodatkowym dziennikiem transakcji Szwajcarii (SSTL) rejestru Szwajcarii, co umożliwi bezpośrednie przekazywanie między rejestrami uprawnień do emisji wydanych w ramach któregokolwiek z ETS (art. 3 ust. 2 umowy). W celu uruchomienia powiązania między EU ETS i ETS Szwajcarii w 2020 r. wdrożono tymczasowe rozwiązanie. Od 2023 r. powiązanie rejestrów między dwoma systemami handlu uprawnieniami do emisji będzie stopniowo przekształcane w stałe powiązanie rejestrów, które ma zostać wdrożone nie później niż w 2024 r., co umożliwi funkcjonowanie powiązanych rynków w odniesieniu do korzyści płynących z płynności rynku i realizację transakcji między dwoma powiązanymi systemami w sposób równoważny jednemu rynkowi składającemu się z dwóch systemów i który umożliwia uczestnikom rynku działanie tak, jakby byli na jednym rynku, z zastrzeżeniem jedynie indywidualnych przepisów wykonawczych stron. (Załącznik II do umowy)

Zgodnie z art. 3 ust. 6 umowy administrator rejestru Szwajcarii i centralny administrator Unii określają wspólne procedury operacyjne związane z kwestiami technicznymi lub innymi kwestiami, które są niezbędne do funkcjonowania powiązania, uwzględniając priorytety zawarte w prawodawstwie krajowym. Wspólne procedury operacyjne opracowane przez administratorów stają się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

Wspólne procedury operacyjne zostały przyjęte przez Wspólny Komitet decyzją nr 1/2020. Zaktualizowane wspólne procedury operacyjne w formie przedstawionej w niniejszym dokumencie zostaną przyjęte przez Wspólny Komitet decyzją nr 1/2024. Zgodnie ze wspomnianą decyzją i wnioskiem Wspólnego Komitetu administrator rejestru Szwajcarii i centralny administrator Unii opracowali dalsze wytyczne techniczne celem uruchomienia powiązania oraz będą je aktualizować celem zapewnienia, aby były one stale dostosowywane do postępu technicznego i nowych wymogów związanych z bezpieczeństwem i ochroną tego powiązania oraz jego skutecznym i sprawnym funkcjonowaniem.

2.1. Zakres

Niniejszy dokument odzwierciedla wspólne porozumienie stron umowy w kwestii ustanowienia podstaw proceduralnych powiązania między rejestrami EU ETS i ETS Szwajcarii. Chociaż nakreślono w nim ogólne wymogi proceduralne dotyczące operacji, do uruchomienia powiązania potrzebne będą dalsze wytyczne techniczne.

Jeżeli chodzi o prawidłowe funkcjonowanie, powiązanie będzie wymagało specyfikacji technicznych do jego dalszego uruchomienia. Zgodnie z art. 3 ust. 7 umowy kwestie te szczegółowo opisano w dokumencie dotyczącym norm technicznych powiązania przyjętym odrębną decyzją Wspólnego Komitetu.

Wspólne procedury operacyjne mają na celu zapewnienie, aby usługi informatyczne związane z funkcjonowaniem powiązania między rejestrami EU ETS i ETS Szwajcarii były świadczone

skutecznie i sprawnie, szczególnie jeżeli chodzi o realizację wniosków o usługę, usuwanie awarii usług, naprawianie problemów, jak również realizację rutynowych zadań operacyjnych zgodnie z międzynarodowymi normami zarządzania usługami informatycznymi.

W przypadku stałego powiązania rejestrów potrzebne będą jedynie następujące, przedstawione w niniejszym dokumencie wspólne procedury operacyjne:

- zarządzanie incydentami;
- zarządzanie problemami;
- realizacja wniosków;
- zarządzanie zmianą;
- zarządzanie wersjami;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- zarządzanie bezpieczeństwem informacji.

2.2. Adresaci

Przedmiotowe wspólne procedury operacyjne są skierowane do zespołów wsparcia technicznego rejestrów UE i Szwajcarii.

3. PODEJŚCIE I NORMY

Poniższe zasady dotyczą wszystkich wspólnych procedur operacyjnych:

- UE i Szwajcaria zgadzają się, że wspólne procedury operacyjne określa się na podstawie ITIL (biblioteka dokumentów dotyczących zarządzania infrastrukturą (Information Technology Infrastructure Library), wersja 4). Praktyki wywodzące się z tej normy wykorzystuje się wielokrotnie i dostosowuje się je do szczególnych potrzeb stałego powiązania rejestrów;
- komunikacja i koordynacja niezbędne do realizacji wspólnych procedur operacyjnych między obiema stronami odbywają się za pośrednictwem centrów obsługi rejestrów Szwajcarii i UE. Zadanie zawsze przydziela się w ramach jeden ze stron;
- ewentualne spory dotyczące postępowania ze wspólnymi procedurami operacyjnymi wspólnie analizują i rozpatrują oba centra obsługi. Jeżeli nie uda się osiągnąć porozumienia, obowiązek ustalenia wspólnego rozwiązania przekazuje się na kolejny szczebel;

Kolejne szczeble	UE	CH
Pierwszy szczebel	Unijne centrum obsługi	Szwajcarskie centrum obsługi
Drugi szczebel	Unijny kierownik ds. operacji (*EU Operations Manager*)	Szwajcarski kierownik ds. aplikacji rejestru (*CH Registry Application Manager*)
Trzeci szczebel	Wspólny Komitet (może przekazać ten obowiązek zgodnie z art. 12 ust. 5 umowy w sprawie powiązania)	
Czwarty szczebel	Wspólny Komitet, jeżeli na trzecim szczeblu przekazano ten obowiązek	

- każda ze stron może określić procedury dotyczące funkcjonowania własnego systemu rejestru, uwzględniając wymogi i interfejsy związane z przedmiotowym wspólnymi procedurami operacyjnymi;
- do obsługi wspólnych procedur operacyjnych wykorzystuje się narzędzie zarządzania usługami informatycznymi (*IT Service Management* – ITSM), w szczególności do zarządzania incydentami, zarządzania problemami i realizacji wniosków oraz do komunikacji między stronami;
- możliwa jest również wymiana informacji za pośrednictwem poczty elektronicznej;
- obie strony zapewniają spełnienie wymogów dotyczących bezpieczeństwa informacji zgodnie z instrukcjami postępowania z informacjami.

4. ZARZĄDZANIE INCYDENTAMI

Proces zarządzania incydentami ma na celu jak najszybsze przywrócenie usług informatycznych po wystąpieniu incydentu do normalnego poziomu usług przy jak najmniejszym zakłóceniu działalności.

W ramach zarządzania incydentami należy również zawsze rejestrować incydenty na potrzeby sprawozdawczości i współpracować z innymi procesami, aby stale dążyć do doskonałości.

W ogólnej perspektywie zarządzanie incydentami składa się z następujących działań:

- Wykrywanie i rejestracja incydentów;
- Klasyfikacja i wstępne wsparcie;
- Badanie i diagnoza;
- Rozwiązanie i przywrócenie do stanu używalności;
- Zamknięcie incydentu.

Na wszystkich etapach cyklu życia incydentu proces zarządzania incydentami odpowiada za ciągłe zarządzanie własnością, monitorowanie, śledzenie i komunikację.

4.1. Wykrywanie i rejestracja incydentów

Incydent może zostać wykryty przez zespół wsparcia, automatyczne narzędzia monitorujące lub personel techniczny wykonujący rutynowe działania kontrolne.

Po wykryciu incydent musi zostać zarejestrowany i opatrzony niepowtarzalnym identyfikatorem, który umożliwia odpowiednie śledzenie i monitorowanie incydentu. Niepowtarzalnym identyfikatorem incydentu jest identyfikator przydzielony w ramach wspólnego systemu zgłaszania przez centrum obsługi strony (albo UE, albo Szwajcarii), która poinformowała o incydencie, i należy go stosować w całej komunikacji związanej z tym incydentem.

W przypadku wszystkich incydentów punktem kontaktowym powinno być centrum obsługi strony, która zarejestrowała zgłoszenie.

4.2. Klasyfikacja i wstępne wsparcie

Klasyfikacja incydentu ma na celu zrozumienie, którego systemu lub której usługi on dotyczy i w jakim stopniu, oraz ich identyfikację. Jeżeli klasyfikacja ma być skuteczna, powinna już za pierwszym razem przydzielić incydent do właściwego zasobu, aby przyspieszyć jego rozwiązanie.

W ramach etapu klasyfikacji należy nadać incydentowi kategorię i priorytet, uwzględniając jego wpływ i pilność, aby został rozwiązany w terminie odpowiadającym temu priorytetowi.

Jeżeli incydent może mieć skutki dla poufności lub integralności danych szczególnie chronionych lub skutki dla dostępności systemu, incydent należy określić również jako incydent związany z bezpieczeństwem informacji i zarządzać nim zgodnie z procesem określonym w rozdziale „Zarządzanie incydentami związanymi z bezpieczeństwem informacji" niniejszego dokumentu.

Jeżeli jest to możliwe, centrum obsługi, które zarejestrowało zgłoszenie, przeprowadza wstępną diagnozę. W tym celu centrum obsługi sprawdzi, czy incydent jest znanym błędem. Jeżeli tak, to sposób rozwiązania lub obejścia problemu jest już znany i udokumentowany.

Jeżeli centrum obsługi uda się rozwiązać incydent, to zamyka incydent na tym etapie, ponieważ główny cel zarządzania incydentami został spełniony (a mianowicie szybkie przywrócenie działania usługi u użytkownika końcowego). Jeżeli nie, to centrum obsługi przekaże incydent do odpowiedniego zespołu ds. rozwiązywania problemów celem dalszego zbadania i zdiagnozowania.

4.3. Badanie i diagnoza

Badanie i diagnozę incydentu przeprowadza się, jeżeli centrum obsługi nie było w stanie rozwiązać incydentu w ramach wstępnej diagnozy i zgodnie z procedurą przekazało problem na wyższy szczebel. Przekazanie incydentu jest pełnoprawną częścią procesu badania i diagnozy.

Częstą praktyką stosowaną na etapie badania i diagnozy jest próba odtworzenia incydentu w warunkach kontrolowanych. Istotnym elementem badania i diagnozy incydentu jest zrozumienie właściwej kolejności wydarzeń, które doprowadziły do incydentu.

Przekazanie oznacza przyznanie, że incydentu nie da się rozwiązać na obecnym szczeblu wsparcia technicznego i należy go przekazać do grupy wsparcia wyższego szczebla lub do drugiej strony. Przekazanie może się odbyć na dwa sposoby: poziomo (funkcjonalnie) lub pionowo (hierarchicznie).

Centrum obsługi, które zarejestrowało incydent i uruchomiło procedurę zarządzania nim, jest odpowiedzialne za przekazanie incydentu do odpowiedniego zasobu oraz za śledzenie ogólnego statusu incydentu i monitorowanie, do kogo jest przypisany.

Strona, której przypisano incydent, jest odpowiedzialna za zapewnienie, aby działania, o które wnioskowano, zostały przeprowadzone terminowo, oraz za przesłanie informacji zwrotnej do centrum obsługi swojej strony.

4.4. Rozwiązanie i przywrócenie do stanu używalności

Rozwiązanie incydentu i przywrócenie do stanu używalności przeprowadza się po pełnym zrozumieniu incydentu. Znalezienie rozwiązania incydentu oznacza, że zidentyfikowano sposób naprawienia problemu. Faktyczne zastosowanie rozwiązania to etap przywrócenia do stanu używalności.

Gdy odpowiednie zasoby usuną awarię usługi, incydent przekazuje się z powrotem do odpowiedniego centrum obsługi, które zarejestrowało incydent, aby centrum to potwierdziło użytkownikowi, który zgłosił incydent, że błąd został naprawiony i że incydent można zamknąć. Ustalenia z prac nad incydentem należy zarejestrować na przyszłe potrzeby.

Przywrócenia do stanu używalności może dokonać zespół wsparcia informatycznego lub użytkownik końcowy po otrzymaniu odpowiednich instrukcji.

4.5. Zamknięcie incydentu

Zamknięcie to ostatni etap procesu zarządzania incydentami i odbywa się wkrótce po rozwiązaniu incydentu.

Spośród działań, które należy przeprowadzić na etapie zamknięcia, najważniejsze są następujące:

- weryfikacja wstępnej kategorii przypisanej do incydentu;
- odpowiednie zgromadzenie wszystkich informacji związanych z incydentem;
- odpowiednie udokumentowanie incydentu i aktualizacja bazy wiedzy;
- odpowiednie powiadomienie wszystkich zainteresowanych stron bezpośrednio lub pośrednio dotkniętych incydentem.

Incydent jest oficjalnie zamknięty po przeprowadzeniu etapu zamknięcia incydentu przez centrum obsługi i poinformowaniu o tym drugiej strony.

Jeżeli incydent został zamknięty, już się go nie otwiera. Jeżeli niedługo później incydent powtórzy się, nie otwiera się ponownie pierwotnego incydentu, ale rejestruje się nowy.

Jeżeli zarówno unijne, jak i szwajcarskie centrum obsługi śledzi dany incydent, ostateczne zamknięcie jest obowiązkiem centrum obsługi, które zarejestrowało zgłoszenie.

5. ZARZĄDZANIE PROBLEMAMI

Niniejsza procedura dotyczy sytuacji, gdy zidentyfikowano problem, a tym samym uruchomiono proces zarządzania problemami. Zarządzanie problemami skupia się na poprawie jakości i ograniczeniu liczby zgłaszanych incydentów. Jeden problem może być przyczyną jednego incydentu lub większej ich liczby. Gdy incydent zostanie zgłoszony, celem zarządzania incydentami jest jak najszybsze przywrócenie działania usługi, co może obejmować zastosowanie obejść. Po zarejestrowaniu problemu należy zbadać jego podstawową przyczynę, aby wskazać zmiany, których wprowadzenie zagwarantuje, że problem i powiązane z nim incydenty nie będą więcej występowały.

5.1. Identyfikacja i rejestracja problemu

W zależności od strony, która utworzyła zgłoszenie, punktem kontaktowym w kwestiach dotyczących danego problemu będzie albo unijne, albo szwajcarskie centrum obsługi.

Niepowtarzalnym identyfikatorem problemu jest identyfikator przydzielony przez narzędzie zarządzania usługami informatycznymi (ITSM). Należy go stosować w całej komunikacji związanej z tym problemem.

Procedura zarządzania problemem może zostać uruchomiona w wyniku incydentu lub rozpoczęta z własnej inicjatywy celem naprawienia problemów wykrytych w systemie na dowolnym etapie.

5.2. Określanie priorytetu problemów

Tak samo jak w przypadku incydentów problemom można nadać kategorię odpowiednią dla ich wagi i priorytetu, aby ułatwić ich śledzenie, uwzględniając wpływ powiązanych incydentów i częstotliwość ich występowania.

5.3. Badanie i diagnoza problemu

Każda ze stron może zgłosić problem, a centrum obsługi strony, która rozpoczyna proces, będzie odpowiedzialne za zarejestrowanie problemu, przypisanie go do odpowiedniego zasobu i śledzenie jego ogólnego statusu.

Zespół ds. rozwiązywania problemów, któremu przekazano problem, ma obowiązek zająć się tym problemem w stosownym terminie i komunikować się z centrum obsługi.

Jeżeli zostaną do tego wezwane, obie strony odpowiadają za zapewnienie, aby przydzielone działania zostały przeprowadzone, oraz za przesłanie informacji zwrotnej do centrum obsługi swojej strony.

5.4. Rozwiązanie

Zespół ds. rozwiązywania problemów, któremu przydzielono problem, odpowiada za rozwiązanie tego problemu i za przesłanie stosownych informacji do centrum obsługi swojej strony.

Ustalenia z prac nad problemem należy zarejestrować na przyszłe potrzeby.

5.5. Zamknięcie problemu

Problem jest oficjalnie zamknięty, gdy zostanie naprawiony dzięki wprowadzeniu zmiany. Etap zamknięcia problemu przeprowadza centrum obsługi, które zarejestrowało problem i poinformowało centrum obsługi drugiej strony.

6. REALIZACJA WNIOSKÓW

Proces realizacji wniosków obejmuje kompleksowe zarządzanie wnioskiem dotyczącym nowej lub istniejącej usługi od momentu rejestracji i zatwierdzenia do zamknięcia. Wnioski o usługę to zazwyczaj niewielkie, określone wcześniej, powtarzalne, częste, uprzednio zatwierdzone wnioski o charakterze proceduralnym.

Poniżej przedstawiono najważniejsze działania, które należy przeprowadzić:

6.1. Wszczęcie procedury dotyczącej wniosku

Unijne lub szwajcarskie centrum obsługi otrzymuje informacje dotyczące wniosku o usługę pocztą elektroniczną, telefonicznie, za pośrednictwem narzędzia zarządzania usługami informatycznymi (ITSM) lub jakiegokolwiek innego uzgodnionego kanału komunikacji.

6.2. Rejestracja i analiza wniosku

W przypadku wszystkich wniosków o usługę punktem kontaktowym będzie albo unijne, albo szwajcarskie centrum obsługi w zależności od strony, która zgłosiła wniosek o usługę. Odpowiednie centrum obsługi będzie odpowiedzialne za rejestrację i analizę wniosku o usługę z dochowaniem należytej staranności.

6.3. Zatwierdzenie wniosku

Pracownik centrum obsługi strony, która zgłosiła wniosek o usługę, sprawdza, czy konieczne jest uzyskanie jakichkolwiek zgód od drugiej strony, a jeżeli tak, rozpoczyna proces ich uzyskania. Jeżeli wniosek o usługę nie zostanie zatwierdzony, centrum obsługi odpowiednio aktualizuje i zamyka zgłoszenie.

6.4. Realizacja wniosków

Niniejszy etap jest poświęcony skutecznemu i sprawnemu rozpatrywaniu wniosków o usługę. Należy rozróżnić następujące przypadki:

- realizacja wniosku o usługę wpływa wyłącznie na jedną stronę. W takim przypadku dana strona zleca odpowiednie prace i koordynuje ich wykonanie;
- realizacja wniosku o usługę wpływa zarówno na UE, jak i Szwajcarię. W takim przypadku centra obsługi zlecają prace w obszarach, za które są odpowiedzialne. Centra obsługi koordynują między sobą proces realizacji wniosku o usługę. Ogólna odpowiedzialność spoczywa na centrum obsługi, które otrzymało wniosek o usługę i wszczęło procedurę w jego sprawie.

Po realizacji wniosku o usługę, należy nadać mu status wskazujący, że został rozpatrzony.

6.5. Przekazanie wniosku

W razie potrzeby centrum obsługi może przekazać nierozpatrzony wniosek o usługę do odpowiedniego zasobu (osoby trzeciej).

Wnioski przekazuje się do odpowiednich osób trzecich, tj. wnioski otrzymane przez unijne centrum obsługi muszą przejść przez szwajcarskie centrum obsługi, zanim zostaną przekazane do szwajcarskiej osoby trzeciej – i odwrotnie.

Osoba trzecia, której przekazano wniosek o usługę, ma obowiązek zająć się wnioskiem o usługę w stosownym terminie i komunikować się z centrum obsługi, które przekazało wniosek o usługę.

Centrum obsługi, które zarejestrowało wniosek o usługę, jest odpowiedzialne za śledzenie ogólnego statusu wniosku o usługę i monitorowanie, do kogo jest przypisany.

6.6. Przegląd realizacji wniosku

Właściwe centrum obsługi przedkłada zapis wniosku o usługę do ostatecznej kontroli jakości przed zamknięciem wniosku. Ma to na celu zagwarantowanie, że wniosek o usługę został faktycznie zrealizowany i że dostarczono w odpowiednim stopniu szczegółowości wszystkie informacje niezbędne do opisania cyklu życia wniosku. Ustalenia z prac nad wnioskiem należy ponadto zarejestrować na przyszłe potrzeby.

6.7. Zamknięcie wniosku

Jeżeli strony, którym przypisano wniosek, zgadzają się, że wniosek o usługę został zrealizowany i wnioskodawca uważa sprawę za rozwiązaną, należy nadać wnioskowi status „zamknięty”.

Wniosek o usługę jest formalnie zamknięty, gdy centrum obsługi, które zarejestrowało wniosek o usługę, przeprowadziło etap zamknięcia wniosku i poinformowało centrum obsługi drugiej strony.

7. ZARZĄDZANIE ZMIANĄ

Celem procesu jest zapewnienie stosowania standaryzowanych metod i procedur do sprawnego i szybkiego zarządzania wszystkimi zmianami dotyczącymi kontroli infrastruktury informatycznej, aby zminimalizować liczbę incydentów i ich wpływ na usługę. Zmiany w infrastrukturze informatycznej mogą powstać w reakcji na problemy lub na wymogi narzucone z zewnątrz, np. zmiany w przepisach, lub mogą zostać aktywnie wprowadzone w wyniku dążenia do osiągnięcia większej sprawności i skuteczności lub w celu umożliwienia bądź odzwierciedlenia inicjatyw dotyczących funkcjonowania.

Proces zarządzania zmianami obejmuje szereg różnych działań, w ramach których zbiera się wszystkie informacje szczegółowe na temat wniosku o zmianę na potrzeby przyszłego śledzenia. Procesy te gwarantują, że zmiana zostanie zatwierdzona i przetestowana przed przekazaniem jej do wdrożenia. Za skuteczne wdrożenie odpowiada proces zarządzania wersjami.

7.1. Wniosek o zmianę

Wniosek o zmianę przedkłada się zespołowi zarządzania zmianą do sprawdzenia i zatwierdzenia. W przypadku wszystkich wniosków o zmianę punktem kontaktowym będzie albo unijne, albo szwajcarskie centrum obsługi w zależności od strony, która zgłosiła wniosek. Odpowiednie centrum obsługi będzie odpowiedzialne za rejestrację i analizę wniosku o zmianę z dochowaniem należytej staranności.

Wnioski o zmianę mogą powstać w wyniku:

- incydentu, który wywołuje zmianę;
- istniejącego problemu skutkującego zmianą;
- wniosku użytkownika końcowego o wprowadzenie nowej zmiany;
- zmian będących rezultatem bieżącej konserwacji;
- zmian ustawodawczych.

7.2. Ocena i planowanie zmiany

Niniejszy etap obejmuje działania dotyczące oceny i planowania zmiany. Uwzględnia on działania dotyczące określania priorytetów i planowania służące zminimalizowaniu ryzyka i wpływu.

Jeżeli wdrożenie wniosku o zmianę ma skutki zarówno dla UE, jak i Szwajcarii, strona, która zarejestrowała wniosek o zmianę, przedstawia ocenę i plan zmiany drugiej stronie do weryfikacji.

7.3. Zatwierdzanie zmiany

Każdy zarejestrowany wniosek o zmianę musi zostać zatwierdzony na odpowiednim szczeblu.

7.4. Wdrożenie zmiany

Zmiany wdraża się w ramach procesu zarządzania wersjami. Zespoły ds. zarządzania wersjami obu stron stosują swoje własne procesy, które obejmują planowanie i testowanie. Przeglądu zmiany dokonuje się po zakończeniu wdrażania. Aby zagwarantować, że wszystko poszło zgodnie z planem, obowiązujący proces zarządzania zmianami jest stale poddawany przeglądowi i aktualizowany, gdy jest to konieczne.

8. ZARZĄDZANIE WERSJAMI

Wersja to jedna zmiana w usłudze informatycznej lub większa ich liczba zebrane w planie wersji, które muszą zostać zatwierdzone, przygotowane, stworzone, przetestowane i wdrożone jednocześnie. Wersja może oznaczać poprawkę błędu, zmianę w sprzęcie lub w innych komponentach, zmiany w oprogramowaniu, aktualizacje aplikacji, zmiany w dokumentacji lub w procesach. Zawartość każdej wersji organizuje się, testuje i wdraża jako jedną całość.

Zarządzanie wersjami ma na celu planowanie, tworzenie, testowanie i sprawdzanie oraz zapewnianie zdolności do świadczenia zaprojektowanych usług, które spełnią wymagania zainteresowanych stron i pozwolą osiągnąć zamierzone cele. Kryteria akceptacji wszelkich zmian w usłudze zostaną określone i udokumentowane podczas etapu koordynacji projektu i przekazane do zespołów zarządzania wersjami.

Wersja zazwyczaj składa się z szeregu poprawek służących rozwiązaniu problemu i usprawnieniu usługi. Obejmuje nowe lub zmienione oprogramowanie oraz wszelki nowy lub zmieniony sprzęt niezbędne do wdrożenia zatwierdzonych zmian.

8.1. Planowanie wersji

Pierwszy etap procesu polega na przypisaniu zatwierdzonych zmian do pakietów wersji oraz określeniu zakresu i zawartości wersji. W oparciu o te informacje w podprocesie planowania wersji opracowuje się harmonogram tworzenia, testowania i wdrożenia wersji.

W planowaniu należy określić:

- zakres i zawartość wersji;
- ocenę ryzyka i profil ryzyka dotyczące danej wersji;
- klientów/użytkowników, na których dana wersja wpłynie;
- zespół odpowiedzialny za daną wersję;
- strategię dostarczenia i wdrożenia;
- zasoby na potrzeby danej wersji i jej wdrożenia.

Strony informują się nawzajem o swoich planach dotyczących wersji i planowych pracach konserwacyjnych. Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują swoje plany i ustalają wspólny termin prac konserwacyjnych.

8.2. Tworzenie i testowanie pakietu wersji

Etap tworzenia i testowania w ramach procesu zarządzania wersjami polega na określeniu metody służącej do wykonania wersji lub pakietu wersji oraz do utrzymania środowisk kontrolowanych przed zmianą środowiska produkcyjnego, jak również testowania wszystkich zmian we wszystkich wdrożonych środowiskach.

Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują swoje plany dostarczenia i testy. Obejmuje to następujące aspekty:

- sposób i czas dostarczenia składników wersji i komponentów usługi;
- typowy czas realizacji; procedurę na wypadek opóźnienia;
- sposób śledzenia postępów w dostarczaniu i uzyskiwaniu potwierdzenia;
- wskaźniki służące do monitorowania działań w zakresie dostarczenia wersji oraz do ustalenia, czy zakończyły się pomyślnie;

- wspólne przypadki testowe dotyczące istotnych funkcjonalności i zmian.

Po zakończeniu tego podprocesu wszystkie niezbędne elementy wersji są gotowe do przejścia do etapu wdrożenia do środowiska produkcyjnego.

8.3. Przygotowanie wdrożenia

Podproces przygotowania zapewnia, aby plany komunikacji zostały poprawnie określone, a powiadomienia przygotowane do wysłania do wszystkich zainteresowanych stron i użytkowników końcowych, na których zmiany będą miały wpływ, oraz aby wersja była zintegrowana z procesem zarządzania zmianami celem zagwarantowania, że wszystkich zmian dokonuje się w sposób kontrolowany i po zatwierdzeniu przez odpowiednie fora.

Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują następujące działania:

- zapis wniosków o zmianę na potrzeby ustalenia harmonogramu i przygotowania wdrożenia do środowiska produkcyjnego;
- utworzenie planu wdrożenia;
- metodę cofnięcia zmian, aby w przypadku niepowodzenia wdrożenia można było przywrócić poprzedni stan;
- powiadomienia wysyłane do wszystkich niezbędnych stron;
- zobowiązanie do zatwierdzenia wdrożenia wersji na odpowiednim szczeblu.

8.4. Cofnięcie wersji

Jeżeli wdrożenie nie powiodło się lub podczas testów ustalono, że wdrożenie było nieskuteczne lub nie spełniło uzgodnionych kryteriów akceptacji/jakości, zespoły ds. zarządzania wersjami obu stron muszą cofnąć zmiany i przywrócić poprzedni stan. Należy poinformować wszystkie niezbędne zainteresowane strony, w tym użytkowników końcowych, na których zmiany wpłyną lub których dotyczyły. Z zastrzeżeniem zatwierdzenia proces można rozpocząć od nowa na którymkolwiek z poprzednich etapów.

8.5. Przegląd i zamknięcie wersji

Przegląd wdrożenia powinien obejmować następujące działania:

- zebranie informacji zwrotnych na temat zadowolenia klientów, użytkowników lub zadowolenia ze świadczenia usługi w związku z wdrożeniem (zgromadzenie informacji zwrotnych i ocena ich przydatności dla stałego ulepszania usługi);
- przegląd wszelkich kryteriów jakości, których nie spełniono;
- sprawdzenie kompletności działań, niezbędnych poprawek i zmian;
- upewnienie się, że na koniec wdrożenia nie ma żadnych problemów dotyczących zdolności, zasobów, możliwości lub funkcjonowania;
- sprawdzenie, czy wszystkie problemy, znane błędy i obejścia zostały udokumentowane i zaakceptowane przez klienta, użytkowników końcowych, dział wsparcia operacyjnego i inne strony, których dotyczą zmiany;
- monitorowanie incydentów i problemów wywołanych wdrożeniem (udzielenie wczesnego wsparcia powdrożeniowego zespołom operacyjnym, jeżeli dana wersja spowodowała wzrost ilości pracy);
- aktualizację dokumentacji wsparcia technicznego (tj. dokumentów zawierających informacje techniczne);

- oficjalne przekazanie wdrożenia wersji do działu obsługi usług;
- udokumentowanie wyciągniętych wniosków;
- zebranie podsumowań wersji od zespołów wdrożeniowych;
- oficjalne zamknięcie wersji po weryfikacji zapisu wniosków o zmianę.

9. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie incydentami związanymi z bezpieczeństwem informacji to proces postępowania z incydentami związanymi z bezpieczeństwem informacji w celu umożliwienia przekazania informacji o incydencie zainteresowanym stronom, które mogły zostać nim dotknięte; oceny incydentu i ustalenia jego priorytetu; oraz reakcji na incydent służącej rozstrzygnięciu kwestii wszelkich faktycznych, podejrzewanych lub możliwych przypadków naruszenia poufności, dostępności lub integralności szczególnie chronionych zasobów informacyjnych.

9.1. Kategoryzacja incydentów związanych z bezpieczeństwem informacji

Wszystkie incydenty, które wpływają na powiązanie między rejestrem Unii i rejestrem Szwajcarii, analizuje się pod kątem ustalenia, czy nastąpiło naruszenie poufności, integralności lub dostępności jakichkolwiek danych szczególnie chronionych, które wpisano do wykazu danych szczególnie chronionych.

Jeżeli doszło do naruszenia, incydent określa się jako incydent związany z bezpieczeństwem informacji, natychmiast rejestruje się go w narzędziu zarządzania usługami informatycznymi (ITSM) i postępuje się z nim zgodnie z procedurą stosowaną w takim przypadku.

9.2. Postępowanie z incydentami związanymi z bezpieczeństwem informacji

Incydenty związane z bezpieczeństwem informacji należą do obowiązków trzeciego szczebla i ich rozwiązaniem zajmuje się specjalny zespół ds. zarządzania incydentami.

Zespół ds. zarządzania incydentami odpowiada za:

- przeprowadzenie pierwszej analizy, nadanie incydentowi kategorii i ocenę wagi incydentu;
- koordynację działań między wszystkimi zainteresowanymi stronami, uwzględniając pełną dokumentację analizy incydentu, decyzje podjęte w celu poradzenia sobie z incydentem i ewentualne rozpoznane słabe punkty;
- W zależności od wagi incydentu związanego z bezpieczeństwem informacji – terminowe przekazanie go na odpowiedni szczebel w celu uzyskania informacji lub decyzji.

W procesie zarządzania bezpieczeństwem informacji wszystkie informacje dotyczące incydentów klasyfikuje się jako dane o najwyższym poziomie wrażliwości, ale w żadnym wypadku nie niższym niż SENSITIVE: *ETS*.

W przypadku trwającego postępowania lub słabego punktu, który można nieuczciwie wykorzystać, oraz do momentu jego naprawienia informacje klasyfikuje się jako SPECIAL HANDLING: *ETS Critical*.

9.3. Identyfikacja incydentów związanych z bezpieczeństwem informacji

W zależności od rodzaju zdarzenia związanego z bezpieczeństwem, osoba odpowiedzialna za bezpieczeństwo informacji określa odpowiednie organizacje w celu podjęcia z nimi współpracy i włączenia ich do zespołu ds. zarządzania incydentami.

9.4. Analiza incydentów związanych z bezpieczeństwem informacji

Zespół ds. zarządzania incydentami działa w porozumieniu ze wszystkimi zaangażowanymi organizacjami i odpowiednimi członkami ich zespołów, w stosownych przypadkach, w celu zbadania incydentu. Podczas analizy ustala się skalę utraty poufności, integralności lub dostępności zasobu i ocenia się skutki dla wszystkich organizacji, których dotyczy incydent. Następnie określa się działania wstępne i następcze mające na celu rozwiązanie incydentu i zarządzanie jego wpływem, w tym wpływ tych działań na zasoby.

9.5. Ocena wagi incydentu związanego z bezpieczeństwem informacji, przekazywanie go i związana z nim sprawozdawczość

Po określeniu charakteru każdego nowego incydentu związanego z bezpieczeństwem informacji jako incydent związany z bezpieczeństwem informacji, zespół ds. zarządzania incydentami ocenia jego wagę i rozpoczyna najpilniejsze niezbędne działania zgodnie z wagą incydentu.

9.6. Sprawozdawczość dotycząca reakcji na incydent związany z bezpieczeństwem informacji

Zespół ds. zarządzania incydentami uwzględnia rezultaty działań służących ograniczeniu skutków incydentu i przywróceniu do stanu używalności w sprawozdaniu w sprawie reakcji na incydent związany z bezpieczeństwem informacji. Sprawozdanie przekazuje się na trzeci szczebel za pośrednictwem zabezpieczonej poczty elektronicznej lub innych wspólnie przyjętych metod bezpiecznej komunikacji.

Właściwa strona zapoznaje się z rezultatami działań służących ograniczeniu skutków incydentu i przywróceniu do stanu używalności oraz:

- przywraca połączenie z rejestrem, jeżeli zostało przerwane;
- przekazuje komunikaty dotyczące incydentu zespołom odpowiedzialnym za rejestr;
- zamyka incydent.

Zespół ds. zarządzania incydentami powinien uwzględnić w sprawozdaniu w sprawie incydentu związanego z bezpieczeństwem informacji – stosując bezpieczne metody – istotne dane szczegółowe, aby zapewnić spójną rejestrację i komunikację oraz umożliwić podjęcie szybkich i odpowiednich działań służących ograniczeniu skutków incydentu. Po zakończeniu prac nad sprawozdaniem zespół ds. zarządzania incydentami przedstawia w odpowiednim terminie sprawozdanie końcowe w sprawie incydentu związanego z bezpieczeństwem informacji.

9.7. Monitorowanie, budowanie zdolności i stałe dążenie do doskonałości

Zespół ds. zarządzania incydentami dostarczy sprawozdania w sprawie wszystkich incydentów związanych z bezpieczeństwem informacji na trzeci szczebel. Sprawozdania zostaną wykorzystane na tym szczeblu do ustalenia:

- słabych punktów w mechanizmach kontrolnych lub operacjach dotyczących bezpieczeństwa, które należy wzmocnić;
- ewentualnej potrzeby w kwestii ulepszenia niniejszej procedury, aby zwiększyć skuteczność reakcji na incydenty;
- możliwości dotyczących szkolenia i budowania zdolności w celu dodatkowego wzmocnienia odporności systemów rejestrów w zakresie bezpieczeństwa informacji, ograniczenia ryzyka zaistnienia przyszłych incydentów i zminimalizowania ich wpływu.

10. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie bezpieczeństwem informacji ma na celu zapewnienie poufności, integralności i dostępności należących do danej organizacji niejawnych informacji, danych i usług informatycznych. Poza elementami technicznymi, w tym informacjami na temat ich budowy i testów (zob. normy techniczne powiązania), do spełnienia wymogów w zakresie bezpieczeństwa dotyczących stałego powiązania rejestrów konieczne są następujące wspólne procedury operacyjne:

10.1. Identyfikacja danych szczególnie chronionych

Wrażliwość elementu danych ocenia się poprzez ustalenie, jaki wpływ na działalność (np. straty finansowe, utrata wizerunku, naruszenie przepisów...) miałoby naruszenie bezpieczeństwa związane z taką informacją.

Szczególnie chronione zasoby informacyjne identyfikuje się na podstawie wpływu, jaki mają na powiązanie.

Poziom wrażliwości tych danych ocenia się zgodnie ze skalą wrażliwości obowiązującą w przypadku przedmiotowego powiązania i opisaną szczegółowo w sekcji niniejszego dokumentu zatytułowanej „Postępowanie z incydentami związanymi z bezpieczeństwem informacji".

10.2. Poziomy wrażliwości zasobów informacyjnych

Po identyfikacji zasobu informacyjnego klasyfikuje go się za pomocą następujących zasad:

- jeżeli określono, że co najmniej jeden z następujących aspektów – poufności, integralności lub dostępności – znajduje się na poziomie WYSOKIM, zasób klasyfikuje się do grupy SPECIAL HANDLING: *ETS Critical*.
- jeżeli określono, że co najmniej jeden z następujących aspektów – poufności, integralności lub dostępności – znajduje się na poziomie ŚREDNIM, zasób klasyfikuje się do grupy SENSITIVE: *ETS*;
- jeżeli określono, że następujące aspekty – poufności, integralności lub dostępności – znajdują się wyłącznie na poziomie NISKIM, zasób klasyfikuje się jako oznaczenie UE: SENSITIVE: *ETS Joint Procurement.* Oznaczenie CH: LIMITED: ETS.

10.3. Przypisywanie zasobów informacyjnych do właściciela

Wszystkie zasoby informacyjne powinny być przypisane do określonego właściciela. Zasoby informacyjne ETS należące do powiązania między EUTL i SSTL lub z nim związane powinny zostać zawarte we wspólnym wykazie zasobów utrzymywanym przez obie strony. Zasoby informacyjne ETS poza powiązaniem między EUTL i SSTL powinny zostać zawarte w wykazie zasobów utrzymywanym przez odpowiednią stronę.

Strony uzgodnią, kto jest właścicielem każdego zasobu informacyjnego należącego do powiązania między EUTL i SSTL lub z nim związanego. Właściciel zasobu informacyjnego odpowiada za ocenę jego wrażliwości.

Właściciel powinien posiadać poziom uprzywilejowania stosowny do wartości przypisanego mu zasobu lub przypisanych mu zasobów. Należy uzgodnić i sformalizować odpowiedzialność właściciela za zasób lub zasoby oraz obowiązek utrzymywania przez niego wymaganego poziomu poufności, integralności i dostępności.

10.4. Rejestracja danych szczególnie chronionych

Wszystkie dane szczególnie chronione rejestruje się w wykazie danych szczególnie chronionych.

W stosownych przypadkach uwzględnia się i rejestruje w wykazie danych szczególnie chronionych agregację danych szczególnie chronionych, która mogłaby wywołać większy wpływ niż pojedynczy element danych (np. zbiór danych przechowywanych w bazie danych systemu).

Wykaz danych szczególnie chronionych nie jest niezmienny. Zagrożenia, luki w zabezpieczeniach, prawdopodobieństwo lub skutki incydentów związanych z bezpieczeństwem informacji powiązane z tymi zasobami mogą się zmienić bez ostrzeżenia, a do działalności systemów rejestrów mogą zostać wprowadzone nowe zasoby.

W związku z tym należy dokonywać regularnego przeglądu wykazu danych szczególnie chronionych i natychmiast rejestrować w nim wszelkie nowe dane zidentyfikowane jako szczególnie chronione.

Każdy zapis w wykazie danych szczególnie chronionych obejmuje co najmniej następujące informacje:

- opis danych,
- właściciela danych,
- poziom wrażliwości,
- wskazanie, czy dane zawierają dane osobowe,
- dodatkowe informacje, jeżeli są wymagane.

10.5. Postępowanie z danymi szczególnie chronionymi

Podczas przetwarzania poza powiązaniem między rejestrem Unii i rejestrem Szwajcarii z danymi szczególnie chronionymi postępuje się zgodnie z instrukcjami postępowania z informacjami.

Z danymi szczególnie chronionymi przetwarzanymi w ramach powiązania między rejestrem Unii i rejestrem Szwajcarii postępuje się zgodnie z wymogami stron dotyczącymi bezpieczeństwa.

10.6. Zarządzanie dostępem

Celem zarządzania dostępem jest przyznawanie upoważnionym użytkownikom praw do korzystania z usługi oraz uniemożliwienie dostępu użytkownikom nieupoważnionym. Zarządzanie dostępem jest czasem jest nazywane „zarządzaniem prawami” lub „zarządzaniem tożsamością”.

W przypadku stałego powiązania rejestrów i jego działania obie strony muszą posiadać dostęp do następujących elementów:

- Wiki: środowiska współpracy służącego do wymiany wspólnych informacji, takich jak planowanie wersji;
- narzędzia zarządzania usługami informatycznymi (ITSM) służącego do zarządzania incydentami i problemami (zob. rozdział 3 „Podejście i normy”);
- systemu wymiany wiadomości: każda ze stron zapewnia bezpieczny system przekazywania wymiany wiadomości na potrzeby przesyłania wiadomości zawierających dane dotyczące transakcji.

Administrator rejestru Szwajcarii i centralny administrator Unii zapewniają, aby prawa dostępu były aktualne, i pełnią rolę punktów kontaktowych dla swoich stron w odniesieniu do działań związanych

z zarządzaniem dostępem. Wnioski o dostęp rozpatruje się zgodnie z procedurami realizacji wniosków.

10.7. Zarządzanie certyfikatami/kluczami

Każda ze stron odpowiada za zarządzanie własnymi certyfikatami/kluczami (generowanie, rejestracja, przechowywanie, instalacja, stosowanie, odnawianie, cofanie, tworzenie kopii zapasowej i odzyskiwanie certyfikatów/kluczy). Jak określono w normach technicznych powiązania, stosuje się jedynie certyfikaty elektroniczne wydane przez centrum certyfikacji uznawane przez obie strony. Postępowanie z certyfikatami/kluczami i ich przechowywanie muszą być zgodnie z przepisami zawartymi w instrukcjach postępowania z informacjami.

Strony koordynują między sobą wszelkie cofnięcie lub odnowienie certyfikatów i kluczy. Odbywa się to zgodnie z procedurami realizacji wniosków.

Administrator rejestru Szwajcarii i centralny administrator Unii wymienią się certyfikatami/kluczami za pośrednictwem zabezpieczonych środków komunikacji zgodnie z przepisami określonymi w instrukcjach postępowania z informacjami.

Wszelka weryfikacja certyfikatów/kluczy dokonywana jakąkolwiek metodą pomiędzy stronami odbędzie się w sposób pozapasmowy.

ZAŁĄCZNIK III

NORMY TECHNICZNE POWIĄZANIA

na podstawie art. 3 ust. 7 Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych

Norma stałego powiązania rejestrów

Spis treści

1. Glosariusz 30
2. Wprowadzenie 33
2.1. Zakres 33
2.2. Adresaci 34
3. Przepisy ogólne 34
3.1. Architektura łącza komunikacyjnego 34
3.1.1. Wymiana wiadomości 34
3.1.2. Wiadomość XML – opis wysokiego poziomu 34
3.1.3. Okna przyjmowania 35
3.1.4. Przepływy wiadomości związanych z transakcją 35
3.2. Bezpieczeństwo przesyłania danych 38
3.2.1. Zapora sieciowa i połączenie międzysieciowe 38
3.2.2. Wirtualna sieć prywatna (VPN) 38
3.2.3. Wdrażanie IPSec 39
3.2.4. Protokół bezpiecznego przekazywania wymiany wiadomości 39
3.2.5. Szyfrowanie i podpisywanie w formacie XML 39
3.2.6. Klucze kryptograficzne 39
3.3. Wykaz funkcji w ramach powiązania 40
3.3.1. Transakcje handlowe 40
3.3.2. Protokół uzgadniania 40
3.3.3. Komunikat testowy 41
3.4. Wymogi rejestracji danych 41
3.5. Wymogi operacyjne 42
4. Przepisy dotyczące dostępności 43
4.1. Opracowywanie dostępności komunikacji 43
4.2. Plan dotyczący inicjowania, komunikacji, ponownej aktywacji oraz testów 43
4.2.1. Testy wewnętrznej infrastruktury z zakresu technologii informacyjno-komunikacyjnych 44

4.2.2. Testy komunikacji 44
4.2.3. Testy całego systemu (koniec-koniec) 44
4.2.4. Testy bezpieczeństwa 45
4.3. Środowisko akceptacyjne/testowe 45
5. Przepisy dotyczące poufności i integralności 46
5.1. Infrastruktura testowania bezpieczeństwa 46
5.2. Przepisy dotyczące zawieszenia i ponownej aktywacji powiązania 46
5.3. Przepisy dotyczące naruszenia bezpieczeństwa 47
5.4. Wytyczne dotyczące testowania bezpieczeństwa 47
5.4.1. Oprogramowanie 47
5.4.2. Infrastruktura 48
5.5. Przepisy dotyczące oceny ryzyka 48

1. GLOSARIUSZ

Tabela 1-1 Akronimy i definicje branżowe

Akronim/termin	Definicja
Uprawnienie	Uprawnienie do emisji jednej tony ekwiwalentu dwutlenku węgla w określonym okresie, które jest ważne jedynie na potrzeby spełnienia wymogów w ramach ETS któregokolwiek podmiotu
CH	Konfederacja Szwajcarska
CHU	Rodzaj uprawnienia stacjonarnego, zwanego również CHU2 (w odniesieniu do drugiego okresu rozliczeniowego protokołu z Kioto), wydawanego przez CH
CHUA	Szwajcarskie uprawnienie do emisji lotniczych
COP	Wspólne procedury operacyjne Procedury opracowane wspólnie w celu uruchomienia powiązania między EU ETS a ETS Szwajcarii
ETR	Rejestr handlu uprawnieniami do emisji
ETS	System uprawnieniami do emisji
UE	Unia Europejska
EUA	Unijne uprawnienie do emisji ogólnych

Akronim/termin	Definicja
EUAA	Unijne uprawnienie do emisji lotniczych
EUCR	Skonsolidowany rejestr Unii Europejskiej
EUTL	Dziennik transakcji Unii Europejskiej
Rejestr	System rejestracji uprawnień przyznanych na podstawie ETS służący do śledzenia własności uprawnień utrzymywanych na kontach elektronicznych
SSTL	Dodatkowy dziennik transakcji Szwajcarii
Transakcja	Proces w rejestrze dotyczący przekazywania uprawnienia z jednego rachunku na inny
System dziennika transakcji	Dziennik transakcji zawiera zapis każdej propozycji transakcji wysyłanej z jednego rejestru do drugiego

Tabela 1-2 Techniczne akronimy i definicje

Akronim	Definicja
Kryptografia asymetryczna	Wykorzystuje klucze publiczne i prywatne do zaszyfrowania i odszyfrowania danych
Centrum certyfikacji	Podmiot, który wydaje certyfikaty elektroniczne
Klucz kryptograficzny	Informacja, która określa wynik funkcjonalny algorytmu kryptograficznego
Odszyfrowywanie	Proces odwrotny do szyfrowania
Podpis cyfrowy	Technika matematyczna stosowana do sprawdzania autentyczności i integralności wiadomości, oprogramowania lub dokumentu elektronicznego
Szyfrowanie	Proces przekształcenia informacji lub danych w kod, w szczególności aby uniemożliwić dostęp osobom nieupoważnionym
Przyjmowanie pliku	Proces odczytywania pliku
Zapora sieciowa	Urządzenie lub oprogramowanie bezpieczeństwa monitorujące i kontrolujące przychodzący i wychodzący ruch sieciowy na podstawie wcześniej określonych reguł
Monitorowanie pulsu	Okresowy sygnał generowany i monitorowany przez sprzęt lub oprogramowanie celem wskazania normalnego funkcjonowania lub zsynchronizowania innych części systemu komputerowego
IPSEC	Protokół IP Security Zestaw protokołów sieciowych, które uwierzytelniają i szyfrują pakiety danych w celu zapewnienia bezpiecznej szyfrowanej komunikacji między dwoma komputerami za pośrednictwem sieci protokołu internetowego
Testy penetracyjne	Praktyka testowania systemu komputerowego, sieci lub aplikacji internetowej służąca znalezieniu luk w zabezpieczeniach, które mógłby wykorzystać atakujący
Proces uzgadniania	Proces zapewniania, aby dwa zbiory wpisów były zgodne
VPN	Wirtualna sieć prywatna

Akronim	Definicja
XML	Rozszerzalny język znaczników Pozwala programistom na stworzenie własnych niestandardowych znaczników umożliwiających określanie, przesyłanie, sprawdzanie i interpretowanie danych między aplikacjami i między organizacjami

2. WPROWADZENIE

Umowa między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych z dnia 23 listopada 2017 r. („umowa") przewiduje wzajemne uznawanie uprawnień do emisji, które można wykorzystać na potrzeby dostosowania się do wymogów systemu handlu uprawnieniami do emisji Unii Europejskiej („EU ETS") lub systemu handlu uprawnieniami do emisji Szwajcarii („ETS Szwajcarii"). W celu uruchomienia powiązania między EU ETS a ETS Szwajcarii ustanowione zostanie bezpośrednie powiązanie między dziennikiem transakcji Unii Europejskiej (EUTL) rejestru Unii a dodatkowym dziennikiem transakcji Szwajcarii (SSTL) rejestru Szwajcarii, co umożliwi bezpośrednie przekazywanie między rejestrami uprawnień do emisji wydanych w ramach któregokolwiek z ETS (art. 3 ust. 2 umowy). W celu uruchomienia powiązania między EU ETS i ETS Szwajcarii w 2020 r. wdrożono tymczasowe rozwiązanie. Od 2023 r. powiązanie rejestrów między dwoma systemami handlu uprawnieniami do emisji będzie stopniowo przekształcane w stałe powiązanie rejestrów, które ma zostać wdrożone nie później niż w 2024 r., co umożliwi funkcjonowanie powiązanych rynków w odniesieniu do korzyści płynących z płynności rynku i realizację transakcji między dwoma powiązanymi systemami w sposób równoważny jednemu rynkowi składającemu się z dwóch systemów i który umożliwia uczestnikom rynku działanie tak, jakby byli na jednym rynku, z zastrzeżeniem jedynie indywidualnych przepisów wykonawczych stron (załącznik II do umowy).

Na podstawie art. 3 ust. 7 umowy administrator rejestru Szwajcarii i centralny administrator rejestru Unii opracowują normy techniczne powiązania oparte na zasadach określonych w załączniku II do umowy, opisując szczegółowe wymogi ustanowienia solidnego i bezpiecznego połączenia między SSTL i EUTL. Normy techniczne powiązania opracowane przez administratorów stają się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

Normy techniczne powiązania zostały przyjęte przez Wspólny Komitet decyzją nr 2/2020. Zaktualizowane normy techniczne powiązania w formie przedstawionej w niniejszym dokumencie zostaną przyjęte przez Wspólny Komitet decyzją nr 1/2024. Zgodnie ze wspomnianą decyzją i wnioskiem Wspólnego Komitetu administrator rejestru Szwajcarii i centralny administrator Unii opracowali dalsze wytyczne techniczne celem uruchomienia powiązania oraz będą je aktualizować celem zapewnienia, aby były one stale dostosowywane do postępu technicznego lub nowych wymogów związanych z bezpieczeństwem i ochroną tego powiązania oraz jego skutecznym i sprawnym funkcjonowaniem.

2.1. Zakres

Niniejszy dokument odzwierciedla wspólne rozumienie stron umowy w kwestii ustanowienia technicznych podstaw powiązania między rejestrami EU ETS i ETS Szwajcarii. Chociaż nakreślono w nim podstawę specyfikacji technicznych pod względem wymogów dotyczących architektury,

obsługi i bezpieczeństwa, do uruchomienia powiązania potrzebne będą dalsze szczegółowe wytyczne.

Jeżeli chodzi o prawidłowe funkcjonowanie, powiązanie będzie wymagało procesów i procedur do dalszego uruchomienia powiązania. Zgodnie z art. 3 ust. 6 umowy kwestie te szczegółowo opisano w osobnym dokumencie na temat wspólnych procedur operacyjnych, przyjętym decyzją Wspólnego Komitetu.

2.2. Adresaci

Niniejszy dokument skierowany jest do administratora rejestru Szwajcarii i centralnego administratora rejestru Unii.

3. PRZEPISY OGÓLNE

3.1. Architektura łącza komunikacyjnego

Celem tej sekcji jest przedstawienie opisu ogólnej architektury uruchomienia powiązania między EU ETS i ETS Szwajcarii oraz związanych z tym poszczególnych komponentów.

Ponieważ bezpieczeństwo jest podstawową częścią określenia architektury, wprowadzono wszelkie środki mające na celu zapewnienie solidnej architektury. Stałe połączenie rejestrów wykorzystuje mechanizm wymiany plików stosując bezpieczne połączenie „Air Gap".

Rozwiązanie techniczne wykorzystuje:

- protokół bezpiecznego przekazywania wymiany wiadomości,
- wiadomości XML,
- podpis cyfrowy i szyfrowanie oparte na standardzie XML,
- VPN.

Poniższy wykres przedstawia ogólny obraz architektury stałego powiązania rejestrów:

3.1.1. Wymiana wiadomości

Podstawą komunikacji między rejestrem Unii a rejestrem Szwajcarii jest mechanizm wymiany wiadomości za pośrednictwem bezpiecznych kanałów. Każdy koniec opiera się na własnym repozytorium otrzymanych wiadomości.

Obie strony prowadzą dziennik otrzymywanych wiadomości wraz ze szczegółowymi informacjami na temat przetwarzania.

Błędy lub nieoczekiwany status wymagają zgłoszenia jako w postaci ostrzeżenia oraz kontaktu między osobami należącymi do zespołów wsparcia.

Błędy i nieoczekiwane zdarzenia są obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi zarządzania incydentami.

3.1.2. Wiadomość XML – opis wysokiego poziomu

Wiadomość XML obejmuje jeden z następujących elementów:

- co najmniej jeden wniosek o transakcję lub przynajmniej jedną odpowiedź na wniosek o transakcję,

- jedną operację/odpowiedź związaną z uzgodnieniem,
- jedną wiadomość testową.

Każda wiadomość zawiera nagłówek z:

- nazwą systemu ETS pochodzenia,
- numerem porządkowym.

3.1.3. Okna przyjmowania

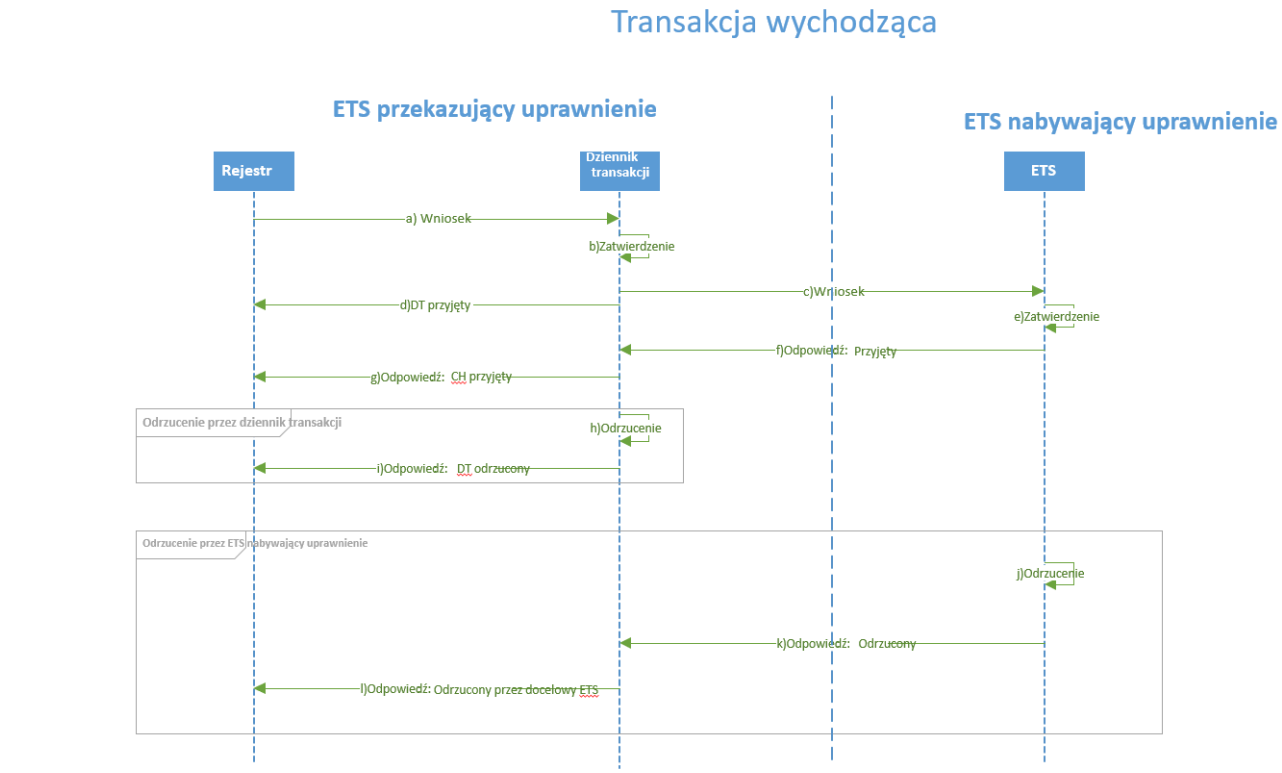
Stałe powiązanie rejestrów opiera się na wcześniej określonych oknach przyjmowania, po których następuje seria nazwanych zdarzeń. Wnioski o transakcje otrzymane za pośrednictwem powiązania zostaną przyjęte wyłącznie w uprzednio ustalonych odstępach i wiążą się ze sprawdzeniem wychodzących i przychodzących transakcji pod względem technicznym. Ponadto uzgodnienia można prowadzić codziennie i inicjować ręcznie.

Zmiany częstotliwości lub terminów każdego z tych zdarzeń będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi realizacji wniosków.

3.1.4. Przepływy wiadomości związanych z transakcją

Transakcje wychodzące

Odzwierciedla to perspektywę ETS przekazującego uprawnienie. Ten konkretny przepływ zobrazowano na kolejnym schemacie sekwencji:



Główny przepływ obejmuje następujące etapy (jak na rysunku powyżej):

a) w przypadku ETS przekazującego uprawnienie wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego),

b) dziennik transakcji zatwierdza wniosek o transakcję,

c) wniosek o transakcję jest wysyłany do ETS przeznaczenia,

d) odpowiedź o przyjęciu jest wysyłana do rejestru ETS pochodzenia,

e) ETS przeznaczenia zatwierdza wniosek o transakcję,

f) ETS przeznaczenia wysyła odpowiedź o przyjęciu z powrotem do dziennika transakcji ETS pochodzenia,

g) dziennik transakcji wysyła do rejestru odpowiedź o przyjęciu.

Alternatywny przepływ „odrzucenia przez dziennik transakcji" (jak na rysunku powyżej, począwszy od lit. a) w przepływie głównym):

a) w systemie pochodzenia wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego),

b) dziennik transakcji nie zatwierdza wniosku,

c) wiadomość o odrzuceniu jest wysyłana do rejestru pochodzenia.

Alternatywny przepływ „odrzucenia przez ETS" (jak na rysunku powyżej, począwszy od lit. d) w przepływie głównym):

a) w ETS pochodzenia wniosek o transakcję jest wysyłany z rejestru do dziennika transakcji po zakończeniu się wszystkich opóźnień w działalności (w stosownych przypadkach opóźnienia 24-godzinnego),

b) dziennik transakcji zatwierdza transakcję,

c) wniosek o transakcję jest wysyłany do ETS przeznaczenia,

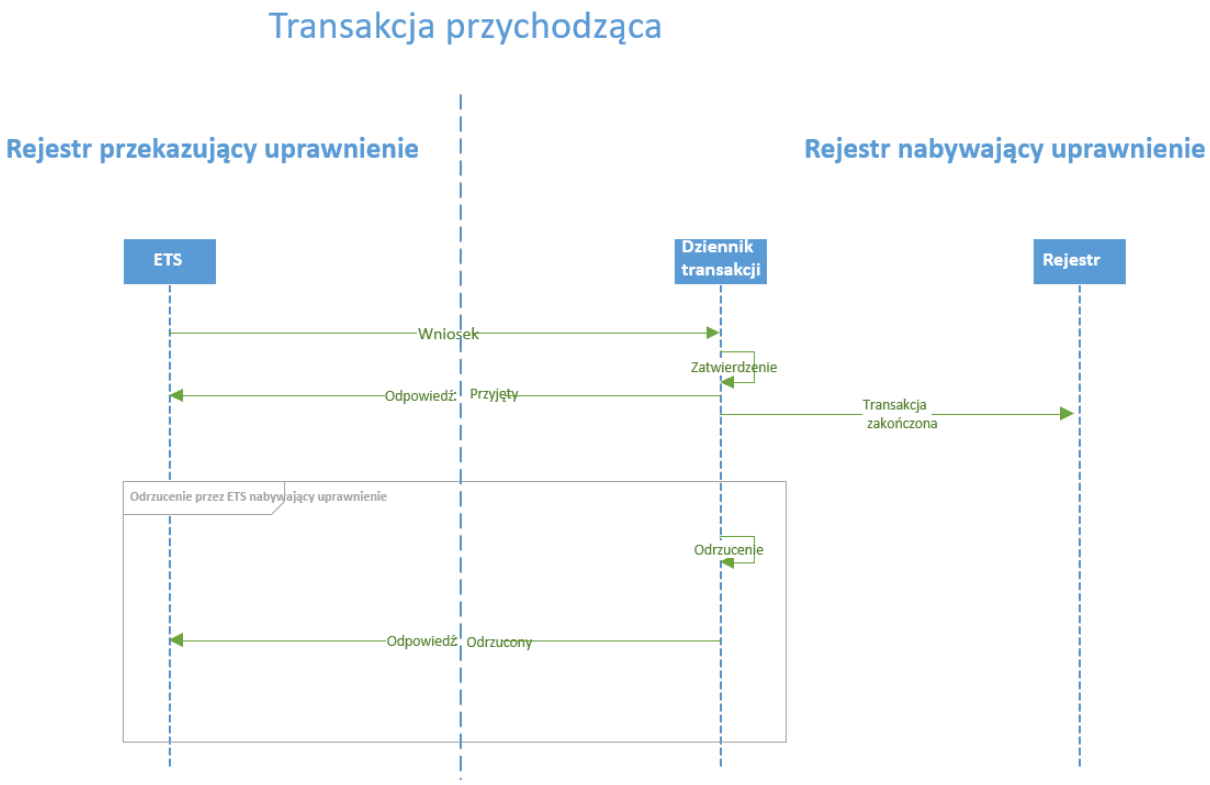
d) wiadomość o przyjęciu jest wysyłana do rejestru ETS pochodzenia,

e) dziennik transakcji ETS nabywającego uprawnienie nie zatwierdza transakcji,

f) ETS nabywający uprawnienie wysyła odpowiedź odmowną do dziennika transakcji ETS przekazującego uprawnienie,

g) dziennik transakcji wysyła odmowę do rejestru.

Transakcje przychodzące



Odzwierciedla to perspektywę ETS nabywającego uprawnienie. Ten konkretny przepływ zobrazowano na kolejnym schemacie sekwencji:

Na schemacie tym przedstawiono:

1) sytuację, w której jeżeli dziennik transakcji ETS nabywającego uprawnienie zatwierdzi wniosek, to wysyła wiadomość o przyjęciu do ETS przekazującego uprawnienie oraz wiadomość „transakcja zakończona” do rejestru ETS nabywającego uprawnienie,

2) sytuację, w której jeżeli dziennik transakcji systemu nabywającego uprawnienie odmówi przyjęcia wniosku przychodzącego i wniosek ten zostanie odrzucony, wniosek o transakcję nie jest wysyłany do rejestru ETS nabywającego uprawnienie.

Protokół

Cykl wiadomości związanych z transakcją obejmuje jedynie dwie wiadomości:

- ETS przekazujący uprawnienie → propozycja transakcji z ETS nabywającego uprawnienie,
- ETS nabywający uprawnienie → odpowiedź na wniosek o transakcję ETS przekazującego uprawnienie: albo o przyjęciu, albo odrzuceniu (w tym powód odrzucenia),
  - przyjęty: transakcja zostaje zakończona,
  - odrzucony: transakcja zostaje przerwana.

Status transakcji

- Status transakcji w ETS przekazującym uprawnienie zostanie ustawiony na „proponowana” po wysłaniu wniosku,
- status transakcji w ETS nabywającym uprawnienie zostanie ustawiony na „proponowana” po otrzymaniu wniosku i w czasie jego rozpatrywania,
- status transakcji w ETS nabywającym uprawnienie zostanie ustawiony na „zakończona”/„przerwana” po przetworzeniu propozycji. ETS nabywający uprawnienie wyśle wówczas odpowiednią wiadomość o przyjęciu/odrzuceniu,
- status transakcji w ETS przekazującym uprawnienie zostanie ustawiony na zakończona/przerwana po otrzymaniu i przetworzeniu wiadomości o przyjęciu/odrzuceniu,
- w przypadku nieotrzymania odpowiedzi, status transakcji w ETS przekazującym uprawnienie pozostanie ustawiony jako proponowana,
- ETS nabywający uprawnienie ustawi na „przerwana” status każdej transakcji pozostającej jako proponowana dłużej niż 30 minut.

Incydenty związane z transakcjami będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi zarządzania incydentami.

3.2. Bezpieczeństwo przesyłania danych

Przekazywane dane będą podlegać czterem poziomom bezpieczeństwa:

1) kontroli dostępu do sieci: zapora sieciowa i warstwa połączenia międzysieciowego,
2) szyfrowaniu na poziomie przesyłania: VPN.
3) szyfrowaniu na poziomie sesji: protokół bezpiecznego przekazywania wymiany wiadomości,
4) szyfrowaniu na poziomie aplikacji: szyfrowanie treści i podpisywanie w formacie XML.

3.2.1. Zapora sieciowa i połączenie międzysieciowe

Powiązanie ustanawia się za pośrednictwem sieci zabezpieczonej sprzętową zaporą sieciową. Zaporę sieciową konfiguruje się za pomocą reguł w taki sposób, aby wyłącznie „zarejestrowani” klienci mogli połączyć się z serwerem VPN.

3.2.2. Wirtualna sieć prywatna (VPN)

Wszelka komunikacja między stronami jest zabezpieczana z wykorzystaniem technologii wirtualnej sieci prywatnej (VPN). Technologie VPN zapewniają możliwość „tworzenia korytarza” przez sieć taką jak internet z jednego punktu do drugiego, zabezpieczającego wszelką komunikację. Przed stworzeniem korytarza VPN wydawany jest certyfikat elektroniczny dla punktu końcowego potencjalnego klienta, co pozwala klientowi na dostarczenie potwierdzenia tożsamości w trakcie negocjowania połączenia. Każda ze stron jest odpowiedzialna za zainstalowanie certyfikatu w swoim punkcie końcowym VPN. Korzystając z certyfikatu elektronicznego, każdy końcowy serwer VPN uzyska dostęp do centrum certyfikacji w celu negocjowania danych uwierzytelniających. Podczas procesu tworzenia korytarza negocjowane jest szyfrowanie, zapewniające, aby wszelka komunikacja za pośrednictwem korytarza była zabezpieczona.

Punkty końcowe klienta VPN konfiguruje się, aby na stałe utrzymać korytarz VPN w celu umożliwienia niezawodnej, dwustronnej komunikacji między stronami w czasie rzeczywistym w dowolnym momencie.

Ogólnie rzecz biorąc, Unia Europejska wykorzystuje zabezpieczoną transeuropejską telematyczną sieć komunikacyjną między administracjami (STESTA) jako prywatną sieć opartą na IP. W związku z tym sieć ta jest również odpowiednia dla stałego powiązania rejestrów.

3.2.3. Wdrażanie IPSec

Stosowanie protokołu IPSec celem utworzenia międzylokacyjnej infrastruktury VPN zapewni międzylokacyjne uwierzytelnianie, integrację i szyfrowanie danych. Konfiguracje IPSec w VPN zapewniają właściwe uwierzytelnianie między dwoma punktami końcowymi połączenia VPN. Strony zidentyfikują i uwierzytelnią zdalnego klienta za pośrednictwem połączenia IPSec, korzystając z certyfikatów elektronicznych wydanych przez centrum certyfikacji i uznawanych przez drugi koniec.

IPSec zapewnia również integralność danych wszelkiej komunikacji prowadzonej za pośrednictwem korytarza VPN. Pakiety danych są skracane i podpisywane z wykorzystaniem informacji uwierzytelniających ustanowionych przez VPN. Poufność danych jest zapewniana w podobny sposób – poprzez umożliwienie szyfrowania IPSec.

3.2.4. Protokół bezpiecznego przekazywania wymiany wiadomości

Stałe powiązanie rejestrów opiera się na wielu warstwach szyfrowania służących bezpiecznej wymianie danych między stronami. Oba systemy i ich różne środowiska są wzajemnie powiązane na poziomie sieci za pomocą korytarzy VPN. Na poziomie aplikacji pliki są przekazywane z wykorzystaniem protokołu bezpiecznego przekazywania wymiany wiadomości na poziomie sesji.

3.2.5. Szyfrowanie i podpisywanie w formacie XML

W ramach plików XML podpisywanie i szyfrowanie odbywa się na dwóch poziomach. Każdy wniosek o transakcję, odpowiedź na wniosek o transakcję oraz komunikat dotyczący uzgodnienia są elektronicznie podpisywane indywidualnie.

Na drugim etapie każdy element podrzędny elementu „wiadomość” jest indywidualnie szyfrowany.

Ponadto, jako trzeci etap i w celu zapewnienia integralności i niezaprzeczalności całej wiadomości, wiadomość będąca elementem podstawowym jest podpisywana elektronicznie. Skutkuje to wysokim poziomem zabezpieczenia danych opartych na formacie XML. Przy technicznym wdrożeniu przestrzega się norm ustanowionych przez konsorcjum World Wide Web.

Aby odszyfrować i zweryfikować wiadomość proces jest wykonywany w odwrotnej kolejności.

3.2.6. Klucze kryptograficzne

Do celów szyfrowania i podpisywania stosowana będzie kryptografia wykorzystująca klucz publiczny.

W szczególnym przypadku IPSec korzysta się z certyfikatu elektronicznego wydanego przez centrum certyfikacji i uznawanego przez obie strony. To centrum certyfikacji weryfikuje tożsamość i wydaje certyfikaty, które są wykorzystywane do niepodważalnej identyfikacji organizacji i ustanowienia kanałów bezpiecznej transmisji danych między stronami.

Z kluczy kryptograficznych korzysta się do podpisywania i szyfrowania kanałów komunikacji i plików z danymi. Publiczne certyfikaty są elektronicznie wymieniane między stronami z wykorzystaniem bezpiecznych kanałów i weryfikowane w sposób pozapasmowy. Procedura ta stanowi integralną część procesu zarządzania bezpieczeństwem informacji określonego we wspólnych procedurach operacyjnych.

3.3. Wykaz funkcji w ramach powiązania

Powiązanie określa system przesyłania szeregu funkcji realizujących procesy biznesowe wynikające z umowy. Powiązanie obejmuje również specyfikację procesu uzgadniania oraz wiadomości testowych, które umożliwią wdrożenie monitorowania pulsu.

3.3.1. Transakcje handlowe

Z perspektywy handlowej powiązanie uwzględnia cztery (4) rodzaje wniosków o transakcję.

- Przekazanie z zewnątrz:
  - po wejściu w życie powiązania ETS unijne i szwajcarskie uprawnienia będą zamienne i tym samym ich przekazanie między stronami będzie w pełni możliwe,
  - wysłanie przekazania za pośrednictwem powiązania będzie obejmowało rachunek przekazującego w ETS oraz rachunek nabywającego w drugim ETS,
  - przekazanie może obejmować dowolną liczbę czterech (4) rodzajów uprawnień:
    - szwajcarskich uprawnień do emisji ogólnych (CHU);
    - szwajcarskich uprawnień do emisji lotniczych (CHUA);
    - unijnych uprawnień do emisji ogólnych (EUA);
    - unijnych uprawnień do emisji lotniczych (EUAA).
- Przydział międzynarodowy:

operatorzy statku powietrznego administrowani za pośrednictwem jednego ETS mający obowiązki wobec drugiego ETS oraz uprawnieni do otrzymania bezpłatnych uprawnień od tego drugiego ETS otrzymają bezpłatne uprawnienia do emisji lotniczych od tego drugiego ETS w drodze transakcji przydziału międzynarodowego.

- Cofnięcie przydziału międzynarodowego:

transakcja ta będzie miała miejsce w przypadku, w którym przydział bezpłatnych uprawnień do rachunku posiadania operatora statku powietrznego w ramach drugiego ETS będzie musiał zostać cofnięty w całości.

- Zwrot nadmiernego przydziału:

podobny do cofnięcia, ale w przypadku gdy przydział nie musi być w pełni cofnięty i konieczne jest zwrócenie do przydzielającego ETS jedynie uprawnień przydzielonych w nadmiarze.

3.3.2. Protokół uzgadniania

Uzgodnienia będą mieć miejsce dopiero po zamknięciu okien przyjmowania, zatwierdzania i przetwarzania wiadomości.

Uzgodnienia stanowią integralną część środków służących zachowaniu bezpieczeństwa i spójności powiązania. Obie strony ustalą dokładne terminy uzgodnień przed sporządzeniem harmonogramu.

Zaplanowane codzienne uzgodnienia mogą się odbywać, jeżeli obie strony wyrażą na nie zgodę. Będą wykonywane co najmniej uzgodnienia zaplanowane, jednak po przeprowadzeniu przyjęcia.

Mimo to każda ze stron może rozpocząć ręczne uzgodnienia w dowolnym momencie.

Zmiany terminów i częstotliwości zaplanowanych uzgodnień będą obsługiwane z zachowaniem procedur operacyjnych określonych w sekcji wspólnych procedur operacyjnych poświęconej procesowi realizacji wniosków.

3.3.3. Komunikat testowy

Wiadomość testowa ma służyć testowaniu łączności typu koniec-koniec. Wiadomość będzie zawierać dane, które wskażą, że jest to wiadomość testowa, i po otrzymaniu jej przez drugi koniec zostanie przesłana na nią odpowiedź.

3.4. Wymogi rejestracji danych

Aby wesprzeć konieczność zachowywania przez obie strony odpowiednich i spójnych informacji oraz zapewnić narzędzia do wykorzystania w procesie uzgadniania służące do usunięcia niespójności, obie strony będą prowadzić cztery (4) rodzaje dzienników danych:

- dzienniki transakcji,
- dzienniki uzgadniania,
- archiwum wiadomości,
- ścieżki audytu wewnętrznego.

Wszelkie dane w tych dziennikach muszą być przechowywane przez okres co najmniej trzech (3) miesięcy do celów rozwiązywania problemów, a ich dalsze zachowanie będzie zależeć od obowiązującego prawa na każdym końcu na potrzeby przeprowadzenia audytu. Pliki dziennika starsze niż trzy (3) miesiące można zarchiwizować w bezpiecznej lokalizacji w niezależnym systemie informatycznym, o ile ich wyszukanie lub uzyskanie do nich dostępu będzie możliwe w rozsądnym czasie.

Dzienniki transakcji

Zarówno podsystem EUTL, jak i podsystem SSTL, stanowią wdrożenie dzienników transakcji. Są one wzajemnie weryfikowane między obydwoma systemami ETS.

Dokładniej rzecz ujmując, w dziennikach transakcji będzie rejestrowana każda propozycja transakcji wysyłana do drugiego ETS. Każdy zapis zawiera wszystkie pola treści transakcji oraz późniejszy wynik transakcji (odpowiedź ETS otrzymującego propozycję). W dziennikach transakcji będą rejestrowane również transakcje przychodzące, a także odpowiedzi wysyłane do ETS pochodzenia.

Dzienniki uzgadniania

Dziennik uzgadniania zawiera zapis każdego komunikatu dotyczącego uzgodnienia wymienionego między obydwiema stronami, w tym identyfikator uzgodnienia, znacznik czasowy i wynik uzgodnienia: status uzgodnienia „przyjęte” lub „rozbieżne”. W ramach stałego powiązania rejestrów komunikaty dotyczące uzgodnienia stanowią integralną część wymienianych wiadomości i w związku z tym są przechowywane zgodnie z opisem w sekcji „archiwum wiadomości”.

Obie strony rejestrują każdy wniosek i odpowiedź w dzienniku uzgadniania. Chociaż informacje zamieszczane w dzienniku uzgadniania nie są udostępniane bezpośrednio jako część samego uzgodnienia, dostęp do tych informacji może być konieczny, aby rozstrzygnąć niespójności.

Archiwum wiadomości

Wymaga się, aby obie strony archiwizowały kopie wymienianych danych (pliki XML), wysyłanych i otrzymywanych oraz fakt, czy dane te lub wiadomości XML miały odpowiedni format.

Archiwum ma służyć głównie do celów przeprowadzania audytu – posiadania dowodu tego, co zostało wysłane drugiej stronie i od niej otrzymane. W tym kontekście wraz z plikami należy archiwizować również powiązane z nimi certyfikaty.

Pliki te dostarczą także dodatkowych informacji na potrzeby rozwiązywania problemów.

Ścieżki audytu wewnętrznego

Dzienniki te są określane i stosowane przez strony we własnym zakresie.

3.5. Wymogi operacyjne

Wymiana danych między obydwoma systemami w ramach stałego powiązania rejestrów nie jest w pełni niezależna, co oznacza, że do uruchomienia powiązania wymaga operatorów i procedur. W tym celu wyszczególniono kilka ról i narzędzi.

4. PRZEPISY DOTYCZĄCE DOSTĘPNOŚCI

4.1. Opracowywanie dostępności komunikacji

Architekturę stałego powiązania rejestrów stanowią zasadniczo infrastruktura z zakresu technologii informacyjno-komunikacyjnych i oprogramowanie, które umożliwiają komunikację między ETS Szwajcarii i EU ETS. Zapewnienie wysokiego poziomu dostępności, integralności i poufności tego przepływu danych staje się zatem podstawowym aspektem, który należy uwzględnić przy opracowywaniu stałego powiązania rejestrów. W przypadku projektu, w którym infrastruktura z zakresu technologii informacyjno-komunikacyjnych, niestandardowe oprogramowanie oraz procesy odgrywają integralną rolę, należy wziąć pod uwagę wszystkie trzy elementy, aby opracować odporny system.

Odporność infrastruktury z zakresu technologii informacyjno-komunikacyjnych

Podstawowe elementy architektoniczne szczegółowo opisano w rozdziale niniejszego dokumentu dotyczącym przepisów ogólnych. Po stronie infrastruktury z zakresu technologii informacyjno-komunikacyjnych stałe powiązanie rejestrów ustanawia odporną sieć VPN tworzącą zabezpieczone korytarze komunikacji, za pośrednictwem których odbywa się bezpieczna wymiana wiadomości. Inne elementy infrastruktury są konfigurowane w wysokiej dostępności lub opierają się na mechanizmach rezerwowych.

Odporność niestandardowego oprogramowania

Niestandardowe moduły oprogramowania zwiększają odporność poprzez ponawianie próby nawiązania komunikacji z drugim końcem przez określony czas, jeżeli z jakiegoś powodu jest on niedostępny.

Odporność usługi

W ramach stałego powiązania rejestrów wymiana danych między stronami odbywa się we wcześniej określonych odstępach czasu. Niektóre z etapów niezbędnych podczas uprzednio zaplanowanej wymiany danych wymagają ręcznej interwencji operatorów systemu lub administratorów rejestru. Biorąc ten aspekt pod uwagę oraz w celu zwiększenia dostępności i powodzenia wymiany:

- w procedurach operacyjnych przewidziano okna czasowe na przeprowadzenie każdego etapu,
- moduły oprogramowania stałego powiązania rejestrów realizują asynchroniczną komunikację,
- automatyczny proces uzgadniania wykryje, jeżeli na którymś końcu wystąpiły problemy z przyjęciem plików z danymi,
- procesy monitorowania (infrastruktura z zakresu technologii informacyjno-komunikacyjnych i moduły niestandardowego oprogramowania) są rozpatrywane w ramach procedur zarządzania incydentami i uruchamiają te procedury (jak określono w dokumencie na temat wspólnych procedur operacyjnych). Procedury służące ograniczeniu czasu potrzebnego na przywrócenie normalnego funkcjonowania po wystąpieniu incydentów są niezbędne, aby zapewnić wysokie współczynniki dostępności.

4.2. Plan dotyczący inicjowania, komunikacji, ponownej aktywacji oraz testów

Wszystkie poszczególne elementy związane z architekturą stałego powiązania rejestrów muszą przejść serię indywidualnych i wspólnych testów, aby potwierdzić, że platforma na poziomie infrastruktury z zakresu technologii informacyjno-komunikacyjnych oraz systemu informacyjnego jest gotowa. Przeprowadzenie tych testów operacyjnych jest obowiązkowym warunkiem wstępnym

za każdym razem, gdy platforma zmienia status stałego powiązania rejestrów z zawieszonego na funkcjonujący.

Aktywacja statusu powiązania, który oznacza funkcjonowanie, wymaga zatem wykonania uprzednio określonego planu testów z powodzeniem. Musi to potwierdzić, że przed rozpoczęciem składania wniosków o transakcje dotyczące produkcji między obydwiema stronami, każdy rejestr przeprowadził najpierw szereg wewnętrznych testów, a następnie zatwierdził łączność koniec-koniec.

W planie testów należy wskazać ogólną strategię testów oraz podać szczegółowe informacje na temat infrastruktury testowania. W szczególności w odniesieniu do każdego elementu we wszystkich blokach testów plan ten musi obejmować:

- kryteria i narzędzia testu,
- role przypisane do przeprowadzenia testu,
- oczekiwane wyniki (pozytywne i negatywne),
- program testu,
- rejestrację wymogów w zakresie wyników testu,
- dokumentację rozwiązywania problemów,
- postanowienia dotyczące eskalacji.

Jako proces, testy dotyczące aktywacji statusu oznaczającego funkcjonowanie można podzielić na cztery (4) konceptualne bloki lub etapy.

4.2.1. Testy wewnętrznej infrastruktury z zakresu technologii informacyjno-komunikacyjnych

Testy te mają być przeprowadzone lub poddane kontroli indywidualnie przez administratorów rejestru na każdym końcu.

Wszystkie elementy infrastruktury z zakresu technologii informacyjno-komunikacyjnych na każdym końcu muszą być przetestowane indywidualnie. Obejmuje to każdy pojedynczy komponent infrastruktury. Testy te można wykonać automatycznie lub ręcznie, ale muszą one zweryfikować, czy każdy element infrastruktury funkcjonuje.

4.2.2. Testy komunikacji

Testy te rozpoczynają się indywidualnie u każdej strony i kończą we współpracy z drugim końcem.

Gdy poszczególne elementy funkcjonują, należy przetestować kanały komunikacji między obydwoma rejestrami. W tym celu każda strona weryfikuje, czy dostęp do internetu działa, czy ustanowiono kanały VPN oraz czy istnieje międzylokacyjne połączenie IP. Następnie należy potwierdzić drugiemu końcowi, że elementy infrastruktury lokalnej i zdalnej oraz połączenie IP są możliwe do osiągnięcia.

4.2.3. Testy całego systemu (koniec-koniec)

Testy te wykonuje się na każdym końcu, a wyniki muszą być udostępnione drugiej stronie.

Po przetestowaniu kanałów komunikacji i wszystkich poszczególnych komponentów obu rejestrów każdy koniec przygotowuje serię symulowanych transakcji i uzgodnień reprezentatywnych dla wszystkich funkcji, które mają zostać wdrożone w ramach powiązania.

4.2.4. Testy bezpieczeństwa

Testy te mają być przeprowadzone lub zainicjowane przez administratorów rejestru na każdym końcu, jak wyszczególniono w sekcji „Wytyczne testowania bezpieczeństwa" oraz „Przepisy dotyczące oceny ryzyka".

Stałe powiązanie rejestrów można uznać za posiadające status oznaczający funkcjonowanie, dopiero gdy wszystkie cztery etapy/bloki zakończą się przewidywalnymi wynikami.

Zasoby testowania

Każda strona polega na określonych zasobach testowania (konkretnej infrastrukturze oprogramowania i sprzętu z zakresu technologii informacyjno-komunikacyjnych) i opracowuje funkcje testowania w swoich odnośnych systemach w celu wsparcia ręcznego i nieustannego sprawdzania platformy. Administratorzy rejestru mogą przeprowadzić ręczne indywidualne lub wspólne procedury testowania w dowolnym momencie. Aktywacja statusu oznaczającego funkcjonowanie sama w sobie jest procesem ręcznym.

Podobnie przewidziano, że platforma dokonuje automatycznych kontroli w regularnych odstępach czasu. Kontrole te służą zwiększeniu dostępności platformy poprzez wczesne wykrywanie potencjalnych problemów z infrastrukturą lub oprogramowaniem. Ten program monitorowania platformy składa się z dwóch elementów:

- monitorowania infrastruktur z zakresu technologii informacyjno-komunikacyjnych: infrastruktura na obu końcach będzie monitorowana przez dostawców usług infrastrukturalnych z zakresu technologii informacyjno-komunikacyjnych. Automatyczne testy będą obejmować poszczególne elementy infrastruktury oraz dostępność kanałów komunikacji,
- monitorowanie aplikacji: moduły oprogramowania stałego powiązania rejestrów będą realizować monitorowanie komunikacji systemowej na poziomie aplikacji (albo ręcznie, albo w regularnych odstępach czasu), które przetestuje dostępność powiązania między końcami poprzez symulację niektórych transakcji za pośrednictwem powiązania.

4.3. Środowisko akceptacyjne/testowe

Architektura rejestru Unii i rejestru Szwajcarii składa się z następujących trzech środowisk:

- produkcyjnego: środowisko to przechowuje rzeczywiste dane i przetwarza rzeczywiste transakcje,
- akceptacyjnego: środowisko to zawiera nierzeczywiste lub zamaskowane, reprezentatywne dane. Jest to środowisko, w którym operatorzy systemów obu stron zatwierdzają nowe wersje,
- testowego: środowisko to zawiera nierzeczywiste lub zamaskowane, reprezentatywne dane. Środowisko to ogranicza się do administratorów rejestru i służy do przeprowadzania testów integracyjnych przez obie strony.

Z wyjątkiem VPN te trzy środowiska są w pełni niezależne od siebie, co oznacza, że sprzęt, oprogramowanie, bazy danych, środowiska wirtualne, adresy IP, porty są ustanawiane i funkcjonują niezależnie od siebie.

Jeżeli chodzi o strukturę VPN, komunikacja między trzema środowiskami musi być w pełni niezależna, co zapewnia się za pomocą STESTA.

5. PRZEPISY DOTYCZĄCE POUFNOŚCI I INTEGRALNOŚCI

W ramach mechanizmów i procedur bezpieczeństwa przewidziano dwuosobową rolę (zasadę czworga oczu) odnoszącą się do operacji odbywających się za pośrednictwem powiązania między rejestrem Unii i rejestrem Szwajcarii. Dwuosobowa rola ma zastosowanie zawsze, gdy zajdzie taka potrzeba, może jednak nie mieć zastosowania do wszystkich kroków podejmowanych przez administratorów rejestru.

Wymogi bezpieczeństwa rozważa się i uwzględnia w planie zarządzania bezpieczeństwem, który obejmuje również procesy związane z obsługą incydentów dotyczących bezpieczeństwa w następstwie ewentualnego naruszenia bezpieczeństwa. Operacyjną część tych procesów opisano we wspólnych procedurach operacyjnych.

5.1. Infrastruktura testowania bezpieczeństwa

Każda strona angażuje się w ustanowienie infrastruktury testowania bezpieczeństwa (korzystając ze wspólnego zestawu sprzętu i oprogramowania wykorzystywanego do wykrywania luk na etapie opracowywania i funkcjonowania):

- oddzielonej od środowiska produkcyjnego,
- w ramach której bezpieczeństwo jest analizowane przez zespół niezależny od opracowywania i funkcjonowania systemu.

Każda strona zobowiązuje się do przeprowadzenia zarówno analizy statycznej, jak i dynamicznej.

W przypadku analizy dynamicznej (takiej jak testy penetracyjne) obie strony zobowiązują się do ograniczenia ocen zazwyczaj do środowiska testowego i akceptacyjnego (jak określono w sekcji „Środowisko akceptacyjne/testowe”). Odstępstwa od tej polityki podlegają wyrażeniu zezwolenia przez obie strony.

Przed wdrożeniem w środowisku produkcyjnym każdy moduł oprogramowania łącza (jak określono w sekcji „Architektura łącza komunikacyjnego”) testuje się pod względem bezpieczeństwa.

Infrastruktura testowa musi być oddzielona od infrastruktury produkcyjnej zarówno na poziomie sieci, jak i na poziomie infrastrukturalnym, oraz umożliwiać przeprowadzenie testów wymaganych do sprawdzenia zgodności z wymogami bezpieczeństwa.

5.2. Przepisy dotyczące zawieszenia i ponownej aktywacji powiązania

Jeżeli istnieje podejrzenie, że bezpieczeństwo rejestru Szwajcarii, SSTL, rejestru Unii lub EUTL zostało naruszone, obie strony natychmiast przekazują sobie te informacje oraz zawieszają powiązanie między SSTL i EUTL.

Procedury dotyczące udostępnienia informacji, decyzji o zawieszeniu i decyzji o ponownej aktywacji są częścią procesu realizacji wniosku w ramach wspólnych procedur operacyjnych.

Zawieszenia

Zawieszenie powiązania rejestrów zgodnie z załącznikiem II do umowy może mieć miejsce ze względu na:

- powody administracyjne (konserwacja itp.), a zatem będzie to zawieszenie planowane,

- powody związane z bezpieczeństwem (lub awarię infrastruktury informatycznej), a zatem będzie to zawieszenie nieplanowane.

W sytuacji awaryjnej każda ze stron poinformuje drugą i jednostronnie zawiesi powiązanie rejestrów.

W przypadku podjęcia decyzji o zawieszeniu powiązania rejestrów, każda strona w związku z tym zapewni, aby powiązanie zostało przerwane na poziomie sieci (poprzez zablokowanie części lub wszystkich połączeń przychodzących i wychodzących).

Decyzja o zawieszeniu powiązania rejestrów, planowanym lub nieplanowanym, zostanie podjęta zgodnie z procedurą zarządzania zmianą lub procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji określoną we wspólnych procedurach operacyjnych.

Ponowna aktywacja komunikacji

Decyzja o ponownej aktywacji zostanie podjęta w sposób określony we wspólnych procedurach operacyjnych i w żadnym wypadku nie nastąpi przed zakończeniem z powodzeniem procedur testowania bezpieczeństwa wyszczególnionych w sekcji „Wytyczne testowania bezpieczeństwa" oraz „Plan dotyczący inicjowania, komunikacji, ponownej aktywacji oraz testów".

5.3. Przepisy dotyczące naruszenia bezpieczeństwa

Naruszenie bezpieczeństwa uznaje się za incydent związany z bezpieczeństwem mający wpływ na poufność i integralność informacji szczególnie chronionych lub dostępność przetwarzającego je systemu.

Informacje szczególnie chronione określono w wykazie informacji szczególnie chronionych i można je przetwarzać w systemie lub dowolnej powiązanej części.

Informacje bezpośrednio związane z naruszeniem bezpieczeństwa zostaną uznane za szczególnie chronione, oznaczone jako „SPECIAL HANDLING: *ETS Critical*" i przetworzone zgodnie z instrukcjami przetwarzania, o ile nie ustanowiono inaczej.

Każde naruszenie bezpieczeństwa będzie rozwiązywane zgodnie z rozdziałem wspólnych procedur operacyjnych dotyczącym zarządzania incydentami związanymi z bezpieczeństwem informacji.

5.4. Wytyczne dotyczące testowania bezpieczeństwa

5.4.1. Oprogramowanie

Testowanie bezpieczeństwa, w tym w stosownych przypadkach testy penetracyjne, przeprowadza się przynajmniej na wszystkich głównych nowo wydanych wersjach oprogramowania zgodnie z wymogami bezpieczeństwa określonymi w normach technicznych powiązania, aby ocenić bezpieczeństwo powiązania i związane z nim ryzyko.

Jeżeli w ciągu ostatnich 12 miesięcy nie wydano głównej wersji, testowanie bezpieczeństwa przeprowadza się na obecnym systemie, biorąc pod uwagę rozwój zagrożeń dla cyberbezpieczeństwa, który nastąpił na przestrzeni ostatnich 12 miesięcy.

Testowania bezpieczeństwa powiązania rejestrów dokonuje się w środowisku akceptacyjnym i – jeżeli jest to wymagane – w środowisku produkcyjnym oraz przy koordynacji i wzajemnym porozumieniu obu stron.

Testowanie aplikacji sieciowej odbędzie się z zachowaniem międzynarodowych standardów otwartych, takich jak standardy opracowane przez Projekt Bezpieczeństwa Aplikacji Sieci Otwartej (OWASP).

5.4.2. Infrastruktura

Infrastruktura wspierająca system produkcji musi być regularnie poddawana przeglądowi pod kątem luk (co najmniej raz w miesiącu) oraz wykrytych usuniętych luk na zasadzie, którą określono w poprzedniej sekcji, z wykorzystaniem aktualnej bazy danych dotyczących luk.

5.5. Przepisy dotyczące oceny ryzyka

Jeżeli stosowane są testy penetracyjne, muszą one zostać uwzględnione w testowaniu bezpieczeństwa.

Każda strona może udzielić zamówienia na przeprowadzenia testowania bezpieczeństwa specjalizującemu się w tym przedsiębiorstwu, o ile przedsiębiorstwo to:

- ma kwalifikacje i doświadczenie w zakresie takiego testowania bezpieczeństwa,
- nie odpowiada bezpośrednio przed twórcą ani jego wykonawcą i nie jest zaangażowane w opracowywanie oprogramowania powiązania ani nie jest podwykonawcą twórcy,
- podpisało umowę poufności celem zachowania poufności wyników i przetwarzania ich na poziomie „SPECIAL HANDLING: ETS Critical” zgodnie z instrukcjami przetwarzania.