EURÓPSKA
KOMISIA

V Bruseli 20. 3. 2024
COM(2024) 125 final

ANNEX

PRÍLOHA

k

návrhu rozhodnutia Rady

o pozícii, ktorá sa má v mene Európskej únie zaujať v spoločnom výbore zriadenom Dohodou medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov v súvislosti so zmenami prílohy II k dohode, spoločných operačných postupov a prepájacích technických noriem

ROZHODNUTIE č. 1/2024 SPOLOČNÉHO VÝBORU ZRIADENÉHO DOHODOU MEDZI EURÓPSKOU ÚNIOU A ŠVAJČIARSKOU KONFEDERÁCIOU O PREPOJENÍ ICH SYSTÉMOV OBCHODOVANIA S EMISIAMI SKLENÍKOVÝCH PLYNOV

z...

pokiaľ ide o zmenu prílohy II k dohode, spoločných operačných postupov a prepájacích technických noriem

SPOLOČNÝ VÝBOR,

so zreteľom na Dohodu medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov[1] (ďalej len „dohoda“), a najmä na jej článok 9 a článok 13 ods. 2,

keďže:

(1) Rozhodnutím spoločného výboru č. 2/2019[2] sa stanovilo predbežné riešenie na sfunkčnenie prepojenia medzi systémom EU ETS a ETS Švajčiarska.

(2) Spoločný výbor sa na svojom treťom zasadnutí zhodol na potrebe analyzovať nákladovú efektívnosť trvalého prepojenia medzi registrom Únie a registrom Švajčiarska.

(3) Spoločný výbor sa na svojom piatom zasadnutí schválil správu, ktorú predložila pracovná skupina zriadená rozhodnutiami spoločného výboru č. 1/2020[3] a 2/2020[4] a v ktorej táto pracovná skupina analyzovala a odporučila prístup na zavedenie trvalého prepojenia medzi registrom Únie a registrom Švajčiarska.

(4) S cieľom zohľadniť technické požiadavky trvalého prepojenia medzi registrom Únie a registrom Švajčiarska, ako aj zjednodušiť ustanovenia prílohy II k dohode vzhľadom na technologický vývoj, by sa príloha II k dohode mala zmeniť.

(5) S cieľom zabezpečiť súlad spoločných operačných postupov a prepájacích technických noriem s prílohou II k dohode by sa tieto dokumenty mali takisto zmeniť.

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Príloha II k dohode sa nahrádza prílohou I k tomuto rozhodnutiu.

2. Spoločné operačné postupy uvedené v článku 3 ods. 6 dohody sú stanovené v prílohe II k tomuto rozhodnutiu.

3. Prepájacie technické normy uvedené v článku 3 ods. 7 dohody sú stanovené v prílohe III k tomuto rozhodnutiu.

Článok 2

Toto rozhodnutie nadobúda účinnosť dňom jeho prijatia.

Vyhotovené v anglickom jazyku v [Bruseli][Berne] dňa [xx 2024].

---

1 Ú. v. EÚ L 322, 7.12.2017, s. 3.
2 Ú. v. EÚ L 314, 29.9.2020, s. 68.
3 Ú. v. EÚ L 226, 25.6.2021, s. 2.
4 Ú. v. EÚ L 226, 25.6.2021, s. 16.

Za spoločný výbor

tajomníčka za Európsku úniu	*predsedníčka*	*tajomníčka za Švajčiarsko*

PRÍLOHA I

„PRÍLOHA II

PREPÁJACIE TECHNICKÉ NORMY

S cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska sa v roku 2020 zaviedlo predbežné riešenie. Od roku 2023 sa prepojenie registrov medzi týmito dvoma systémami obchodovania s emisiami postupne rozvíja do trvalého prepojenia registrov, ktorého zavedenie sa očakáva najneskôr v roku 2024 a ktoré umožní fungovanie prepojených trhov, pokiaľ ide o výhody vyplývajúce z likvidity trhu a vykonávanie transakcií medzi týmito dvoma prepojenými systémami spôsobom, ktorý je rovnocenný s jedným trhom zloženým z dvoch systémov a ktorý umožňuje účastníkom trhu konať tak, ako keby boli na jednom trhu, pričom podlieha len jednotlivým regulačným ustanoveniam zmluvných strán. V prepájacích technických normách sa uvádza:

– štruktúra komunikačného prepojenia,

– komunikácia medzi SSTL a EUTL,

– bezpečnosť prenosu údajov,

– zoznam funkcií (transakcie, zosúhlasenie atď.),

– vymedzenie transportnej vrstvy,

– požiadavky na logovanie údajov,

– prevádzkové opatrenia (telefonické centrum, podpora),

– komunikačný plán a skúšobný postup,

– postup testovania zabezpečenia.

V prepájacích technických normách sa uvedie, že správcovia majú podniknúť všetky primerané kroky, aby SSTL, EUTL a prepojenie boli v prevádzke 24 hodín denne a 7 dní v týždni a aby prerušenia prevádzky SSTL, EUTL a prepojenia boli obmedzené na minimum.

V prepájacích technických normách sa stanovia dodatočné požiadavky na zabezpečenie švajčiarskeho registra, SSTL, registra Únie a EUTL, ktoré sa zdokumentujú v tzv. bezpečnostnom riadiacom pláne. V prepájacích technických normách sa konkrétne špecifikujú tieto skutočnosti:

– ak existuje podozrenie, že bolo narušené zabezpečenie švajčiarskeho registra, SSTL, registra Únie alebo EUTL, obidve zmluvné strany sa okamžite navzájom informujú a prerušia prepojenie medzi SSTL a EUTL,

– ak dôjde k narušeniu zabezpečenia, zmluvné strany sa zaväzujú, že sa o tejto skutočnosti budú okamžite navzájom informovať. V rozsahu, v akom sú dostupné technické podrobnosti, si správca švajčiarskeho registra a ústredný správca registra Únie do 24 hodín od narušenia bezpečnosti navzájom zašlú hlásenie o tomto incidente (dátum, príčina, dôsledky, nápravné opatrenia).

Skôr, ako sa vytvorí komunikačné prepojenie medzi SSTL a EUTL, a vždy, keď je potrebná nová verzia alebo aktualizácia SSTL alebo EUTL, sa zabezpečenie otestuje postupom stanoveným v prepájacích technických normách.

V prepájacích technických normách sa zavedú dve testovacie prostredia popri produkčnom prostredí:

Zmluvné strany poskytnú prostredníctvom správcu švajčiarskeho registra a ústredného správcu registra Únie dôkazy o tom, že v predchádzajúcich 12 mesiacoch bolo vykonané nezávislé hodnotenie zabezpečenia ich systémov v súlade s bezpečnostnými požiadavkami stanovenými v prepájacích technických normách. Pri každej novej zásadnej verzii softvéru (major release) sa vykoná testovanie zabezpečenia a najmä penetračné testy, a to v súlade s bezpečnostnými požiadavkami stanovenými v prepájacích technických normách. Penetračné testy nesmie vykonávať vývojár softvéru ani subdodávateľ vývojára softvéru.“

PRÍLOHA II

SPOLOČNÉ OPERAČNÉ POSTUPY (SOP)

podľa článku 3 ods. 6 dohody medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov

Postupy trvalého prepojenia registrov

Obsah

1. Glosár 9
2. Úvod 10
2.1. Rozsah pôsobnosti 10
2.2. Adresáti 11
3. Prístup a normy 11
4. Riadenie incidentov 12
4.1. Zisťovanie a zaznamenávanie incidentov 12
4.2. Klasifikácia a počiatočná podpora 12
4.3. Vyšetrovanie a diagnostika 13
4.4. Riešenie krízových situácií a obnova služby 13
4.5. Uzavretie incidentu 13
5. Riadenie problémov 15
5.1. Identifikácia a záznam problému 15
5.2. Priorizácia problému 15
5.3. Vyšetrovanie a diagnostika problému 15
5.4. Vyriešenie 15
5.5. Uzavretie problému 15
6. Vybavovanie žiadosti 15
6.1. Iniciovanie žiadosti 16
6.2. Registrovanie a analýza žiadostí 16
6.3. Schválenie žiadosti 16
6.4. Vybavovanie žiadosti 16
6.5. Postúpenie žiadosti 16
6.6. Kontrola vybavovania žiadostí 16
6.7. Uzavretie žiadosti 17
7. Riadenie zmien 18
7.1. Žiadosť o zmenu 18

7.2. Hodnotenie a plánovanie zmien....18
7.3. Schválenia zmien....18
7.4. Vykonanie zmeny....18
8. Riadenie vydaní....18
8.1. Plánovanie vydania....19
8.2. Vytvorenie a otestovanie balíka vydaní....19
8.3. Príprava na zavedenie....19
8.4. Návrat do pôvodného stavu....20
8.5. Preskúmanie a uzavretie vydania....20
9. Riadenie bezpečnostných incidentov....20
9.1. Kategorizácia incidentov v oblasti bezpečnosti informácií....21
9.2. Riešenie incidentov v oblasti bezpečnosti informácií....21
9.3. Identifikácia bezpečnostných incidentov....21
9.4. Analýza bezpečnostných incidentov....21
9.5. Posudzovanie závažnosti bezpečnostných incidentov, postúpenie a podávanie správ21
9.6. Podávanie správ o reakcii na bezpečnostný incident....21
9.7. Monitorovanie, budovanie kapacít a kontinuálne zlepšovanie....22
10. Riadenie bezpečnosti informácií....22
10.1. Identifikácia citlivých informácií....22
10.2. Úrovne citlivosti informačných aktív....22
10.3. Priradenie vlastníka informačných aktív....23
10.4. Registrácia citlivých informácií....23
10.5. Zaobchádzanie s citlivými informáciami....23
10.6. Riadenie prístupu....23
10.7. Správa certifikátov/kľúčov....24

1. GLOSÁR

Tabuľka 1 – Skratky a definície

Skratka/Termín	Definícia
Certifikačný orgán (CA)	Subjekt, ktorý vydáva digitálne certifikáty
CH	Švajčiarska konfederácia
ETS	Systém obchodovania s emisiami
EÚ	Európska únia
IMT	Tím pre riadenie incidentov
Informačné aktívum	Informácia, ktorá je cenná pre spoločnosť alebo organizáciu
IT	Informačné technológie
ITIL	Knižnica pre infraštruktúru informačných technológií
ITSM	Riadenie služieb v oblasti informačných technológií
LTS	Prepájacie technické normy
Register	Systém účtovania kvót vydaných v rámci ETS, ktorý sleduje vlastníctvo kvót vedených na elektronických účtoch.
RFC	Žiadosť o zmenu
SIL	Zoznam citlivých informácií
SR	Žiadosť o službu
Wiki	Webové sídlo, na ktorom si používatelia môžu vymieňať informácie a poznatky pridaním alebo prispôsobením obsahu priamo prostredníctvom webového prehliadača.

2. ÚVOD

V dohode medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov z 23. novembra 2017 (ďalej len „dohoda“) sa stanovuje vzájomné uznávanie emisných kvót, ktoré možno použiť na dosiahnutie súladu v rámci systému obchodovania s emisiami Európskej únie (ďalej len „EU ETS“) alebo systému obchodovania s emisiami Švajčiarska (ďalej len „ETS Švajčiarska“). S cieľom realizovať prepojenie medzi EU ETS a ETS Švajčiarska sa zriadi priame prepojenie medzi protokolom transakcií Európskej únie (European Union Transaction Log – EUTL) registra Únie a dodatkovým protokolom transakcií Švajčiarska (Swiss Supplementary Transaction Log – SSTL) švajčiarskeho registra, čím sa umožní prenos emisných kvót vydaných v rámci ktoréhokoľvek z týchto dvoch ETS medzi registrami (článok 3 ods. 2 dohody). S cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska sa v roku 2020 zaviedlo predbežné riešenie. Od roku 2023 sa prepojenie registrov medzi týmito dvoma systémami obchodovania s emisiami postupne rozvíja do trvalého prepojenia registrov, ktorého zavedenie sa očakáva najneskôr v roku 2024 a ktoré umožní fungovanie prepojených trhov, pokiaľ ide o výhody vyplývajúce z likvidity trhu a vykonávanie transakcií medzi týmito dvoma prepojenými systémami spôsobom, ktorý je rovnocenný s jedným trhom zloženým z dvoch systémov a ktorý umožňuje účastníkom trhu konať tak, ako keby boli na jednom trhu, pričom podlieha len jednotlivým regulačným ustanoveniam zmluvných strán. (Príloha II k dohode)

Podľa článku 3 ods. 6 dohody švajčiarsky správca registra a ústredný správca registra Únie sú povinní stanoviť spoločné operačné postupy týkajúce sa technických alebo iných záležitostí, ktoré sú potrebné na fungovanie prepojenia, pričom sú povinní vziať do úvahy priority domácich právnych predpisov. Spoločné operačné postupy vypracované správcami nadobudnú účinnosť po prijatí rozhodnutia spoločného výboru.

Spoločné operačné postupy prijal spoločný výbor rozhodnutím č. 1/2020. Aktualizované spoločné operačné postupy prijme spoločný výbor rozhodnutím č. 1/2024. V súlade s týmto rozhodnutím a žiadosťami spoločného výboru švajčiarsky správca registra a ústredný správca registra Únie vypracovali a aktualizujú ďalšie technické usmernenia s cieľom sfunkčniť prepojenie a zabezpečiť, aby sa tieto usmernenia neustále prispôsobovali technickému pokroku a novým požiadavkám týkajúcim sa bezpečnosti a zabezpečenia prepojenia, ako aj jeho účinného a efektívneho fungovania.

2.1. Rozsah pôsobnosti

Tento dokument predstavuje všeobecnú zhodu zmluvných strán dohody týkajúcu sa vytvorenia procesných základov prepojenia medzi registrami EU ETS a ETS Švajčiarska. I keď sa v ňom uvádzajú celkové procedurálne požiadavky z hľadiska fungovania, na sfunkčnenie prepojenia budú potrebné ďalšie technické usmernenia.

Pokiaľ ide o riadne fungovanie, prepojenie si bude vyžadovať technické špecifikácie slúžiace na zabezpečenie jeho ďalšieho sfunkčnenia. Podľa článku 3 ods. 7 dohody sa tieto záležitosti podrobne uvádzajú v dokumente týkajúcom sa prepájacích technických noriem, ktorý sa má prijať samostatne, a to rozhodnutím spoločného výboru.

Cieľom spoločných operačných postupov je zabezpečiť, aby boli IT služby súvisiace s fungovaním prepojenia medzi registrami EU ETS a ETS Švajčiarska vykonávané efektívne a účinne, najmä pokiaľ ide o vybavovanie žiadostí o službu, riešenie zlyhania služby, odstraňovanie problémov, ako aj vykonávanie bežných prevádzkových úloh podľa medzinárodných noriem pre riadenie IT služieb.

V prípade trvalého prepojenia registra budú potrebné iba tieto spoločné operačné postupy, ktoré sú súčasťou tohto dokumentu:

- Riadenie incidentov
- Riadenie problémov
- Vybavovanie žiadosti
- Riadenie zmien
- Riadenie vydaní
- Riadenie bezpečnostných incidentov
- Riadenie bezpečnosti informácií.

2.2. Adresáti

Cieľovou skupinou týchto spoločných operačných postupov sú podporné tímy registrov EÚ a Švajčiarska.

3. PRÍSTUP A NORMY

Na všetky spoločné operačné postupy sa vzťahuje táto zásada:

- EÚ a Švajčiarsko sa dohodli na vymedzení spoločných operačných postupov na základe ITIL (knižnica pre infraštruktúru informačných technológií, verzia 4). Uplatňujú sa postupy uvedené v tejto norme, ktoré sú prispôsobené osobitným potrebám súvisiacim s trvalým prepojením registra.
- Komunikácia a koordinácia potrebná na spracovanie spoločných operačných postupov medzi obidvoma zmluvnými stranami sa uskutočňuje prostredníctvom centier podpory registrov Švajčiarska a EÚ. Úlohy sa vždy prideľujú v rámci jednej zmluvnej strany.
- Ak nedôjde k dohode o spôsobe pristupovania k spoločným operačným postupom, obidve centrá zanalyzujú a medzi sebou vyriešia túto otázku. Ak dohodu nie je možné dosiahnuť, nájdenie spoločného riešenia sa postúpi o úroveň vyššie.

Úrovne postúpenia	**EÚ**	**CH**
1. úroveň	Centrum podpory EÚ	Centrum podpory Švajčiarska
2. úroveň	Manažér operačných postupov EÚ	Švajčiarsky manažér pre aplikáciu registra
3. úroveň	Spoločný výbor (ktorý by mohol delegovať túto zodpovednosť podľa článku 12 ods. 5 dohody o prepojení)	
4. úroveň	Spoločný výbor, ak je delegovaná 3. úroveň	

- Každá zmluvná strana môže určiť postupy fungovania svojho vlastného registračného systému, pričom zohľadní požiadavky a rozhrania týkajúce sa týchto spoločných operačných postupov.
- Nástroj riadenia IT služieb (ITSM) sa používa na podporu spoločných operačných postupov, najmä riadenie incidentov, riešenie problémov a vybavovanie žiadostí a komunikáciu medzi obidvoma zmluvnými stranami.

- Okrem toho je povolená výmena informácií e-mailom.
- Obidve zmluvné strany zabezpečia, aby boli požiadavky na bezpečnosť informácií splnené v súlade s pokynmi pre zaobchádzanie s informáciami.

4. RIADENIE INCIDENTOV

Cieľom procesu riadenia incidentov je čo najrýchlejšie po incidente a s minimálnym narušením prevádzky vrátiť IT služby na prevádzkovú úroveň.

Pri riadení incidentov by sa mali viesť aj záznamy o incidentoch na účely podávania správ a tento proces by mal byť integrovaný s inými procesmi s cieľom neustále ho zlepšovať.

Z globálneho hľadiska riadenie incidentov zahŕňa tieto činnosti:

- Zisťovanie a zaznamenávanie incidentov
- Klasifikácia a počiatočná podpora
- Vyšetrovanie a diagnostika
- Riešenie krízových situácií a obnova služby
- Uzavretie incidentu.

Počas celého trvania incidentu sa v rámci procesu riadenia incidentov neustále zabezpečuje zodpovednosť povolaných osôb, monitorovanie, sledovanie a komunikácia.

4.1. Zisťovanie a zaznamenávanie incidentov

Incident môže odhaliť podporná skupina, automatizované monitorovacie nástroje alebo technický personál vykonávajúci rutinný dohľad.

Po zistení sa incident musí zaznamenať a musí sa mu prideliť jednoznačný identifikátor umožňujúci jeho riadne sledovanie a monitorovanie. Jedinečný identifikátor incidentu je identifikátor, ktorý mu v spoločnom systéme tiketovania pridelí centrum podpory danej zmluvnej strany (EÚ alebo Švajčiarska), ktoré incident odhalilo, a musí sa používať v každej komunikácii týkajúcej sa tohto incidentu.

V prípade všetkých incidentov by kontaktným bodom malo byť to centrum podpory zmluvnej strany, ktoré daný tiket zaregistrovalo.

4.2. Klasifikácia a počiatočná podpora

Cieľom klasifikácie incidentov je zistiť a určiť, aký systém a/alebo služba sú zasiahnuté a do akej miery. Aby bola klasifikácia účinná, mala by nasmerovať incident k správnemu tímu na prvýkrát, aby sa urýchlilo jeho vyriešenie.

Klasifikačná fáza by mala kategorizovať incident a určiť jeho prioritu podľa jeho vplyvu a naliehavosti, aby mohol byť riešený podľa harmonogramu danej priority.

Ak má incident potenciálny vplyv na dôvernosť alebo integritu citlivých údajov a/alebo na dostupnosť systému, daný incident sa zároveň označí za bezpečnostný incident a následne sa rieši podľa postupu vymedzeného v kapitole „Správa incidentov v oblasti bezpečnosti“ tohto dokumentu.

Ak je to možné, centrum podpory, ktoré zaregistrovalo tento tiket, vykoná prvú diagnostiku. Centrum podpory pritom zistí, či v prípade daného incidentu ide o známu chybu. Ak áno, potom je postup riešenia alebo dočasné riešenie už známe a zdokumentované.

Ak centrum podpory tento incident úspešne vyrieši, potom ho v tomto okamihu uzavrie, keďže primárny účel riadenia incidentov (teda rýchle obnovenie služby pre koncového používateľa) bol splnený. Ak to tak nie je, centrum podpory tento incident postúpi príslušnej riešiteľskej skupine na ďalšie vyšetrovanie a diagnostiku.

4.3. Vyšetrovanie a diagnostika

Vyšetrovanie a diagnostika incidentov sa uplatňujú v prípade, že centrum podpory nemôže v rámci počiatočnej diagnostiky vyriešiť daný incident, a preto ho náležite postúpi ďalej. Postúpenie incidentov je plnohodnotnou súčasťou procesu vyšetrovania a diagnostiky.

Bežnou praxou vo fáze vyšetrovania a diagnostiky je pokus zopakovať incident za kontrolovaných podmienok. Pri vykonávaní vyšetrovania a diagnostiky incidentu je dôležité, aby sa zistilo správne poradie udalostí, ktoré k incidentu viedli.

Postúpenie je uznanie toho, že incident nemožno vyriešiť na úrovni daného centra podpory a musí sa postúpiť podpornej skupine na vyššej úrovni alebo druhej zmluvnej strane. Postúpenie môže prebiehať dvomi spôsobmi: horizontálne (funkčne) alebo vertikálne (hierarchicky).

Centrum podpory, ktoré incident zaznamenalo a začalo ho riešiť, je zodpovedné za postúpenie incidentu príslušnému tímu a za sledovanie celkového stavu a pridelenie incidentu.

Zmluvná strana, ktorej bol incident pridelený, je zodpovedná za zabezpečenie včasnej realizácie požadovaných opatrení a za poskytnutie spätnej väzby svojmu vlastnému centru podpory.

4.4. Riešenie krízových situácií a obnova služby

Keď sa incident úplne preskúma, dôjde k jeho riešeniu a obnove služby. Nájdenie riešenia incidentu znamená, že spôsob nápravy tohto problému bol identifikovaný. Realizácia riešenia je fázou obnovy služby.

Po tom, ako príslušné tímy vyriešia zlyhanie služby, incident je postúpený späť príslušnému centru podpory, ktoré incident zaregistrovalo, a u iniciátora incidentu sa potvrdí, že chyba bola odstránená a že incident možno uzavrieť. Zistenia zo spracovania incidentu sa zaznamenajú na budúce použitie.

Obnovu služby môže vykonať personál IT podpory alebo sa koncovému používateľovi poskytne súbor pokynov, podľa ktorých má postupovať.

4.5. Uzavretie incidentu

Uzavretie je posledným krokom v procese riadenia incidentov a uskutoční sa krátko po vyriešení incidentu.

V rámci kontrolného zoznamu činností, ktoré je potrebné počas fázy uzavretia incidentu vykonať, treba zdôrazniť:

- overenie počiatočnej kategorizácie, ktorá bola priradená k incidentu,
- správne zachytenie všetkých informácií týkajúcich sa incidentu,
- riadne zdokumentovanie incidentu a aktualizáciu vedomostnej základne,
- primeranú komunikáciu s každou zainteresovanou stranou, ktorej sa incident priamo alebo nepriamo dotýka.

Incident sa formálne uzavrie vtedy, keď centrum podpory ukončí fázu uzavretia incidentu a oznámi to druhej zmluvnej strane.

Keď je incident uzavretý, znovu sa neotvára. Ak v krátkom čase dôjde k opätovnému výskytu incidentu, pôvodný incident sa znovu neotvára, namiesto toho sa musí zaregistrovať nový incident.

Ak incident sledujú centrá podpory EÚ a Švajčiarska, konečné uzavretie je zodpovednosťou toho centra podpory, ktoré tiket zaregistrovalo.

5. RIADENIE PROBLÉMOV

Tento postup by sa mal dodržať vždy, keď sa zistí problém, čím sa spúšťa proces riadenia problémov. Riadenie problémov sa zameriava na zvýšenie kvality a zníženie objemu výskytu incidentov. Problém môže byť príčinou jedného alebo viacerých incidentov. Ak sa podá správa o incidente, cieľom riadenia incidentov je obnoviť danú službu čo najrýchlejšie, aj pomocou dočasných riešení. Keď vznikne problém, cieľom je vyšetriť hlavnú príčinu problému, aby sa identifikovala zmena, ktorá zabezpečí, že problém a súvisiace incidenty sa už neobjavia.

5.1. Identifikácia a záznam problému

V závislosti od toho, ktorá zmluvná strana iniciovala tiket, kontaktným miestom pre otázky súvisiace s daným problémom bude centrum podpory EÚ alebo Švajčiarska.

Jedinečný identifikátor problému je identifikátor, ktorý mu pridelí riadenie IT služieb (ITSM). Musí sa používať pri každej komunikácii týkajúcej sa daného problému.

Problém môže spôsobovať incident alebo môže byť otvorený samostatne s cieľom odstrániť problémy zistené v systéme, a to v akejkoľvek fáze.

5.2. Priorizácia problému

Problémy sa môžu kategorizovať podľa ich závažnosti a priority rovnako ako incidenty s cieľom uľahčiť ich sledovanie, pričom sa zohľadní vplyv súvisiacich incidentov a frekvencia ich výskytu.

5.3. Vyšetrovanie a diagnostika problému

Každá zmluvná strana môže nastoliť problém a centrum podpory iniciujúcej zmluvnej strany bude zodpovedné za jeho zaregistrovanie, pridelenie príslušnému tímu a sledovanie jeho celkového stavu.

Riešiteľská skupina, ktorej bol problém postúpený, je zodpovedná za včasné riešenie problému a za komunikáciu s centrom podpory.

Obidve zmluvné strany sú na požiadanie zodpovedné za zabezpečenie vykonávania pridelených opatrení a za poskytnutie spätnej väzby svojmu vlastnému centru podpory.

5.4. Vyriešenie

Riešiteľská skupina, ktorej je problém pridelený, je zodpovedná za vyriešenie tohto problému a poskytnutie príslušných informácií svojmu vlastnému centru podpory.

Zistenia zo spracovania problému sa majú zaznamenať na budúce použitie.

5.5. Uzavretie problému

Problém sa formálne uzavrie, keď sa problém vyrieši vykonaním zmeny. Centrum podpory, ktoré zaregistrovalo problém, ukončí fázu uzavierania problému a informuje o tom centrum podpory druhej zmluvnej strany.

6. VYBAVOVANIE ŽIADOSTI

Proces vybavovania žiadosti je komplexné vybavovanie žiadosti o novú alebo existujúcu službu od okamihu jej zaregistrovania a schválenia až do momentu jej uzavretia. Žiadosti o služby majú zvyčajne menší rozsah, sú vopred definované, opakovateľné, časté, vopred schválené a majú charakter procedurálnych žiadostí.

Hlavné kroky, ktoré sa musia dodržať, sú uvedené ďalej:

6.1. Iniciovanie žiadosti

Informácie súvisiace so žiadosťou o službu sa predkladajú centru podpory EÚ alebo Švajčiarska e-mailom, telefonicky alebo prostredníctvom nástroja riadenia IT služieb (ITSM) alebo akéhokoľvek iného dohodnutého komunikačného kanála.

6.2. Registrovanie a analýza žiadostí

Pre všetky žiadosti o službu by kontaktným miestom malo byť centrum podpory EÚ alebo Švajčiarska, v závislosti od toho, ktorá zmluvná strana žiadosť o službu predložila. Toto centrum podpory bude zodpovedné za riadnu registráciu a analýzu žiadosti o službu.

6.3. Schválenie žiadosti

Pracovník centra podpory zmluvnej strany, ktorá žiadosť o službu podala, skontroluje, či je potrebné schválenie druhej zmluvnej strany, a ak áno, tak si ho vyžiada. Ak žiadosť o službu nie je schválená, centrum podpory tiket aktualizuje a uzavrie ho.

6.4. Vybavovanie žiadosti

Tento krok slúži na účinné a efektívne spracovanie žiadostí o služby. Treba rozlišovať medzi týmito prípadmi:

- Vybavovanie žiadosti o službu sa týka len jednej zmluvnej strany. V tomto prípade táto zmluvná strana vydá pracovné príkazy a koordinuje vykonanie.
- Realizácia žiadosti o službu má vplyv na systém EÚ aj Švajčiarska. V tomto prípade vydávajú centrá podpory pracovné príkazy vo svojej oblasti zodpovednosti. Spracovanie vybavovania žiadosti sa koordinuje medzi obidvoma centrami podpory. Celkovú zodpovednosť nesie to centrum podpory, ktoré dostalo a iniciovalo žiadosť o službu.

Keď bola žiadosť o službu vyriešená, musí sa umiestniť do stavu „vyriešené“.

6.5. Postúpenie žiadosti

Centrum podpory môže v prípade potreby postúpiť nevybavenú žiadosť o službu príslušnému tímu (tretia strana).

Žiadosť sa postupuje príslušným tretím stranám, t. j. centrum podpory EÚ bude musieť postupovať cez centrum podpory Švajčiarska, ak má byť žiadosť postúpená švajčiarskej tretej strane a naopak.

Tretia strana, ktorej bola postúpená žiadosť o službu, je zodpovedná za včasné riešenie žiadosti o službu a za komunikáciu s centrom podpory, ktorá jej žiadosť o službu postúpila.

Centrum podpory, ktoré zaregistrovalo žiadosť o službu, je zodpovedné za sledovanie jej celkového stavu a jej pridelenie.

6.6. Kontrola vybavovania žiadostí

Pred uzavretím žiadosti predkladá príslušné centrum podpory správu o žiadosti o službu na účely konečnej kontroly kvality. Cieľom je zabezpečiť, aby sa daná žiadosť o službu skutočne spracovala a aby sa dostatočne podrobne uviedli všetky informácie potrebné na opis životného cyklu žiadosti. Okrem toho sa zistenia zo spracovania žiadosti majú zaznamenať pre budúce použitie.

6.7. Uzavretie žiadosti

Ak sa zmluvné strany, ktorým bola žiadosť o službu pridelená, dohodnú, že daná žiadosť bola vybavená, a žiadateľ sa domnieva, že daný prípad je vyriešený, nastaví sa stav „uzavreté“.

Žiadosť o službu sa formálne uzavrie vtedy, keď centrum podpory, ktoré danú žiadosť o službu zaregistrovalo, ukončí fázu uzavretia žiadosti a informuje o tom centrum podpory druhej zmluvnej strany.

7. RIADENIE ZMIEN

Cieľom je zabezpečiť, aby sa používali štandardizované metódy a postupy na efektívne a rýchle spracovanie všetkých zmien týkajúcich sa kontroly IT infraštruktúry s cieľom minimalizovať počet akýchkoľvek súvisiacich incidentov a ich vplyv na službu. Zmeny v IT infraštruktúre môžu vzniknúť v reakcii na problémy alebo externe vznesené požiadavky, napr. legislatívne zmeny, alebo proaktívne na účely zlepšenia efektívnosti a účinnosti alebo s cieľom umožniť obchodné iniciatívy alebo ich zohľadniť.

Proces riadenia zmien zahŕňa rôzne kroky, ktoré zachytávajú všetky podrobnosti týkajúce sa žiadosti o zmenu na účely budúceho sledovania. Týmito procesmi sa zabezpečuje, aby sa zmena pred zavedením validovala a otestovala. Úspešné zavedenie zmeny sa realizuje prostredníctvom procesu riadenia vydaní.

7.1. Žiadosť o zmenu

Žiadosť o zmenu (RFC) sa predkladá tímu pre riadenie zmien na validáciu a schválenie. V prípade všetkých žiadostí o zmenu by kontaktným bodom malo byť centrum podpory EÚ alebo Švajčiarska, v závislosti od toho, ktorá zmluvná strana žiadosť predložila. Toto centrum podpory bude zodpovedné za riadnu registráciu a analýzu žiadosti.

K predloženiu žiadostí o zmenu môže dôjsť z dôvodu:

- incidentu, ktorý zmenu spôsobí,
- existujúceho problému, v dôsledku ktorého dôjde k zmene,
- požiadavky na novú zmenu zo strany koncového používateľa,
- zmeny v dôsledku prebiehajúcej údržby,
- legislatívnej zmeny.

7.2. Hodnotenie a plánovanie zmien

Táto etapa sa týka posudzovania zmien a činností plánovania. Zahŕňa činnosti priorizácie a plánovania s cieľom minimalizovať riziko a vplyv.

Ak má vykonávanie RFC vplyv tak na EÚ, ako aj na Švajčiarsko, zmluvná strana, ktorá RFC zaregistrovala, v spolupráci s druhou stranou overí hodnotenie a plánovanie danej zmeny.

7.3. Schválenia zmien

Každá zaregistrovaná žiadosť o zmenu sa musí schváliť na príslušnej úrovni postúpenia.

7.4. Vykonanie zmeny

Vykonanie zmeny sa uskutočňuje procesom riadenia vydaní. Tímy obidvoch zmluvných strán pre riadenie vydaní postupujú podľa vlastných postupov, ktoré zahŕňajú plánovanie a testovanie. Po dokončení vykonania zmeny sa uskutoční kontrola zmeny. V záujme postupu podľa plánu sa existujúci proces riadenia zmien neustále prehodnocuje a v prípade potreby aktualizuje.

8. RIADENIE VYDANÍ

Vydanie predstavuje jednu alebo viacero zmien IT služieb súhrnne uvedených v pláne vydaní, ktoré budú musieť byť povolené, pripravené, vytvorené, otestované a zavedené. Vydanie môže predstavovať opravu chyby, zmenu hardvéru alebo iných komponentov, zmeny softvéru, aktualizáciu

verzií aplikácií, zmeny dokumentácie a/alebo procesov. Obsah každého vydania sa riadi, testuje a zavádza ako jeden celok.

Cieľom riadenia vydaní je naplánovať, vytvoriť, otestovať a validovať a pritom zabezpečiť schopnosť poskytovať navrhované služby, prostredníctvom ktorých sa budú plniť požiadavky zainteresovaných strán a dosahovať plánované ciele. Počas koordinácie návrhu sa zadefinujú a zdokumentujú kritériá prijateľnosti týkajúce sa všetkých zmien danej služby a poskytnú sa tímom zodpovedným za riadenie vydaní.

Vydanie zvyčajne pozostáva z viacerých opráv problémov a vylepšení služby. Obsahuje požadovaný nový alebo zmenený softvér a akýkoľvek nový alebo zmenený hardvér potrebný na vykonanie schválených zmien.

8.1. Plánovanie vydania

Prvým krokom v tomto procese je priradenie schválených zmien do balíkov vydaní a definovanie rozsahu a obsahu vydaní. Na základe týchto informácií sa v rámci čiastkového procesu plánovania vydaní vypracuje harmonogram vytvorenia, testovania a zavedenia vydania.

V rámci plánovania by sa mal zadefinovať:

- rozsah a obsah vydania,
- posúdenie rizika a rizikový profil vydania,
- klient/používatelia, ktorých sa vydanie dotkne,
- tím zodpovedný za vydanie,
- stratégia realizácie a zavedenia,
- Zdroje pre vydanie a zavedenie.

Obidve zmluvné strany sa navzájom informujú o plánovaní svojich vydaní a časoch údržby. Ak sa vydanie týka tak EÚ, ako aj Švajčiarska, koordinujú plánovanie a určujú spoločný čas údržby.

8.2. Vytvorenie a otestovanie balíka vydaní

Pri vytváraní a testovaní procesu riadenia vydaní sa stanoví prístup realizácie vydania alebo balíka vydaní a údržby kontrolovaného prostredia pred zmenou produkcie, ako aj testovanie všetkých zmien vo všetkých zavedených prostrediach.

Ak sa vydanie týka EÚ, ako aj Švajčiarska, koordinujú plány dodania a testovanie. Patria sem tieto aspekty:

- spôsob a čas dodania jednotiek vydania a komponentov služby,
- aké sú obvyklé časy realizácie; čo sa stane, ak dôjde k oneskoreniu,
- ako sledovať napredovanie dodávky a získať potvrdenie,
- kritériá na monitorovanie a určenie úspešnosti zavádzania vydania,
- spoločné testovacie prípady pre príslušné funkcie a zmeny.

Na konci tohto čiastkového procesu sú všetky požadované komponenty vydania pripravené na vstup do fázy spustenia reálnej prevádzky.

8.3. Príprava na zavedenie

Prípravný čiastkový proces zabezpečuje, aby boli komunikačné plány definované správne a oznámenia pripravené na odoslanie všetkým dotknutým zainteresovaným stranám a konečným

používateľom a aby sa dané vydanie začlenilo do procesu riadenia zmien s cieľom zabezpečiť kontrolované vykonanie všetkých zmien a ich schválenie požadovanými subjektmi.

Ak sa vydanie týka EÚ, ako aj Švajčiarska, obidve zmluvné strany koordinujú tieto činnosti:

- záznam žiadosti o zmenu v súvislosti s plánovaním a prípravou zavedenia do produkčného prostredia,
- vytvorenie plánu vykonávania,
- spôsob návratu, aby bolo v prípade zlyhania zavedenia možné vrátiť predchádzajúci stav,
- oznámenia zaslané všetkým stranám,
- žiadosť o schválenie realizácie vydania na príslušnej úrovni postúpenia.

8.4. Návrat do pôvodného stavu

Ak sa zavedenie nepodarilo zrealizovať alebo z testovania vyplynulo, že zavedenie nebolo úspešné alebo nezodpovedalo dohodnutým kritériám prijateľnosti/kvality, tímy obidvoch zmluvných strán, ktoré sú zodpovedné za riadenie vydaní, budú musieť vrátiť systém do pôvodného stavu. Bude potrebné informovať všetky potrebné zainteresované strany vrátane dotknutých/cieľových koncových používateľov. Až do schválenia sa proces môže znovu začať v ktorejkoľvek z predchádzajúcich etáp.

8.5. Preskúmanie a uzavretie vydania

Pri kontrole zavedenia by sa mali vykonať tieto činnosti:

- získať spätnú väzbu o spokojnosti zákazníkov a používateľov s dodaním a zavedením služby (zhromaždiť spätnú väzbu a zohľadniť ju pri neustálom zlepšovaní služby),
- preskúmať všetky kritériá kvality, ktoré neboli splnené,
- skontrolovať, či sú všetky opatrenia, potrebné opravy a zmeny kompletné,
- zabezpečiť, aby po dokončení zavedenia nezostali nevyriešené žiadne otázky týkajúce sa funkčnosti, zdrojov, kapacity alebo výkonnosti,
- skontrolovať, či sú všetky problémy, známe chyby a dočasné riešenia zdokumentované a akceptované zákazníkom, koncovými používateľmi, prevádzkovou podporou a inými dotknutými stranami,
- monitorovať incidenty a problémy spôsobené zavedením (poskytnúť podporu operačným tímom v začiatočnej fáze v prípade, že vydanie spôsobilo zvýšenie objemu práce),
- aktualizovať podpornú dokumentáciu (t. j. technické informačné dokumenty),
- formálne odovzdať zavedenie vydania do prevádzkových operácií,
- zdokumentovať získané poznatky,
- zhromaždiť od realizačných tímov súhrnnú dokumentáciu o vydaní,
- formálne uzavrieť vydanie po overení záznamu týkajúceho sa žiadosti o zmenu.

9. RIADENIE BEZPEČNOSTNÝCH INCIDENTOV

Riadenie bezpečnostných incidentov je proces riešenia bezpečnostných incidentov, s cieľom informovať potenciálne ovplyvnené zainteresované strany o incidente; hodnotenie incidentu a priorizácia a reakcia na incident v záujme vyriešenia všetkých skutočných alebo potenciálnych narušení dôvernosti, dostupnosti alebo integrity citlivých informačných aktív alebo podozrení na takéto narušenie.

9.1. Kategorizácia incidentov v oblasti bezpečnosti informácií

Všetky incidenty, ktoré majú vplyv na prepojenie medzi registrom Únie a švajčiarskym registrom, sa analyzujú s cieľom určiť možné narušenie dôvernosti, integrity alebo dostupnosti akýchkoľvek citlivých informácií zaznamenaných v zozname citlivých informácií (SIL).

V kladnom prípade sa incident charakterizuje ako incident v oblasti bezpečnosti informácií, ktorý sa okamžite zaregistruje v nástroji riadenia IT služieb (ITSM) a ako taký sa riadi.

9.2. Riešenie incidentov v oblasti bezpečnosti informácií

Bezpečnostné incidenty sa riešia na 3. úroveň postúpenia, pričom riešením incidentov sa bude zaoberať osobitný tím pre riadenie incidentov (IMT).

IMT je zodpovedný za:

- vykonanie prvej analýzy, kategorizovanie a stanovenie závažnosti incidentu,
- koordináciu činností všetkých zainteresovaných strán vrátane úplného zdokumentovania analýzy konkrétneho incidentu, rozhodnutí prijatých na riešenie daného incidentu a možných zistených nedostatkov,
- v závislosti od závažnosti bezpečnostného incidentu za včasné postúpenie na príslušnú úroveň na účely informovania a/alebo rozhodnutia.

V procese riadenia bezpečnosti informácií sú všetky informácie týkajúce sa udalostí klasifikované na najvyššej úrovni citlivosti informácií, v každom prípade však minimálne ako SENSITIVE: ETS.

V prípade prebiehajúceho vyšetrovania a/alebo nedostatku, ktorý by sa mohol zneužiť, až pokým nedôjde k odstráneniu predmetného problému, sa informácie klasifikujú ako SPECIAL HANDLING: *ETS Critical*.

9.3. Identifikácia bezpečnostných incidentov

Na základe typu bezpečnostného incidentu určí pracovník pre bezpečnosť informácií príslušné organizácie, ktoré majú byť zapojené do činností IMT a ktoré majú byť súčasťou tohto tímu.

9.4. Analýza bezpečnostných incidentov

Pri skúmaní incidentu spolupracuje IMT so všetkými zainteresovanými organizáciami a podľa potreby s príslušnými členmi ich tímov. Počas analýzy sa určí rozsah dôvernosti, integrity alebo straty dostupnosti aktív a posúdia sa dôsledky pre všetky dotknuté organizácie. Ďalej sa vymedzia počiatočné a následné opatrenia na vyriešenie incidentu a na riadenie jeho vplyvu vrátane vplyvu týchto opatrení na zdroje.

9.5. Posudzovanie závažnosti bezpečnostných incidentov, postúpenie a podávanie správ

IMT posúdi závažnosť každého nového bezpečnostného incidentu po jeho označení za bezpečnostný incident a okamžite začne s realizáciou potrebného opatrenia podľa závažnosti incidentu.

9.6. Podávanie správ o reakcii na bezpečnostný incident

IMT uvedie informácie o obmedzení dôsledkov incidentu a výsledky obnovy služby v správe o reakcii na incident v oblasti bezpečnosti informácií. Správa sa predkladá na 3. úrovni postúpenia pomocou zabezpečeného e-mailu alebo iných vzájomne akceptovaných prostriedkov bezpečnej komunikácie.

Zodpovedná zmluvná strana preskúma obmedzenia dôsledkov a výsledky obnovy služby a:

- opäť pripojí register v prípade, že bol predtým odpojený,
- zabezpečí komunikáciu o incidente s tímami zodpovednými za správu registra,
- uzavrie incident.

IMT by mal zabezpečeným spôsobom v správe o reakcii na incident v oblasti bezpečnosti informácií uviesť relevantné podrobnosti s cieľom zabezpečiť konzistentné zaznamenávanie a komunikáciu a umožniť okamžité a náležité opatrenia na obmedzenie dôsledkov incidentu. Po jeho dokončení predloží IMT v príslušnej lehote záverečnú správu o reakcii na incident v oblasti bezpečnosti informácií.

9.7. Monitorovanie, budovanie kapacít a kontinuálne zlepšovanie

IMT poskytne správy o všetkých bezpečnostných incidentoch 3. úrovni postúpenia. Správy budú použité na tejto úrovni postúpenia, aby bolo možné určiť:

- slabé miesta v bezpečnostných kontrolách a/alebo operačnom postupe, ktoré treba posilniť,
- prípadné potreby zdokonaliť tento postup s cieľom zlepšiť jeho účinnosť pri reakcii na incidenty,
- možnosti školenia a budovania kapacít v záujme ďalšieho posilnenia odolnosti registračných systémov v oblasti bezpečnosti informácií, znižovania rizika budúcich incidentov a minimalizovania ich vplyvu.

10. RIADENIE BEZPEČNOSTI INFORMÁCIÍ

Cieľom riadenia bezpečnosti informácií je zabezpečiť dôvernosť, integritu a dostupnosť utajovaných skutočností, údajov a IT služieb organizácie. Okrem technických komponentov vrátane ich návrhu a testovania (pozri prepájacie technické normy) sú na splnenie bezpečnostných požiadaviek pre trvalé prepojenie registra potrebné tieto spoločné operačné postupy.

10.1. Identifikácia citlivých informácií

Citlivosť informácie sa posudzuje stanovením, aký vplyv na podnik by mohlo mať narušenie bezpečnosti v prípade tejto informácie (napr. finančné straty, poškodenie povesti, porušenie právnych predpisov...).

Citlivé informačné aktíva sa identifikujú na základe ich vplyvu na prepojenie.

Úroveň citlivosti týchto informácií sa posudzuje podľa škály citlivosti, ktorá sa uplatňuje na toto prepojenie a je podrobne opísaná v oddiele tohto dokumentu „Riešenie incidentov v oblasti bezpečnosti informácií“.

10.2. Úrovne citlivosti informačných aktív

Informačné aktívum sa pri svojej identifikácii klasifikuje podľa týchto pravidiel:

- pri identifikácii aspoň jednej VYSOKEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako SPECIAL HANDLING: *ETS Critical*,
- pri identifikácii aspoň jednej STREDNEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako SENSITIVE: *ETS*,
- pri identifikácii iba NÍZKEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako Marking EU: SENSITIVE: *ETS Joint Procurement.* Marking CH: LIMITED: ETS.

10.3. Priradenie vlastníka informačných aktív

Všetky informačné aktíva by mali mať priradeného vlastníka. Informačné aktíva ETS, ktoré patria k prepojeniu medzi EUTL a SSTL alebo sú s ním spojené, by sa mali uviesť v spoločnom inventúrnom súpise aktív vedenom obidvomi zmluvnými stranami. Informačné aktíva ETS mimo prepojenia medzi EUTL a SSTL by sa mali zahrnúť do inventúrneho súpisu aktív, ktorý vedie príslušná zmluvná strana.

Zmluvné strany sa majú dohodnúť na vlastníctve každého informačného aktíva, ktoré patrí k prepojeniu medzi EUTL a SSTL, alebo je s ním spojené. Vlastník informačného aktíva je zodpovedný za posúdenie jeho citlivosti.

Vlastník by mal mať dostatok pracovníkov s funkciami a skúsenosťami zodpovedajúcimi hodnote prideleného aktíva, resp. aktív. Mala by sa dohodnúť a formalizovať zodpovednosť vlastníka za aktívum, resp. aktíva, ako aj jeho povinnosť zachovávať požadovanú úroveň dôvernosti, integrity a dostupnosti.

10.4. Registrácia citlivých informácií

Všetky citlivé informácie sa registrujú v zozname citlivých informácií.

V relevantných prípadoch sa zohľadní a v zozname citlivých informácií zaregistruje súhrn citlivých informácií, ktorý by mohol mať väčší vplyv, ako je vplyv jedinej informácie (napr. súbor informácií uložených v databáze systému).

Zoznam citlivých informácií nemá stály charakter. Charakter hrozieb, zraniteľných miest či pravdepodobnosť alebo dôsledky bezpečnostných incidentov súvisiacich s aktívami sa môžu bez akéhokoľvek upozornenia meniť, pričom sa do prevádzky registračných systémov môžu zavádzať nové aktíva.

Zoznam citlivých informácií sa preto pravidelne preskúmava a akékoľvek nové informácie, ktoré sú označené za citlivé, sa do neho okamžite zaregistrujú.

Zoznam citlivých informácií obsahuje v prípade každého zápisu aspoň tieto informácie:

- opis informácie,
- vlastníka informácie,
- úroveň citlivosti,
- upozornenie o tom, či informácie zahŕňajú osobné údaje,
- dodatočné informácie, ak sú potrebné.

10.5. Zaobchádzanie s citlivými informáciami

Ak sa citlivé informácie spracúvajú mimo prepojenia medzi registrom Únie a švajčiarskym registrom, spracúvajú sa v súlade s pokynmi pre zaobchádzanie.

Citlivé informácie spracúvané v prepojení medzi registrom Únie a švajčiarskym registrom sa spracúvajú v súlade s bezpečnostnými požiadavkami zmluvných strán.

10.6. Riadenie prístupu

Cieľom riadenia prístupu je udeliť oprávneným používateľom právo na využívanie služby a zároveň zabrániť prístupu neoprávnených používateľov. Riadenie prístupu sa niekedy označuje aj ako „riadenie práv“ alebo „riadenie totožnosti“.

V prípade trvalého prepojenia registra a jeho fungovania potrebujú obidve zmluvné strany prístup k týmto komponentom:

- Wiki: prostredie pre spoluprácu na výmenu spoločných informácií, ako je plánovanie vydaní,
- nástroj riadenia IT služieb (ITSM) na riadenie incidentov a problémov (pozri kapitolu 3 „Prístup a normy“),
- systém výmeny správ: každá zmluvná strana zabezpečuje bezpečný systém výmeny správ na účely prenosu správ obsahujúcich údaje o transakciách.

Švajčiarsky správca registra a ústredný správca registra Únie zabezpečujú, aby pre ich zmluvné strany boli prístupy aktuálne a fungovali ako kontaktné miesta, pokiaľ ide o činnosti súvisiace s riadením prístupu. Žiadosti o prístup sa riešia v súlade s postupmi vybavovania žiadosti.

10.7. Správa certifikátov/kľúčov

Každá zmluvná strana je zodpovedná za správu svojich vlastných certifikátov/kľúčov (generovanie, registrácia, ukladanie, inštalácia, používanie, predĺženie platnosti, zrušenie, zálohovanie a obnova platnosti certifikátov/kľúčov). Ako sa uvádza v prepájacích technických normách, musia sa používať len digitálne certifikáty vydané certifikačným orgánom (CA), ktorému obidve zmluvné strany dôverujú. Zaobchádzanie s certifikátmi/kľúčmi a ich uchovávanie musí byť v súlade s ustanoveniami uvedenými v pokynoch pre zaobchádzanie.

Každé zrušenie a/alebo predĺženie platnosti certifikátu a kľúča sa musí koordinovať obidvoma zmluvnými stranami. Tieto procesy prebiehajú v súlade s postupmi vybavovania žiadosti.

Švajčiarsky správca registra a ústredný správca registra Únie si vymenia certifikáty/kľúče cez zabezpečené komunikačné prostriedky podľa ustanovení uvedených v pokynoch pre zaobchádzanie.

Akékoľvek overovanie certifikátov/kľúčov medzi zmluvnými stranami sa uskutoční mimo IP sieť.

PRÍLOHA III

PREPÁJACIE TECHNICKÉ NORMY

podľa článku 3 ods. 7 dohody medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov

Normy pre trvalé prepojenie registrov

Obsah

1. Glosár 27
2. Úvod 30
2.1. Rozsah pôsobnosti 30
2.2. Adresáti 30
3. Všeobecné ustanovenia 31
3.1. Štruktúra komunikačného prepojenia 31
3.1.1. Výmena správ 31
3.1.2. Správa XML – Všeobecný opis 31
3.1.3. Okná pre príjem 31
3.1.4. Toky správ o transakciách 32
3.2. Zabezpečenie prenosu dát 35
3.2.1. Firewall a sieťové prepojenie 35
3.2.2. Virtuálna privátna sieť (VPN) 35
3.2.3. Implementácia IPSec 35
3.2.4. Prenosový protokol zabezpečenej výmeny správ 36
3.2.5. Šifrovanie a podpis XML 36
3.2.6. Šifrovacie kľúče 36
3.3. Zoznam funkcií v rámci prepojenia 36
3.3.1. Obchodné transakcie 36
3.3.2. Protokol zosúhlasenia 37
3.3.3. Skúšobná správa 37
3.4. Požiadavky na evidenciu údajov 37
3.5. Prevádzkové požiadavky 38
4. Ustanovenia o dostupnosti 39
4.1. Návrh dostupnosti komunikácie 39
4.2. Inicializácia, komunikácia, reaktivácia a plán testovania 39

4.2.1. Interné testy infraštruktúry IKT 40
4.2.2. Testy komunikácie 40
4.2.3. Testy celého systému (medzi koncovými bodmi) 40
4.2.4. Testy zabezpečenia 40
4.3. Akceptačné/testovacie prostredie 41
5. Ustanovenia o dôvernosti a integrite 41
5.1. Infraštruktúra na testovanie zabezpečenia 41
5.2. Ustanovenia o pozastavení prepojenia a jeho reaktivácii 42
5.3. Ustanovenia o narušení bezpečnosti 42
5.4. Usmernenia pre testy zabezpečenia 43
5.4.1. Softvér 43
5.4.2. Infraštruktúra 43
5.5. Ustanovenia o posudzovaní rizika 43

1. GLOSÁR

Tabuľka 1-1 – Všeobecné skratky a definície

Skratka/Termín	Definícia
Kvóta	Kvóta oprávňujúca vypustiť jednu tonu ekvivalentu oxidu uhličitého počas určitého obdobia, pričom táto kvóta je platná len na účely splnenia požiadaviek EU ETS alebo ETS Švajčiarska.
CH	Švajčiarska konfederácia
CHU	Typ stacionárnych emisných kvót, nazývaných aj CHU2 (odkazujúcich na druhé záväzné obdobie Kjótskeho protokolu), ktoré vydala CH
CHUA	Švajčiarska kvóta pre leteckú dopravu
COP	Spoločné operačné postupy Spoločne vypracované postupy s cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska.
ETR	Register na obchodovanie s emisnými kvótami
ETS	Systém obchodovania s emisiami
EÚ	Európska únia

Skratka/Termín	Definícia
EUA	Všeobecná kvóta EÚ
EUAA	Kvóta EÚ pre leteckú dopravu
EUCR	Konsolidovaný register Európskej únie
EUTL	Protokol transakcií Európskej únie
Register	Systém účtovania kvót vydaných v rámci ETS, ktorý sleduje vlastníctvo kvót vedených na elektronických účtoch.
SSTL	Dodatkový protokol transakcií Švajčiarska
Transakcia	Proces v registri, ktorý zahŕňa prevod kvóty z jedného účtu na iný.
Systém protokolov transakcií	Protokoly transakcií obsahujú záznam o každej navrhovanej transakcii zaslanej z jedného registra do druhého.

Tabuľka 1-2 Technické skratky a definície

Skratka	Definícia
Asymetrická kryptografia	Používa verejné a súkromné kľúče na šifrovanie a dešifrovanie dát.
Certifikačný orgán (CA)	Subjekt, ktorý vydáva digitálne certifikáty.
Šifrovací kľúč	Informácia, ktorá určuje funkčný výstup šifrovacieho algoritmu.
Dešifrovanie	Opačný proces k šifrovaniu.
Digitálny podpis	Matematická technika používaná na validáciu autentickosti a integrity správy, softvéru alebo digitálneho dokumentu.
Šifrovanie	Proces premeny informácií alebo dát na kód, najmä s cieľom zabrániť neoprávnenému prístupu.
Príjem súboru	Proces čítania súboru.
Firewall	Zariadenie alebo softvér sieťovej bezpečnosti, ktorý monitoruje a kontroluje prichádzajúcu a odchádzajúcu sieťovú prevádzku na základe vopred stanovených pravidiel.
Monitorovanie pravidelného signálu	Pravidelný signál generovaný a monitorovaný hardvérom alebo softvérom s cieľom indikovať bežnú prevádzku alebo synchronizovať iné časti počítačového systému.
IPSEC	IP SECurity. Súbor sieťových protokolov, ktorý autentifikuje a šifruje dátové pakety s cieľom poskytnúť zabezpečenú šifrovanú komunikáciu medzi dvoma počítačmi cez sieť internetového protokolu.
Penetračné testovanie	Spôsob testovania počítačového systému, siete alebo webovej aplikácie, ktorého cieľom je nájsť zraniteľné miesta v oblasti zabezpečenia, ktoré by útočník mohol využiť.
Proces zosúhlasenia	Proces zabezpečenia zhody dvoch súborov záznamov.
VPN	Virtuálna privátna sieť
XML	Rozšíriteľný značkový jazyk. Umožňuje programátorom vytvoriť si vlastné prispôsobené značky, ktoré umožňujú definovať, prenášať, validovať a interpretovať dáta medzi aplikáciami a medzi organizáciami.

2. ÚVOD

V dohode medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov z 23. novembra 2017 (ďalej len „dohoda“) sa stanovuje vzájomné uznávanie emisných kvót, ktoré možno použiť na dosiahnutie súladu v rámci systému obchodovania s emisiami Európskej únie (ďalej len „EU ETS“) alebo systému obchodovania s emisiami Švajčiarska (ďalej len „ETS Švajčiarska“). S cieľom realizovať prepojenie medzi EU ETS a ETS Švajčiarska sa zriadi priame prepojenie medzi protokolom transakcií Európskej únie (European Union Transaction Log – EUTL) registra Únie a dodatkovým protokolom transakcií Švajčiarska (Swiss Supplementary Transaction Log – SSTL) švajčiarskeho registra, čím sa umožní prenos emisných kvót vydaných v rámci ktoréhokoľvek z týchto dvoch ETS medzi registrami (článok 3 ods. 2 dohody). S cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska sa v roku 2020 zaviedlo predbežné riešenie. Od roku 2023 sa prepojenie registrov medzi týmito dvoma systémami obchodovania s emisiami postupne rozvíja do trvalého prepojenia registrov, ktorého zavedenie sa očakáva najneskôr v roku 2024 a ktoré umožní fungovanie prepojených trhov, pokiaľ ide o výhody vyplývajúce z likvidity trhu a vykonávanie transakcií medzi týmito dvoma prepojenými systémami spôsobom, ktorý je rovnocenný s jedným trhom zloženým z dvoch systémov a ktorý umožňuje účastníkom trhu konať tak, ako keby boli na jednom trhu, pričom podlieha len jednotlivým regulačným ustanoveniam zmluvných strán (príloha II k dohode).

Podľa článku 3 ods. 7 dohody švajčiarsky správca registra a ústredný správca registra Únie vypracujú prepájacie technické normy na základe zásad stanovených v prílohe II k dohode s opisom podrobných požiadaviek na vytvorenie stabilného a bezpečného spojenia medzi SSTL a EUTL. Prepájacie technické normy vypracované správcami nadobudnú účinnosť, keď sa prijmú vo forme rozhodnutia spoločného výboru.

Prepájacie technické normy prijal spoločný výbor rozhodnutím č. 2/2020. Aktualizované prepájacie technické normy prijme spoločný výbor rozhodnutím č. 1/2024. V súlade s týmto rozhodnutím a žiadosťami spoločného výboru švajčiarsky správca registra a ústredný správca registra Únie vypracovali a aktualizujú ďalšie technické usmernenia s cieľom sfunkčniť prepojenie a zabezpečiť, aby sa tieto usmernenia neustále prispôsobovali technickému pokroku a/alebo novým požiadavkám týkajúcim sa bezpečnosti a zabezpečenia prepojenia, ako aj jeho účinného a efektívneho fungovania.

2.1. Rozsah pôsobnosti

Tento dokument predstavuje všeobecnú zhodu zmluvných strán dohody týkajúcu sa vytvorenia technických základov prepojenia medzi registrami EU ETS a ETS Švajčiarska. Aj keď uvádza základnú líniu pre technické špecifikácie z hľadiska požiadaviek na štruktúru, služby a zabezpečenie, na sfunkčnenie prepojenia budú potrebné aj niektoré ďalšie podrobné usmernenia.

Na správne fungovanie si prepojenie bude vyžadovať procesy a postupy slúžiace na zabezpečenie jeho ďalšieho sfunkčnenia. Podľa článku 3 ods. 6 dohody sa tieto záležitosti podrobne uvádzajú v dokumente týkajúcom sa spoločných operačných postupov, prijatom rozhodnutím spoločného výboru.

2.2. Adresáti

Tento dokument je určený švajčiarskemu správcovi registra a ústrednému správcovi registra Únie.

3. VŠEOBECNÉ USTANOVENIA

3.1. Štruktúra komunikačného prepojenia

Účelom tohto oddielu je poskytnúť opis všeobecnej štruktúry sfunkčnenia prepojenia medzi EU ETS a ETS Švajčiarska a jej jednotlivých zložiek.

Pretože kľúčovou časťou pre definovanie štruktúry je zabezpečenie, boli prijaté všetky opatrenia, aby sa vytvorila spoľahlivá štruktúra. Trvalé prepojenie registrov využíva mechanizmus výmeny súborov ako implementáciu zabezpečeného prepojenia leteckých rozdielov.

Technické riešenie používa:

- prenosový protokol zabezpečenej výmeny správ,
- správy XML,
- digitálny podpis a šifrovanie založené na XML,
- VPN.

Nasledujúci obrázok poskytuje celkový pohľad na štruktúru trvalého prepojenia registrov:

3.1.1. Výmena správ

Komunikácia medzi registrom Únie a švajčiarskym registrom je založená na mechanizme výmeny správ prostredníctvom zabezpečených kanálov. Každý koniec využíva vlastné úložisko prijatých správ.

Obidve zmluvné strany si vedú záznamy prijatých správ spolu s podrobnosťami o spracovaní.

Chyby alebo neočakávaný stav sa budú oznamovať ako upozornenia a medzi podpornými tímami by sa mal by sa udržiavať ľudský kontakt.

Chyby a neočakávané udalosti sa riešia v súlade s prevádzkovými postupmi stanovenými v procese riadenia incidentov v rámci spoločných operačných postupov.

3.1.2. Správa XML – Všeobecný opis

Správa XML obsahuje jeden z týchto prvkov:

- jednu alebo viacero transakčných žiadostí a/alebo jednu alebo viacero transakčných odpovedí,
- jednu operáciu/odpoveď na zosúhlasenie,
- jednu testovaciu správu.

Každá správa obsahuje záhlavie s týmito údajmi:

- východiskový systém ETS,
- poradové číslo.

3.1.3. Okná pre príjem

Trvalé prepojenie registra je založené na vopred určených oknách pre príjem, po ktorých nasleduje súbor pomenovaných udalostí. Transakčné žiadosti prijaté cez prepojenie budú prijaté len vo vopred stanovených intervaloch a zahŕňajú technickú validáciu odchádzajúcich a prichádzajúcich transakcií. Okrem toho môže zosúhlasenie prebiehať denne a môže sa spustiť manuálne.

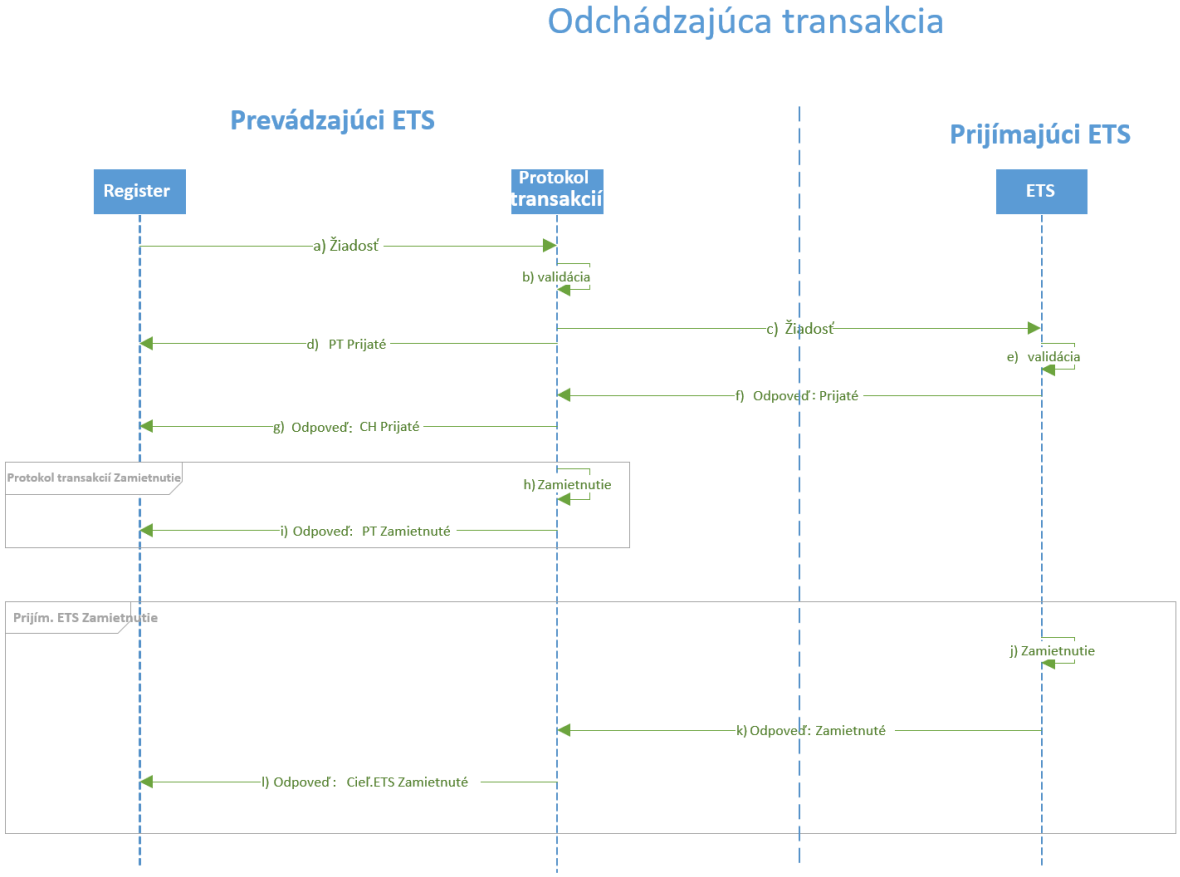
Zmeny frekvencie a/alebo načasovania ktorejkoľvek z týchto udalostí sa budú spracovávať v

súlade s prevádzkovými postupmi stanovenými v procese plnenia požiadaviek spoločných operačných postupov.

3.1.4. Toky správ o transakciách

Odchádzajúce transakcie

Vyjadrené je hľadisko prevádzajúceho ETS. Špecifický tok je znázornený na tomto sekvenčnom diagrame:



Hlavný tok znázorňuje tieto kroky (ako na obrázku vyššie):

a) Pokiaľ ide o prevádzajúci ETS, transakčná žiadosť sa odošle z registra do protokolu transakcií hneď po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch).

b) Protokol transakcií transakčnú žiadosť validuje.

c) Transakčná žiadosť sa odošle do cieľového ETS.

d) Do registra východiskového ETS sa zašle odpoveď o akceptácii.

e) Cieľový ETS transakčnú žiadosť validuje.

f) Cieľový ETS zašle odpoveď o akceptácii späť do protokolu transakcií východiskového ETS.

g) protokol transakcií zašle odpoveď o akceptácii do registra.

Alternatívny tok „Zamietnutie v protokole transakcií“ [ako na obrázku vyššie, začínajúc od písmena a) v hlavnom toku]:

a) Vo východiskovom systéme sa transakčná žiadosť zašle z registra do protokolu transakcií po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch).

b) Protokol transakcií žiadosť nevaliduje.

c) správa o zamietnutí sa zašle do východiskového registra.

Alternatívny tok „Zamietnutie v ETS“ [ako na obrázku vyššie, začínajúc od písmena d) v hlavnom toku]:

a) Vo východiskovom ETS sa transakčná žiadosť zašle z registra do protokolu transakcií po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch).

b) Protokol transakcií transakciu validuje.

c) Transakčná žiadosť sa odošle do cieľového ETS.

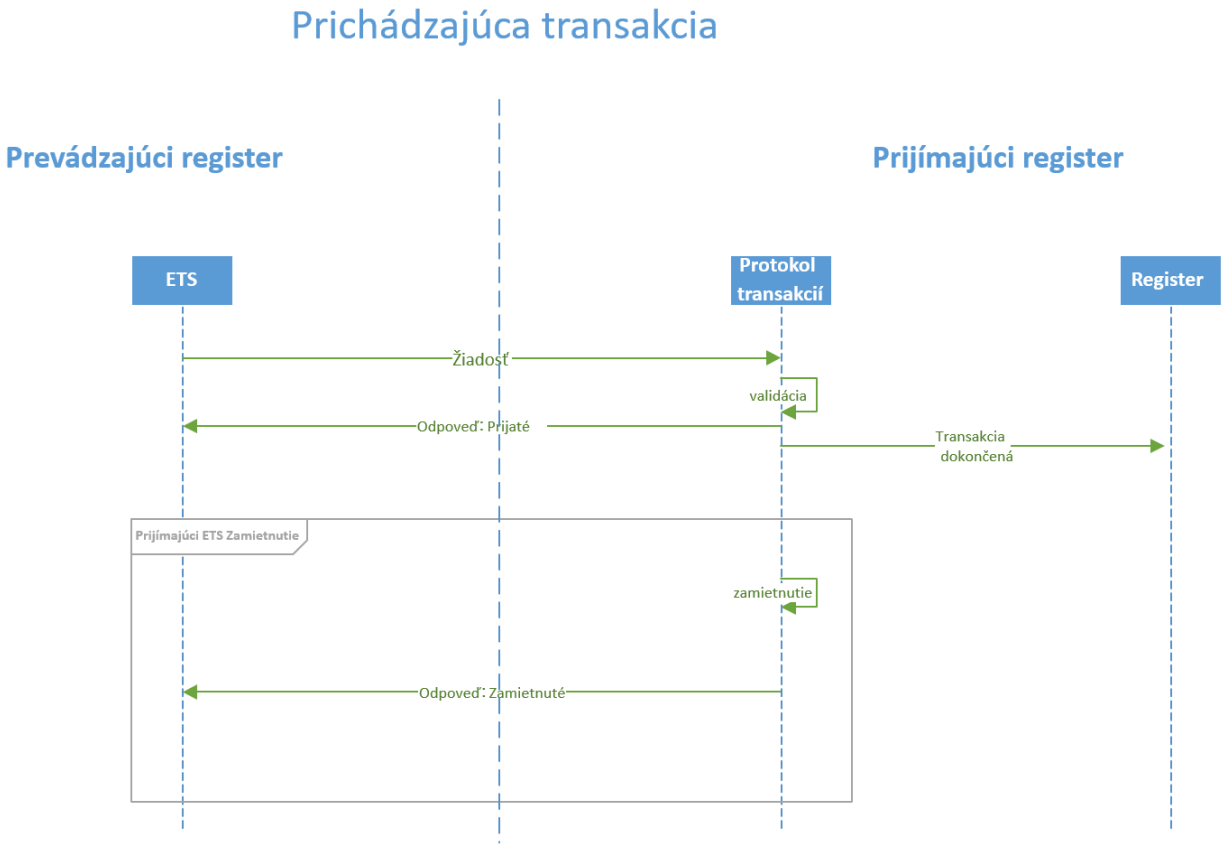
d) Do registra východiskového ETS sa zašle odpoveď o akceptácii.

e) Protokol transakcií prijímajúceho ETS transakciu nevaliduje.

f) Prijímajúci ETS odošle odpoveď o zamietnutí do protokolu transakcií prevádzajúceho ETS.

g) protokol transakcií zašle zamietnutie do registra.

Prichádzajúce transakcie



Vyjadrené je hľadisko prijímajúceho ETS. Špecifický tok je znázornený na tomto sekvenčnom diagrame:

Tento diagram znázorňuje:

1. Keď protokol transakcií prijímajúceho ETS validuje žiadosť, zašle správu o akceptácii do prevádzajúceho ETS a správu „transakcia dokončená“ do registra prijímajúceho ETS.
2. Ak je v prijímajúcom protokole transakcií prichádzajúca žiadosť zamietnutá a zamietne sa, transakčná žiadosť sa do registra prijímajúceho ETS neodošle.

Protokol

Cyklus správ o transakciách zahŕňa len dve správy:

- Prevádzajúci ETS → Návrh na transakciu v prijímajúcom ETS.
- Prijímajúci ETS → Transakčná odpoveď v prevádzajúcom ETS: Prijaté alebo zamietnuté (vrátane dôvodu zamietnutia).
  - Prijaté: Transakcia je dokončená.
  - Zamietnuté: Transakcia je zrušená.

Stav transakcie

- Stav transakcie v rámci prevádzajúceho ETS sa pri odoslaní žiadosti nastaví na „navrhovaná“.

- Stav transakcie v rámci prijímajúceho ETS sa pri prijatí žiadosti nastaví na „navrhovaná“, kým sa nespracuje.
- Stav transakcie v rámci prijímajúceho ETS sa po spracovaní návrhu nastaví na „dokončená“/„zrušená“. Prijímajúci ETS potom odošle príslušnú správu o akceptácii/zamietnutí.
- Stav transakcie prevádzajúceho ETS sa po prijatí a spracovaní správy o akceptácii/zamietnutí nastaví na „dokončená“/„zrušená“.
- Ak nebola prijatá žiadna odpoveď, zostane stav transakcie v prevádzajúcom ETS taký, aký bol navrhnutý.
- Prijímajúci ETS nastaví každú transakciu, ktorá zostane v takom stave, ako bola navrhnutá, dlhšie ako 30 minút, na „zrušenú“.

Incidenty súvisiace s transakciami sa budú riešiť v súlade s prevádzkovými postupmi stanovenými v procese riadenia incidentov v rámci spoločných operačných postupov.

3.2. Zabezpečenie prenosu dát

V priebehu prenosu budú údaje podliehať štyrom stupňom zabezpečenia:

1. Riadenie prístupu do siete: Firewall a vrstva sieťového prepojenia.
2. Šifrovanie na úrovni prenosu: VPN.
3. Šifrovanie na úrovni relácie: Prenosový protokol zabezpečenej výmeny správ.
4. Šifrovanie na úrovni aplikácie: šifrovanie a podpis obsahu XML.

3.2.1. Firewall a sieťové prepojenie

Prepojenie sa vytvorí cez sieť chránenú hardvérovým firewallom. Firewall sa konfiguruje pomocou pravidiel tak, aby sa na server VPN mohli pripojiť len „registrovaní“ klienti.

3.2.2. Virtuálna privátna sieť (VPN)

Všetka komunikácia medzi zmluvnými stranami sa musí chrániť pomocou technológie virtuálnej privátnej siete (VPN). Technológie VPN poskytujú možnosť „tunelovania“ cez sieť, ako je internet, z jedného bodu do druhého, pričom všetka komunikácia je chránená. Pred vytvorením tunela VPN sa budúcemu koncovému bodu klienta vydáva digitálny certifikát, ktorý umožňuje klientovi pri vyjednávaní pripojenia preukázať svoju totožnosť. Každá strana je zodpovedná za inštaláciu certifikátu do svojho koncového bodu VPN. Pomocou digitálnych certifikátov sa každý koncový server VPN pripojí k centrálnej autorite na vyjednanie autentifikačných prihlasovacích údajov. Pri vytváraní tunela sa vyjedná šifrovanie, čím sa zabezpečí, že všetka komunikácia cez tunel bude chránená.

Klientské koncové body VPN sa nakonfigurujú tak, aby udržovali tunel VPN natrvalo s cieľom vždy umožniť spoľahlivú, obojsmernú komunikáciu v reálnom čase medzi zmluvnými stranami.

Európska únia vo všeobecnosti využíva bezpečné transeurópske telematické služby pre správne orgány (STESTA) ako súkromnú sieť založenú na IP. Táto sieť je preto vhodná aj pre trvalé prepojenie registrov.

3.2.3. Implementácia IPSec

Používanie protokolu IPSec na vytvorenie infraštruktúry VPN zabezpečí site-to-site autentifikáciu, integritu dát a šifrovanie dát. Konfigurácie IPSec VPN zabezpečujú riadnu autentifikáciu medzi

dvoma koncovými bodmi v spojení VPN. Zmluvné strany identifikujú a autentifikujú vzdialeného klienta prostredníctvom pripojenia IPSec pomocou digitálnych certifikátov, ktoré poskytla certifikačná autorita uznaná druhým koncovým bodom.

IPSec zabezpečuje aj integritu dát pri všetkej komunikácií prechádzajúcej cez tunel VPN. Dátové pakety sa hašujú a podpisujú pomocou autentifikačných informácií vytvorených VPN. Dôvernosť dát je zaručená podobne umožnením šifrovania IPSec.

3.2.4. Prenosový protokol zabezpečenej výmeny správ

Trvalé prepojenie registra používa na zabezpečenú výmenu dát medzi zmluvnými stranami niekoľko šifrovacích vrstiev. Obidva systémy a ich rôzne prostredia sú vzájomne prepojené na úrovni siete prostredníctvom tunelov VPN. Na úrovni aplikácie sa súbory prenášajú pomocou prenosového protokolu zabezpečenej výmeny správ na úrovni relácie.

3.2.5. Šifrovanie a podpis XML

V rámci XML súborov prebieha podpísanie a šifrovanie na dvoch úrovniach. Každá transakčná žiadosť, transakčná odpoveď a správa o zosúhlasení sa elektronicky podpisujú individuálne.

V druhom kroku sa individuálne šifruje každý čiastkový prvok prvku „správy“.

Okrem toho, ako tretí krok a s cieľom zabezpečiť integritu a nespochybniteľnosť celej správy, sa elektronicky podpisuje koreňový prvok správy. Výsledkom je vysoká úroveň ochrany dátového obsahu XML. V rámci technickej realizácie sa dodržiavajú normy Konzorcia World Wide Web.

Na dešifrovanie a overenie správy sa tento proces realizuje v opačnom poradí.

3.2.6. Šifrovacie kľúče

Na šifrovanie a podpisovanie sa bude používať kryptografia s verejným kľúčom.

V konkrétnom prípade IPSec sa musí používať digitálny certifikát vydaný certifikačnou autoritou (CA), ktorej obidve zmluvné strany dôverujú. Táto certifikačná autorita overuje totožnosť a vydáva certifikáty, ktoré sa použijú na pozitívnu identifikáciu organizácie a nastavenie zabezpečených dátových komunikačných kanálov medzi zmluvnými stranami.

Šifrovacie kľúče sa používajú na podpisovanie a šifrovanie komunikačných kanálov a dátových súborov. Verejné certifikáty si zmluvné strany digitálne vymieňajú pomocou zabezpečených kanálov a overujú sa mimopásmovo (out-of-band). Tento postup je neoddeliteľnou súčasťou procesu riadenia informačnej bezpečnosti v rámci spoločných operačných postupov.

3.3. Zoznam funkcií v rámci prepojenia

Prepojenie špecifikuje prenosový systém pre sériu funkcií, ktorými sa vykonávajú obchodné postupy vychádzajúce z dohody. Prepojenie zahŕňa aj špecifikáciu procesu zosúhlasenia a testovacích správ, ktoré umožnia monitorovanie pravidelného signálu.

3.3.1. Obchodné transakcie

Z obchodného hľadiska má prepojenie štyri (4) typy transakčných žiadostí:

- Externý prevod:

- Po nadobudnutí platnosti prepojenia ETS sú kvóty EÚ a Švajčiarska medzi zmluvnými stranami zameniteľné, a teda plne prevoditeľné.
- Prevod odoslaný cez prepojenie bude zahŕňať prevádzajúci účet v jednom ETS a prijímajúci účet v druhom ETS.
- Prevod môže zahŕňať akékoľvek množstvo štyroch (4) druhov kvót:
    - Švajčiarske všeobecné kvóty (CHU)
    - Švajčiarske kvóty pre leteckú dopravu (CHUA)
    - Všeobecné kvóty EÚ (EUA)
    - Kvóty EÚ pre leteckú dopravu (EUAA)

- Medzinárodné pridelenie:

Prevádzkovatelia lietadiel, ktorých spravuje jeden ETS s povinnosťami v druhom ETS a ktorí majú nárok na bezplatné kvóty z toho druhého ETS, dostanú z druhého systému bezplatné kvóty pre leteckú dopravu prostredníctvom transakcie medzinárodného prideľovania.

- Zrušenie medzinárodného pridelenia:

Táto transakcia sa uskutoční v prípade, keď sa všetky bezplatné kvóty pridelené na holdingový účet prevádzkovateľa lietadla iným ETS musia zrušiť.

- Vrátenie nadmerného pridelenia:

Podobne ako v prípade zrušenia, ale tomto prípade nie je potrebné zrušiť celý prídel, a do prideľujúceho ETS sa musia vrátiť len nadmerne pridelené kvóty.

3.3.2. Protokol zosúhlasenia

Zosúhlasenia sa uskutočnia až potom, ako sa zatvoria okná pre príjem správ, ich validáciu a spracovanie.

Zosúhlasenia sú neoddeliteľnou súčasťou opatrení na zaistenie bezpečnosti a konzistentnosti prepojenia. Obidve zmluvné strany sa pred vytvorením akéhokoľvek harmonogramu dohodnú na presnom načasovaní zosúhlasenia. Plánované denné zosúhlasenie sa môže uskutočniť, ak s tým súhlasia obidve zmluvné strany. Po prijatí sa vykoná aspoň plánované zosúhlasenie.

Každá zmluvná strana však môže kedykoľvek začať manuálne zosúhlasenia.

Zmeny načasovania a frekvencie plánovaného zosúhlasenia sa budú spracovávať v súlade s prevádzkovými postupmi stanovenými v procese plnenia spoločných operačných postupov.

3.3.3. Skúšobná správa

Testovacia správa je určená na testovanie komunikácie medzi koncovými bodmi. Správa bude obsahovať dáta, ktoré ju identifikujú ako test, a bude zodpovedaná po prijatí druhým koncovým bodom.

3.4. Požiadavky na evidenciu údajov

S cieľom podporiť potrebu obidvoch zmluvných strán, aby si zachovali presné a konzistentné informácie, a poskytnúť nástroje na použitie v procese zosúhlasenia, aby sa vyriešili nezrovnalosti, musia obidve zmluvné strany viesť štyri (4) typy protokolov údajov:

- protokoly transakcií,
- protokoly zosúhlasenia,
- archív správ,
- protokoly vnútorného auditu.

Všetky dáta v týchto protokoloch sa uchovávajú aspoň počas troch (3) mesiacov na účely odstraňovania porúch a ich ďalšie uchovávanie bude závisieť od platných právnych predpisov v každom koncovom bode na účely auditu. Súbory protokolov staršie ako tri (3) mesiace sa môžu archivovať na zabezpečenom mieste v nezávislom IT systéme, pokiaľ bude možné ich stiahnuť alebo k nim získať prístup v primeranej lehote.

Protokoly transakcií

Subsystémy EUTL aj SSTL sú implementáciami protokolov transakcií. Tie sú vzájomne overené medzi obidvoma systémami ETS.

Konkrétnejšie, v protokoloch transakcií sa uchová záznam o každej navrhovanej transakcii odoslanej do druhého ETS. Každý záznam obsahuje všetky polia s obsahom transakcie a následný výsledok danej transakcie (odpoveď prijímajúceho ETS). Protokoly transakcií budú viesť aj záznamy o prichádzajúcich transakciách, ako aj o odpovediach zaslaných východiskovému ETS.

Protokoly zosúhlasenia

Protokol zosúhlasenia obsahuje záznam o každej správe o zosúhlasení medzi obidvoma zmluvnými stranami vrátane identifikácie zosúhlasenia, časovej pečiatky a výsledku zosúhlasenia: Stav zosúhlasenia „Schválené“ alebo „Nezrovnalosti“. Správy o zosúhlasení trvalého prepojenia registrov sú neoddeliteľnou súčasťou vymieňaných správ, a preto sa uchovávajú podľa opisu v časti „archív správ“.

Obidve zmluvné strany zaznamenajú každú žiadosť a odpoveď na ňu v protokole zosúhlasenia. Aj keď sa informácie z protokolu zosúhlasenia nezdieľajú priamo v rámci samotného zosúhlasenia, prístup k tejto informácii môže byť potrebný na vyriešenie nezrovnalostí.

Archív správ

Obidve zmluvné strany sú povinné archivovať kópiu vymieňaných dát (súbory XML), odoslaných a prijatých, a informáciu o tom, či boli tieto dáta alebo správy XML v správnom formáte alebo nie.

Hlavným účelom archivácie je audit s cieľom získať dôkazy o tom, čo bolo druhej strane odoslané a z jej strany prijaté. V tomto zmysle je spolu so súbormi potrebné archivovať aj súvisiace certifikáty.

Tieto súbory budú takisto poskytovať dodatočné informácie na odstraňovanie porúch.

Protokol vnútorného auditu

Tieto protokoly si každá strana definuje a používa sama.

3.5. Prevádzkové požiadavky

Výmena dát medzi obidvoma systémami nie je v trvalom prepojení registrov úplne autonómna, čo znamená, že na fungovanie prepojenia sú potrební operátori a postupy. Na tento účel sú v tomto procese podrobne opísané viaceré úlohy a nástroje.

4. USTANOVENIA O DOSTUPNOSTI

4.1. Návrh dostupnosti komunikácie

Štruktúra trvalého prepojenia registrov je v podstate infraštruktúra IKT a softvér, ktorý umožňuje komunikáciu medzi ETS Švajčiarska a ETS EU. Zabezpečenie vysokej úrovne dostupnosti, integrity a dôvernosti tohto toku dát sa preto stáva základným aspektom, ktorý treba zvažovať pri návrhu trvalého prepojenia registrov. Keďže ide o projekt, v ktorom hlavnú úlohu zohrávajú infraštruktúra IKT, softvér na zákazku a procesy, musia sa zohľadniť všetky tri prvky, aby bolo možné navrhnúť odolný systém.

Odolnosť infraštruktúry IKT

Štrukturálne stavebné prvky sú opísané v kapitole o všeobecných ustanoveniach tohto dokumentu. Na strane infraštruktúry IKT zriaďuje trvalé prepojenie registrov odolnú sieť VPN, ktorá vytvára zabezpečené komunikačné tunely, cez ktoré sa môže uskutočňovať zabezpečená výmena správ. Ostatné prvky infraštruktúry sú konfigurované na vysokú dostupnosť a/alebo sa spoliehajú na záložné mechanizmy.

Odolnosť softvéru na zákazku

Softvérové moduly vyvinuté na zákazku zvyšujú odolnosť opakovanými pokusmi o komunikáciu s druhým koncovým bodom po určitý čas, pokiaľ nie je z nejakého dôvodu dostupný.

Odolnosť služieb

V rámci trvalého prepojenia registrov dochádza k výmene údajov medzi zmluvnými stranami vo vopred stanovených intervaloch. Niektoré z krokov požadovaných v stanovenom harmonograme výmeny dát si vyžadujú manuálny zásah zo strany systémových operátorov a/alebo správcov registrov. Vzhľadom na to a s cieľom zvýšiť dostupnosť a úspešnosť výmen:

- Prevádzkové postupy predpokladajú časové lehoty na vykonanie každého kroku.
- Softvérové moduly trvalého prepojenia registrov implementujú asynchrónnu komunikáciu.
- Automatický proces zosúhlasenia bude detegovať, či sa pri prijímaní súborov údajov na ktoromkoľvek konci vyskytli problémy.
- Zohľadňujú sa monitorovacie procesy (infraštruktúra IKT a softvérové moduly na zákazku), ktoré spúšťajú postupy riadenia incidentov (podľa definície v dokumente o spoločných operačných postupoch). Tieto postupy, ktorých cieľom je skrátiť čas na obnovenie bežnej prevádzky po incidentoch, sú nevyhnutné na zabezpečenie vysokej miery dostupnosti.

4.2. Inicializácia, komunikácia, reaktivácia a plán testovania

Všetky rôzne prvky, ktoré sa týkajú štruktúry trvalého prepojenia registrov, prejdú sériou individuálnych a kolektívnych testov s cieľom potvrdiť, že platforma je na úrovni infraštruktúry IKT a informačného systému pripravená. Tieto prevádzkové testy sú povinným predpokladom vždy, keď sa v platforme trvalé prepojenie registrov zmení z pozastavenia na prevádzkový stav.

Aktivácia prepojenia do prevádzkového stavu si potom vyžaduje úspešnú realizáciu vopred vymedzeného testovacieho plánu. Ten musí potvrdiť, že každý register najprv vykonal súbor interných testov, po ktorých nasleduje validácia spojenia medzi koncovými bodmi predtým, než sa začne predkladanie produkčných transakcií medzi obidvoma zmluvnými stranami.

V testovacom pláne by sa mala uvádzať celková testovacia stratégia a podrobnosti o testovacej infraštruktúre. Každý prvok v každom testovacom bloku by mal konkrétne zahŕňať:

- kritériá a nástroje na testovanie,
- úlohy pridelené na vykonanie testu,
- očakávané výsledky (pozitívne a negatívne),
- časový rozvrh testu,
- zaznamenávanie požiadaviek na výsledky testu,
- dokumentáciu o riešení problémov,
- ustanovenia o postúpení.

Ako proces by sa aktivačné testy prevádzkového stavu mohli rozdeliť do štyroch (4) koncepčných blokov alebo fáz:

4.2.1. Interné testy infraštruktúry IKT

Tieto testy majú vykonávať a/alebo kontrolovať jednotlivo správcovia registrov na každom konci.

Každý prvok infraštruktúry IKT na každom konci sa testuje individuálne. Patrí sem každý jednotlivý komponent infraštruktúry. Tieto testy sa môžu vykonať automaticky alebo manuálne, musia však overiť, či je každý prvok infraštruktúry funkčný.

4.2.2. Testy komunikácie

Tieto testy začne každá strana individuálne a dokončia sa v spolupráci s druhým koncom.

Keď budú jednotlivé prvky funkčné, musia sa otestovať komunikačné kanály medzi obidvoma registrami. Na tento účel každá strana overí, že funguje prístup na internet, tunely VPN sú zriadené a že existuje IP prepojiteľnosť site-to-site. Potom by sa druhému koncu mala potvrdiť dosiahnuteľnosť miestnych a vzdialených prvkov infraštruktúry a IP prepojiteľnosť.

4.2.3. Testy celého systému (medzi koncovými bodmi)

Tieto testy sa majú vykonať na každom konci a výsledky sa poskytnú druhej strane.

Po otestovaní komunikačných kanálov a každého jednotlivého komponentu obidvoch registrov pripraví každý koniec sériu simulovaných transakcií a zosúhlasení, v ktorých sú zastúpené všetky funkcie, ktoré sa majú v rámci prepojenia vykonávať.

4.2.4. Testy zabezpečenia

Tieto testy majú byť vykonávané a/alebo spustené správcami registrov na každom konci, ako je podrobne opísané v oddieloch „Usmernenia pre testy zabezpečenia“ a „Ustanovenia o posudzovaní rizika“.

Až po ukončení každej zo štyroch fáz/blokov s predvídateľnými výsledkami možno považovať trvalé prepojenie registrov za sfunkčnené.

Testovacie zdroje

Každá strana musí využívať špecifické testovacie zdroje (špecifický softvér a hardvér infraštruktúry IKT) a vytvorí si vo svojom príslušnom systéme testovacie funkcie s cieľom podporiť manuálnu a priebežnú validáciu platformy. Správcovia registrov môžu kedykoľvek realizovať manuálne individuálne alebo kooperatívne testovacie postupy. Aktivácia prevádzkového stavu je sama osebe manuálny proces.

Podobne sa tiež predpokladá, že platforma v pravidelných intervaloch vykonáva automatické kontroly. Cieľom týchto kontrol je zvýšiť dostupnosť platformy včasnou detekciou potenciálnych problémov v oblasti infraštruktúry alebo softvéru. Tento plán monitorovania platformy tvoria dva prvky:

- Monitorovanie infraštruktúr IKT: na obidvoch koncoch budú infraštruktúru monitorovať poskytovatelia služieb infraštruktúry IKT. Automatické testy budú zahŕňať rôzne prvky infraštruktúry a dostupnosť komunikačných kanálov.
- Monitorovanie aplikácií: v softvérových moduloch trvalého prepojenia registrov sa bude vykonávať monitorovanie systémovej komunikácie na úrovni aplikácie (buď manuálne a/alebo v pravidelných intervaloch), ktoré bude testovať dostupnosť prepojenia medzi koncovými bodmi simulovaním niektorých transakcií cez prepojenie.

4.3. Akceptačné/testovacie prostredie

Štruktúra registra Únie a registra Švajčiarska pozostáva z týchto troch prostredí:

- Produkcia (PROD): V tomto prostredí sú skutočné údaje a spracúvajú sa v ňom skutočné transakcie.
- Schvaľovanie (ACC): Toto prostredie obsahuje dáta, ktoré nie sú skutočné alebo sú anonymizované a reprezentatívne. Ide o prostredie, v ktorom systémoví operátori obidvoch zmluvných strán validujú nové verzie.
- Testovanie (TEST): Toto prostredie obsahuje dáta, ktoré nie sú skutočné alebo sú anonymizované a reprezentatívne. Toto prostredie sa obmedzuje na správcov registrov a má sa používať na vykonávanie integračných testov obidvoma zmluvnými stranami.

S výnimkou VPN sú tieto tri prostredia vzájomne úplne nezávislé, čo znamená, že hardvér, softvér, databázy, virtuálne prostredia, IP adresy a porty sa nastavujú a prevádzkujú sa nezávisle od seba.

Pokiaľ ide o štruktúru VPN, komunikácia medzi týmito tromi prostrediami musí byť úplne nezávislá, čo sa zabezpečuje pomocou systému STESTA.

5. USTANOVENIA O DÔVERNOSTI A INTEGRITE

Mechanizmy a postupy zabezpečenia predpokladajú v prípade operácií prebiehajúcich v prepojení medzi registrom Únie a švajčiarskym registrom zapojenie dvoch osôb (zásada 4 očí). Zapojenie dvoch osôb sa uplatňuje vždy, keď je to potrebné, nemusí sa však uplatňovať na všetky kroky, ktoré správcovia registrov vykonajú.

Požiadavky na zabezpečenie sa posudzujú a riešia v pláne riadenia zabezpečenia, ktorý podobne zahŕňa procesy týkajúce sa riešenia kybernetickobezpečnostných incidentov po prípadnom narušení zabezpečenia. Prevádzková časť týchto procesov je opísaná v spoločných operačných postupoch.

5.1. Infraštruktúra na testovanie zabezpečenia

Každá zmluvná strana sa zaväzuje vytvoriť infraštruktúru na testovanie zabezpečenia (použitím spoločného súboru softvéru a hardvéru používaného pri zisťovaní zraniteľných miest vo vývojovej a prevádzkovej fáze):

- oddelené od produkčného prostredia,
- kde zabezpečenie analyzuje tím nezávislý od vývoja a prevádzky systému.

Každá strana sa zaväzuje vykonávať statickú aj dynamickú analýzu.

V prípade dynamickej analýzy (ako pri penetračnom testovaní) sa obidve zmluvné strany zaväzujú, že obmedzia hodnotenia na testovacie a akceptačné prostredia (ako sú vymedzené v oddiele „Akceptačné/testovacie prostredie“). Výnimky z tejto politiky podliehajú schváleniu obidvoch zmluvných strán.

Pred zavedením do produkčného prostredia sa každý softvérový modul na prepojenie (ako sa vymedzuje v oddiele „Štruktúra komunikačného prepojenia“) otestuje z hľadiska zabezpečenia.

Testovacia infraštruktúra musí byť od produkčnej infraštruktúry oddelená na úrovni siete, ako aj na úrovni infraštruktúry a musí umožňovať vykonávanie testov zabezpečenia potrebných na kontrolu súladu s požiadavkami na zabezpečenie.

5.2. Ustanovenia o pozastavení prepojenia a jeho reaktivácii

V prípade, že existuje podozrenie, že bolo narušené zabezpečenie švajčiarskeho registra, SSTL, registra Únie alebo EUTL, obidve zmluvné strany sa okamžite navzájom informujú a prerušia prepojenie medzi SSTL a EUTL.

Postupy na výmenu informácií, rozhodnutie pozastavení a rozhodnutie o reaktivácii sú súčasťou procesu plnenia žiadostí v rámci spoločných operačných postupov.

Pozastavenie

Pozastavenie prepojenia registrov v súlade s prílohou II k dohode sa môže uskutočniť z:

- administratívnych dôvodov (údržba,...), a teda dôvodov plánovaných,
- dôvodov súvisiacich so zabezpečením (alebo s poruchami IT infraštruktúry), a teda dôvodov neplánovaných.

V naliehavom prípade jedna strana informuje druhú a jednostranne pozastaví prepojenie registrov.

Ak sa prijme rozhodnutie o pozastavení prepojenia registrov, potom každá strana zabezpečí, aby bolo prepojenie prerušené na úrovni siete (blokovaním častí alebo všetkých prichádzajúcich a odchádzajúcich spojení).

Rozhodnutie o pozastavení prepojenia registrov, či už plánované alebo neplánované, sa prijme v súlade s postupom riadenia zmien a kybernetickobezpečnostných incidentov spoločných operačných postupov.

Reaktivácia komunikácie

Rozhodnutie o reaktivácii sa prijme v súlade s opisom v spoločných operačných postupoch a v každom prípade až po úspešnom ukončení postupov testovania zabezpečenia, ako sa podrobne uvádza v oddieloch „Usmernenia pre testy zabezpečenia“ a „Inicializácia, komunikácia, reaktivácia a plán testovania“.

5.3. Ustanovenia o narušení bezpečnosti

Narušenie bezpečnosti sa považuje za kybernetickobezpečnostný incident, ktorý má vplyv na dôvernosť a integritu všetkých citlivých informácií a/alebo dostupnosť systému, ktorý ich spracúva.

Citlivé informácie sú uvedené v zozname citlivých informácií a môžu sa spracúvať v systéme alebo v akejkoľvek súvisiacej časti.

Informácie, ktoré sa priamo týkajú narušenia bezpečnosti sa budú považovať za citlivé, sa označia „SPECIAL HANDLING: *ETS Critical*“ a budú sa spracúvať v súlade s pokynmi na spracúvanie, pokiaľ nie je stanovené inak.

S každým narušením bezpečnosti sa bude zaobchádzať podľa kapitoly spoločných operačných postupov o riadení kybernetickobezpečnostných incidentov.

5.4. Usmernenia pre testy zabezpečenia

5.4.1. Softvér

Aspoň v rámci všetkých dôležitých nových aktualizácií softvéru sa vykoná testovanie zabezpečenia, v prípade potreby vrátane penetračného testovania, a to v súlade s požiadavkami na zabezpečenie stanovenými v prepájacích technických normách, aby bolo možné posúdiť zabezpečenie prepojenia a súvisiace riziká.

Ak za posledných 12 mesiacov nedošlo k žiadnej dôležitej aktualizácii softvéru, vykoná sa testovanie zabezpečenia súčasného systému vzhľadom na vývoj kybernetických hrozieb, ku ktorému za posledných 12 mesiacov došlo.

Testovanie zabezpečenia prepojenia registrov sa vykoná v akceptačnom prostredí a v prípade potreby v produkčnom prostredí a v koordinácii a po vzájomnej dohode obidvoch zmluvných strán.

Pri testovaní webových aplikácií sa budú dodržiavať medzinárodné otvorené normy, napríklad normy vypracované v rámci projektu Open Web Application Security Project (OWASP).

5.4.2. Infraštruktúra

Infraštruktúra podporujúca produkčný systém sa musí pravidelne skenovať s cieľom nájsť zraniteľné miesta (aspoň raz za mesiac) a zistené zraniteľné miesta sa musia opraviť podľa tej istej zásady, ktorá je vymedzená v predchádzajúcej časti, s využitím aktualizovanej databázy zraniteľných miest.

5.5. Ustanovenia o posudzovaní rizika

Ak je penetračné testovanie použiteľné, musí sa zahrnúť do testovania zabezpečenia.

Každá zmluvná strana môže uzavrieť zmluvu so špecializovanou spoločnosťou na testovanie zabezpečenia za predpokladu, že táto spoločnosť:

- má zručnosti a skúsenosti v oblasti takéhoto testovania zabezpečenia,
- nie je priamo podriadená vývojárovi a/alebo jeho dodávateľovi, nie je ani zapojená do vývoja softvéru prepojenia ani nie je subdodávateľom vývojára,
- podpísala dohodu o nezverejňovaní informácií s cieľom zachovať dôvernosť výsledkov a zaobchádzať s nimi na úrovni „SPECIAL HANDLING: ETS Critical“ v súlade s pokynmi na spracúvanie.