2024/1873

5.7.2024

# SKLEP SVETA (EU) 2024/1873

## z dne 24. junija 2024

## o stališču, ki se v imenu Evropske unije zastopa v Skupnem odboru, ustanovljenem s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov, glede spremembe Priloge II k Sporazumu in skupnih delovnih postopkov in tehničnih standardov za povezavo

**(Besedilo velja za EGP)**

SVET EVROPSKE UNIJE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 192(1), v povezavi s členom 218(9) Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Sporazum med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov ([1]) (v nadaljnjem besedilu: Sporazum) je bil podpisan 23. novembra 2017 v skladu s Sklepom Sveta (EU) 2017/2240 ([2]).

(2) Sporazum je bil sklenjen s Sklepom Sveta (EU) 2018/219 ([3]) in je začel veljati 1. januarja 2020.

(3) Na podlagi člena 12(3) Sporazuma lahko Skupni odbor sprejme sklepe, ki so ob začetku njihove veljavnosti zavezujoči za pogodbenici.

(4) Člen 13(2) Sporazuma določa, da lahko Skupni odbor spremeni priloge k Sporazumu.

(5) Člen 3(6) in (7) določa, da bi morali skupni delovni postopki in tehnični standardi za povezavo začeti učinkovati, ko jih Skupni odbor sprejme s sklepom. Skupni odbor je s sklepoma št. 1/2020 ([4]) in št. 2/2020 ([5]) sprejel skupne delovne postopke oziroma tehnične standarde za povezavo.

(6) Primerno je spremeniti Prilogo II k Sporazumu, da bi se upošteval razvoj povezave med registroma sistema EU za trgovanje z emisijami in švicarskega sistema trgovanja z emisijami ter racionalizirale določbe Priloge II glede na tehnološki razvoj. Za zagotovitev skladnosti skupnih delovnih postopkov in tehničnih standardov za povezavo s Prilogo II bi bilo treba spremeniti tudi navedene dokumente.

([1]) UL L 322, 7.12.2017, str. 3.
([2]) Sklep Sveta (EU) 2017/2240 z dne 10. novembra 2017 o podpisu, v imenu Unije, in o začasni uporabi Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov (UL L 322, 7.12.2017, str. 1).
([3]) Sklep Sveta (EU) 2018/219 z dne 23. januarja 2018 o sklenitvi Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov (UL L 43, 16.2.2018, str. 1).
([4]) Sklep št. 1/2020 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. novembra 2020 o sprejetju skupnih delovnih postopkov [2021/1033] (UL L 226, 25.6.2021, str. 2).
([5]) Sklep št. 2/2020 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. novembra 2020 o spremembi prilog I in II k Sporazumu in sprejetju tehničnih standardov za povezavo [2021/1034] (UL L 226, 25.6.2021, str. 16).

(7) Skupni odbor na svojem sedmem sestanku ali prej po pisnem postopku na podlagi člena 8(4) poslovnika Skupnega odbora ([6]) sprejme sklep glede spremembe Priloge II k Sporazumu in spremembe skupnih delovnih postopkov in tehničnih standardov za povezavo.

(8) Primerno je , da se določi stališče, ki se v imenu Unije zastopa v Skupnem odboru glede spremembe Priloge II k Sporazumu in spremembe skupnih operativnih postopkov in tehničnih standardov za povezavo, saj bo sklep za Unijo zavezujoč.

(9) Stališče Unije v Skupnem odboru bi zato moralo temeljiti na priloženem osnutku sklepa –

SPREJEL NASLEDNJI SKLEP:

*Člen 1*

Stališče, ki se v imenu Unije zastopa na sedmem sestanku Skupnega odbora ali prej po pisnem postopku na podlagi člena 8(4) poslovnika Skupnega odbora, temelji na osnutku sklepa Skupnega odbora, ki je priložen temu sklepu.

*Člen 2*

Ta sklep začne veljati na dan sprejetja..

V Luxembourgu, 24. junija 2024

*Za Svet*

*predsednik*

D. CLARINVAL

([6]) Sklep št. 1/2019 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov, z dne 25. januarja 2019 o sprejetju njegovega poslovnika ter Sklep Sveta (EU) 2018/1279 z dne 18. septembra 2018 o stališču, ki se v imenu Evropske unije zastopa v Skupnem odboru, ustanovljenem na podlagi Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov, glede sprejetja njegovega poslovnika (UL L 239, 24.9.2018, str. 8).

**SKLEP ŠT. 1/2024 SKUPNEGA ODBORA, USTANOVLJENEGA S SPORAZUMOM MED EVROPSKO UNIJO IN ŠVICARSKO KONFEDERACIJO O POVEZAVI NJUNIH SISTEMOV TRGOVANJA Z EMISIJAMI TOPLOGREDNIH PLINOV,**

**z dne …**

**glede spremembe Priloge II k Sporazumu in skupnih delovnih postopkov in tehničnih standardov za povezavo**

SKUPNI ODBOR JE –

ob upoštevanju Sporazuma med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov ([1]) (v nadaljnjem besedilu: Sporazum) ter zlasti člena 9 in člena 13(2) Sporazuma,

ob upoštevanju naslednjega:

(1) Sklep št. 2/2019 Skupnega odbora ([2]) je zagotovil začasno rešitev za operacionalizacijo povezave med EU ETS in švicarskim ETS.

(2) Skupni odbor se je na tretjem sestanku strinjal, da je treba analizirati stroškovno učinkovitost stalne povezave med registrom Unije in švicarskim registrom.

(3) Skupni odbor se je na petem sestanku dogovoril o poročilu, ki ga je predložila delovna skupina, ustanovljena s sklepoma št. 1/2020 ([3]) in št. 2/2020 Skupnega odbora ([4]). V tem poročilu je delovna skupina analizirala in priporočila pristop k vzpostavitvi stalne povezave med registrom Unije in švicarskim registrom.

(4) Da bi se upoštevale tehnične zahteve stalne povezave med registrom Unije in švicarskim registrom ter racionalizirale določbe Priloge II k Sporazumu glede na tehnološki razvoj, bi bilo treba spremeniti Prilogo II k Sporazumu.

(5) Za zagotovitev skladnosti skupnih delovnih postopkov in tehničnih standardov za povezavo s Prilogo II k Sporazumu bi bilo treba spremeniti tudi navedene dokumente –

SPREJEL NASLEDNJI SKLEP:

*Člen 1*

1. Priloga II k Sporazumu se nadomesti z besedilom iz Priloge I k temu sklepu.

2. Skupni delovni postopki iz člena 3(6) Sporazuma so določeni v Prilogi II k temu sklepu. Ti nadomeščajo skupne operativne postopke iz Priloge k Sklepu št. 1/2020.

3. Tehnični standardi za povezavo iz člena 3(7) Sporazuma so določeni v Prilogi III k temu sklepu. Ti nadomeščajo tehnične standarde za povezavo iz Priloge k Sklepu št. 2/2020.

([1]) UL L 322, 7.12.2017, str. 3.

([2]) Sklep št. 2/2019 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. decembra 2019 o spremembi prilog I in II k Sporazumu med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov [2020/1359] (UL L 314, 29.9.2020, str. 68).

([3]) Sklep št. 1/2020 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. novembra 2020 o sprejetju skupnih delovnih postopkov [2021/1033] (UL L 226, 25.6.2021, str. 2).

([4]) Sklep št. 2/2020 Skupnega odbora, ustanovljenega s Sporazumom med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 5. novembra 2020 o spremembi prilog I in II k Sporazumu in sprejetju tehničnih standardov za povezavo [2021/1034] (UL L 226, 25.6.2021, str. 16).

*Člen 2*

Ta sklep začne veljati na dan sprejetja.

V …, …

*Za Skupni odbor*

| *sekretarka za Evropsko unijo* | *predsednica* | *sekretarka za Švico* |
|---|---|---|

*PRILOGA I*

*„PRILOGA II*

**TEHNIČNI STANDARDI ZA POVEZAVO**

Za operacionalizacijo povezave med EU ETS in švicarskim ETS je bila leta 2020 vzpostavljena začasna rešitev. Od leta 2023 dalje bo povezava med registroma dveh sistemov trgovanja z emisijami postopoma postajala stalna povezava med registroma, za katero se pričakuje, da se bo začela izvajati najpozneje leta 2024 in bo omogočila delovanje povezanih trgov v smislu koristi od likvidnosti trga ter izvajanje transakcij med obema povezanima sistemoma na način, ki je enakovreden enemu trgu, sestavljenemu iz dveh sistemov, in ki udeležencem na trgu omogoča, da delujejo, kot da bi bili na enem trgu, ob upoštevanju samo posameznih regulativnih določb pogodbenic.

Tehnični standardi za povezavo določajo:

— zgradbo komunikacijske vezi,

— komunikacijo med SSTL in EUTL,

— varnost prenosa podatkov,

— seznam funkcij (transakcije, usklajevanje itd.),

— opredelitev transportne plasti,

— zahteve glede zapisovanja podatkov,

— operativne ureditve (služba za pomoč uporabnikom, podpora),

— načrt za aktivacijo komunikacije in postopek testiranja,

— postopek testiranja varnosti.

V tehničnih standardih za povezavo je določeno, da morajo administratorji sprejeti vse razumne ukrepe za zagotovitev, da SSTL, EUTL in povezava delujejo 24 ur na dan in 7 dni na teden, ter da mora biti motenj v delovanju SSTL, EUTL in komunikacijske vezi čim manj.

Tehnični standardi za povezavo določajo dodatne varnostne zahteve za švicarski register, SSTL, register Unije in EUTL ter se dokumentirajo v ‚načrtu upravljanja varnosti'. Določajo zlasti, da:

— če obstaja sum, da je varnost švicarskega registra, SSTL, registra Unije ali EUTL ogrožena, se pogodbenici takoj medsebojno obvestita o tem ter prekineta povezavo med SSTL in EUTL,

— se pogodbenici zavezujeta, da si bosta v primeru kršitve varnostnih predpisov takoj izmenjali informacije. Če so na voljo tehnični podatki, si administrator švicarskega registra in centralni administrator Unije v 24 urah potem, ko je bil varnostni incident opredeljen kot kršitev varnostnih predpisov, izmenjata poročilo o incidentu (datum, vzrok, vpliv, popravni ukrepi).

Postopek testiranja varnosti, določen s tehničnimi standardi za povezavo, se izvede pred vzpostavitvijo komunikacijske vezi med SSTL in EUTL in ko je potrebna nova različica ali izdaja SSTL ali EUTL.

Tehnični standardi za povezavo poleg produkcijskega okolja zagotavljajo dve testni okolji, in sicer testno razvojno okolje in sprejemno okolje.

Pogodbenici prek administratorja švicarskega registra in centralnega administratorja Unije zagotovita dokaze, da je bila v preteklih 12 mesecih v skladu z varnostnimi zahtevami, ki jih določajo tehnični standardi za povezavo, opravljena neodvisna ocena varnosti njunih sistemov. Pri vseh večjih novih izdajah programske opreme se v skladu z varnostnimi zahtevami, ki jih določajo tehnični standardi za povezavo, opravita testiranje varnosti in zlasti penetracijsko testiranje. Penetracijskega testiranja ne izvede razvijalec programske opreme ali njegov podizvajalec.“

*PRILOGA II*

**SKUPNI DELOVNI POSTOPKI NA PODLAGI ČLENA 3(6) SPORAZUMA MED EVROPSKO UNIJO IN ŠVICARSKO KONFEDERACIJO O POVEZAVI NJUNIH SISTEMOV TRGOVANJA Z EMISIJAMI TOPLOGREDNIH PLINOV**

## Postopki za stalno povezavo med registroma

Kazalo


1. GLOSAR . . . 9
2. UVOD . . . 9
2.1. Obseg . . . 10
2.2. Naslovniki . . . 10
3. PRISTOP IN STANDARDI . . . 10
4. OBVLADOVANJE INCIDENTOV . . . 11
4.1. Odkrivanje in evidentiranje incidentov . . . 11
4.2. Razvrščanje in začetna podpora . . . 11
4.3. Preiskava in diagnoza . . . 12
4.4. Reševanje in obnovitev . . . 12
4.5. Zaključek incidenta . . . 12
5. ODPRAVLJANJE TEŽAV . . . 13
5.1. Opredelitev in evidentiranje težave . . . 13
5.2. Prednostno razvrščanje težav . . . 13
5.3. Preiskava in diagnoza težav . . . 13
5.4. Reševanje . . . 13
5.5. Zaključek težave . . . 13
6. IZPOLNJEVANJE ZAHTEVKOV . . . 13
6.1. Vlaganje zahtevkov . . . 13
6.2. Evidentiranje in analiza zahtevkov . . . 14
6.3. Odobritev zahtevkov . . . 14
6.4. Izpolnjevanje zahtevkov . . . 14
6.5. Prenos zahtevkov na višjo raven . . . 14
6.6. Pregled izpolnjevanja zahtevkov . . . 14
6.7. Zaključek zahtevka . . . 14
7. UPRAVLJANJE SPREMEMB . . . 14
7.1. Zahtevek za spremembo . . . 15
7.2. Ocenjevanje in načrtovanje spremembe . . . 15
7.3. Odobritve sprememb . . . 15
7.4. Izvedba sprememb . . . 15
8. UPRAVLJANJE IZDAJ . . . 15
8.1. Načrtovanje izdaje . . . 15
8.2. Priprava in preskus svežnja izdaje . . . 16
8.3. Priprava na uvedbo . . . 16

8.4. Povrnitev izdaje . . . 16
8.5. Pregled in zaključek izdaje . . . 16
9. OBVLADOVANJE VARNOSTNIH INCIDENTOV . . . 17
9.1. Kategorizacija incidentov v zvezi z informacijsko varnostjo . . . 17
9.2. Ravnanje v primeru incidentov v zvezi z informacijsko varnostjo . . . 17
9.3. Opredelitev varnostnega incidenta . . . 17
9.4. Analiza varnostnega incidenta . . . 17
9.5. Ocenjevanje resnosti varnostnega incidenta, prenos na višjo raven in poročanje . . . 17
9.6. Poročanje o odzivu na varnostni incident . . . 18
9.7. Spremljanje, krepitev zmogljivosti in nenehno izboljševanje . . . 18
10. UPRAVLJANJE INFORMACIJSKE VARNOSTI . . . 18
10.1. Opredelitev občutljivih informacij . . . 18
10.2. Ravni občutljivosti informacijskih sredstev . . . 18
10.3. Določitev lastnika informacijskih sredstev . . . 18
10.4. Evidentiranje občutljivih informacij . . . 19
10.5. Ravnanje z občutljivimi informacijami . . . 19
10.6. Upravljanje dostopa . . . 19
10.7. Upravljanje potrdil/ključev . . . 19

1. GLOSAR

**Preglednica 1-1: Kratice in opredelitve pojmov**

| Kratica/pojem | Opredelitev |
|---|---|
| Overitelj potrdil | Subjekt, ki izdaja digitalna potrdila |
| CH | Švicarska konfederacija |
| ETS | Sistem za trgovanje z emisijami |
| EU | Evropska unija |
| IMT | Skupina za obvladovanje incidentov |
| Informacijska sredstva | Informacije, ki imajo določeno vrednost za podjetje ali organizacijo |
| IT | Informacijska tehnologija |
| ITIL | Knjižnica infrastrukture informacijske tehnologije |
| ITSM | Upravljanje storitev IT |
| LTS | Tehnični standardi za povezavo |
| Register | Sistem obračunavanja za pravice, izdane v ETS, s katerim se vodi evidenca o lastništvu pravic na elektronskih računih. |
| RFC | Zahtevek za spremembo |
| SIL | Seznam občutljivih informacij |
| SR | Zahtevek za storitev |
| Wiki | Spletno mesto, ki uporabnikom omogoča izmenjavo informacij in znanja z dodajanjem ali prilagajanjem vsebine neposredno prek spletnega brskalnika. |

2. UVOD

Sporazum med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 23. novembra 2017 (v nadaljnjem besedilu: Sporazum) določa medsebojno priznavanje pravic do emisije, ki se lahko uporabljajo za skladnost v okviru sistema Evropske unije za trgovanje z emisijami (v nadaljnjem besedilu: EU ETS) ali sistema Švice za trgovanje z emisijami (v nadaljnjem besedilu: švicarski ETS). Za operacionalizacijo povezave med EU ETS in švicarskim ETS bo vzpostavljena neposredna povezava med evidenco transakcij Evropske unije (EUTL) registra Unije in švicarsko dopolnilno evidenco transakcij (SSTL) švicarskega registra, s čimer bo omogočen prenos pravic do emisije, izdanih v katerem koli ETS, med registroma (člen 3(2) Sporazuma). Za operacionalizacijo povezave med EU ETS in švicarskim ETS je bila leta 2020 vzpostavljena začasna rešitev. Od leta 2023 dalje bo povezava med registroma dveh sistemov trgovanja z emisijami postopoma postajala stalna povezava med registroma, za katero se pričakuje, da se bo začela izvajati najpozneje leta 2024 in bo omogočila delovanje povezanih trgov v smislu koristi od likvidnosti trga ter izvajanje transakcij med obema povezanima sistemoma na način, ki je enakovreden enemu trgu, sestavljenemu iz dveh sistemov, in ki udeležencem na trgu omogoča, da delujejo, kot da bi bili na enem trgu, ob upoštevanju samo posameznih regulativnih določb pogodbenic (Priloga II k Sporazumu).

Na podlagi člena 3(6) Sporazuma administrator švicarskega registra in centralni administrator Unije določita skupne delovne postopke, povezane s tehničnimi ali drugimi zadevami, potrebnimi za delovanje povezave, pri čemer upoštevata prednostne naloge domače zakonodaje. Skupni delovni postopki, ki jih določita administratorja, začnejo učinkovati, ko jih Skupni odbor sprejme s sklepom.

Skupni odbor je skupne delovne postopke sprejel s Sklepom št. 1/2020. Skupni odbor bo posodobljene skupne delovne postopke, navedene v tem dokumentu, sprejel s Sklepom št. 1/2024. V skladu s tem sklepom in zahtevami Skupnega odbora sta administrator švicarskega registra in centralni administrator Unije razvila dodatne tehnične smernice, ki jih bosta dodatno posodabljala, za operacionalizacijo povezave in zagotovitev stalnega prilagajanja teh smernic tehničnemu napredku in novim zahtevam v zvezi z varnostjo in zaščito povezave ter njenim uspešnim in učinkovitim delovanjem.

2.1. Obseg

Ta dokument predstavlja skupno stališče pogodbenic Sporazuma v zvezi z vzpostavitvijo postopkovne podlage za povezavo med registroma EU ETS in švicarskega ETS. V njem so opisane splošne postopkovne zahteve v zvezi z dejavnostmi, za operacionalizacijo povezave pa bo treba pripraviti nekatere dodatne tehnične smernice.

Za zagotovitev pravilnega delovanja povezave bodo za njeno nadaljnjo operacionalizacijo potrebne tehnične specifikacije. Na podlagi člena 3(7) Sporazuma so navedene zadeve podrobno opredeljene v dokumentu s tehničnimi standardi za povezavo (LTS), ki jih Skupni odbor ločeno sprejme s sklepom.

Cilj skupnih delovnih postopkov je zagotoviti, da se storitve IT, povezane z delovanjem povezave med registroma EU ETS in švicarskega ETS, izvajajo učinkovito in smotrno, zlasti v zvezi z izpolnjevanjem zahtevkov za storitve, reševanjem napak pri izvajanju storitve, odpravljanjem težav in izvajanjem rutinskih delovnih nalog v skladu z mednarodnimi standardi upravljanja storitev IT.

Za stalno povezavo med registroma bodo potrebni samo naslednji skupni delovni postopki, ki so vključeni v ta dokument:

— obvladovanje incidentov,

— odpravljanje težav,

— izpolnjevanje zahtevkov,

— upravljanje sprememb,

— upravljanje izdaj,

— obvladovanje varnostnih incidentov,

— upravljanje informacijske varnosti.

2.2. Naslovniki

Ciljna skupina teh skupnih delovnih postopkov sta podporni skupini registra EU in švicarskega registra.

3. PRISTOP IN STANDARDI

Za vse skupne delovne postopke se uporabljajo naslednja načela:

— EU in CH se strinjata, da bosta skupne delovne postopke opredelili na podlagi ITIL (knjižnice infrastrukture informacijske tehnologije, 4. različica). Prakse, ki jih določa ta standard, se ponovno uporabijo in prilagodijo posebnim potrebam, povezanim s stalno povezavo med registroma;

— komunikacija in usklajevanje, ki sta potrebna za izvajanje skupnih delovnih postopkov med pogodbenicama, potekata prek storitvenih centrov registra CH in EU. Naloge se vedno dodelijo znotraj ene od pogodbenic;

— v primeru nesoglasja o izvedbi skupnega delovnega postopka to skupaj analizirata in rešujeta oba storitvena centra; Če soglasja ni mogoče doseči, se iskanje skupne rešitve prenese na naslednjo raven;

| Ravni prenosa | EU | CH |
|---|---|---|
| Prva raven | Storitveni center EU | Storitveni center CH |
| Druga raven | Vodja dejavnosti EU | Vodja uporabe registra CH |
| Tretja raven | Skupni odbor (ki lahko prenese to odgovornost na podlagi člena 12(5) Sporazuma) | |
| Četrta raven | Skupni odbor, če tretja raven prenese odgovornost | |

— vsaka pogodbenica lahko določi postopke za delovanje svojega sistema registra ob upoštevanju zahtev in vmesnikov, povezanih s temi skupnimi delovnimi postopki;

— kot podpora pri izvajanju skupnih delovnih postopkov, zlasti postopkov za obvladovanje incidentov, odpravljanje težav in izpolnjevanje zahtevkov, ter pri komunikaciji med pogodbenicama se uporablja orodje za upravljanje storitev IT (ITSM);

— dovoljena je tudi izmenjava informacij po elektronski pošti;

— pogodbenici zagotavljata, da so zahteve glede informacijske varnosti izpolnjene v skladu z navodili za ravnanje.

4. OBVLADOVANJE INCIDENTOV

Cilj postopka obvladovanja incidentov je, da se po incidentu storitve IT čim prej povrnejo na običajno raven z minimalnimi motnjami poslovanja.

V okviru postopka obvladovanja incidentov bi bilo treba tudi voditi evidenco incidentov za namene poročanja, postopek pa povezati z drugimi postopki za spodbujanje nenehnega izboljševanja.

S splošnega vidika postopek obvladovanja incidentov vključuje naslednje dejavnosti:

— odkrivanje in evidentiranje incidentov,

— razvrščanje in začetna podpora,

— preiskava in diagnoza,

— reševanje in obnovitev,

— zaključek incidenta.

Postopek obvladovanja incidentov ves čas trajanja incidenta obsega naloge obravnavanja lastništva, spremljanja, sledenja in komuniciranja.

4.1. Odkrivanje in evidentiranje incidentov

Incident lahko odkrije podporna skupina s pomočjo orodij za samodejno spremljanje ali tehnično osebje, ki izvaja rutinski nadzor.

Odkriti incident je treba evidentirati in mu dodeliti edinstveni identifikator za ustrezno sledenje in spremljanje incidenta. Edinstveni identifikator incidenta je identifikator, ki ga v skupnem sistemu označevanja dodeli storitveni center pogodbenice (EU ali CH), ki je opozorila na incident, in ga je treba navesti v vsakem sporočilu, povezanem s tem incidentom.

Kontaktna točka za vse incidente bi moral biti storitveni center pogodbenice, ki je incident zabeležil.

4.2. Razvrščanje in začetna podpora

Namen razvrščanja incidentov je razumeti in opredeliti, na kateri sistem in/ali storitev je incident vplival in kako močno. Da bi bilo razvrščanje učinkovito, bi bilo treba incident že v prvem poskusu usmeriti k primernemu viru, da bi se pospešilo reševanje incidenta.

V fazi razvrščanja bi bilo treba incident kategorizirati in prednostno razvrstiti v skladu z njegovim vplivom in nujnostjo, da bi ga bilo mogoče obravnavati v času, ki ustreza prednostni razvrstitvi.

Če incident lahko vpliva na zaupnost ali celovitost občutljivih podatkov in/ali razpoložljivost sistema, se opredeli tudi kot varnostni incident in nato obravnava v skladu s postopkom, opredeljenim v poglavju „Obvladovanje varnostnih incidentov“ tega dokumenta.

Če je mogoče, storitveni center, ki je incident zabeležil, opravi začetno diagnozo. Pri tem preveri, ali je incident znana napaka. Če je, sta postopek reševanja ali alternativna rešitev že znana in dokumentirana.

Če storitveni center uspešno reši incident, ga na tej točki tudi dejansko zaključi, saj je glavni namen obvladovanja incidentov dosežen (tj. hitra obnovitev storitve za končnega uporabnika). Če ga ne reši, ga prenese na višjo raven ustrezni skupini za reševanje, ta pa opravi nadaljnjo preiskavo in diagnozo.

4.3. Preiskava in diagnoza

Postopek preiskave in diagnoze incidenta se uporabi, kadar storitveni center ne more rešiti incidenta z začetno diagnozo, zato ga prenese na ustrezno višjo raven. Prenos incidenta na višjo raven je v celoti del postopka preiskave in diagnoze.

Običajna praksa v fazi preiskave in diagnoze je poskus poustvarjanja incidenta v nadzorovanih pogojih. Pri preiskavi in diagnozi incidenta je pomembno razumeti pravilen vrstni red dogodkov, ki so pripeljali do incidenta.

S prenosom na višjo raven se prizna, da incidenta na trenutni ravni podpore ni mogoče rešiti in da ga je treba posredovati podporni skupini na višji ravni ali drugi pogodbenici. Prenos na višjo raven lahko poteka na dva načina: horizontalno (t. i. funkcionalni prenos) ali vertikalno (t. i. hierarhični prenos).

Odgovornost storitvenega centra, ki je evidentiral in odprl postopek reševanja incidenta, je, da se incident prenese na višjo raven k primernemu viru ter zagotovi sledenje splošnemu statusu in dodelitev naloge reševanja incidenta.

Odgovornost pogodbenice, ki ji je bil incident dodeljen, je, da zagotovi pravočasno izvedbo zahtevanih dejanj in povratne informacije svojemu storitvenemu centru.

4.4. Reševanje in obnovitev

Reševanje incidenta in obnovitev se izvedeta, ko se incident v celoti razume. Iskanje rešitve za incident pomeni, da je bilo ugotovljeno, kako rešiti težavo. Sama uporaba rešitve pomeni fazo obnovitve.

Ko primeren vir odpravi napako pri izvajanju storitve, se incident preusmeri nazaj na ustrezen storitveni center, ki je zabeležil incident in ki skupaj z osebo, ki je odprla postopek za reševanje incidenta, potrdi, da je bila napaka popravljena in da se incident lahko zaključi. Ugotovitve, pridobljene pri obdelavi incidenta, se evidentirajo za prihodnjo uporabo.

Obnovitev lahko izvede osebje za podporo IT ali pa se končnemu uporabniku zagotovijo navodila, ki jih mora upoštevati.

4.5. Zaključek incidenta

Zaključek je zadnji korak v postopku obvladovanja incidentov in se izvede kmalu po rešitvi incidenta.

Na kontrolnem seznamu dejanj, ki jih je treba opraviti v fazi zaključka, je poudarjeno naslednje:

— preverjanje začetne kategorije, ki je bila dodeljena incidentu,

— ustrezno zajemanje vseh informacij v zvezi z incidentom,

— ustrezno dokumentiranje incidenta in posodobitev baze znanja,

— ustrezno obveščanje vseh deležnikov, na katere je incident neposredno ali posredno vplival.

Incident se uradno zaključi, ko storitveni center izvede fazo zaključka incidenta in o tem obvesti drugo pogodbenico.

Ko je incident zaključen, se ne bo več ponovno odprl. Če se incident kmalu ponovi, se prvotni incident ne odpre ponovno, temveč se zabeleži nov incident.

Če incident izsledita storitvena centra EU in CH, je za zaključek incidenta odgovoren tisti storitveni center, ki je incident zabeležil.

5. ODPRAVLJANJE TEŽAV

Postopek odpravljanja težav bi bilo treba uporabiti za vsako ugotovljeno težavo, zaradi katere se ta postopek tudi sproži. Odpravljanje težav je osredotočeno na povečanje kakovosti in zmanjšanje števila nastalih incidentov. Težava lahko povzroči enega ali več incidentov. Ko se poroča o incidentu, je cilj obvladovanja incidentov čim hitreje obnoviti delovanje storitve, po možnosti tudi z alternativnimi rešitvami. Ko nastane težava, je cilj preiskati temeljni vzrok zanjo, da bi se opredelila sprememba, ki bo zagotovila, da se težava in z njo povezani incidenti ne bodo ponovili.

5.1. Opredelitev in evidentiranje težave

Odvisno od tega, katera pogodbenica je težavo zabeležila, bo kontaktna točka za zadeve, povezane s težavo, storitveni center EU ali CH.

Edinstveni identifikator težave je identifikator, ki se dodeli z orodjem za upravljanje storitev IT (ITSM). Navesti ga je treba v vsakem sporočilu, povezanem s to težavo.

Postopek odpravljanja težav lahko sproži incident ali se lahko kadar koli začne kot dejanje na lastno pobudo zaradi odpravljanja ugotovljenih napak v sistemu.

5.2. Prednostno razvrščanje težav

Težave se lahko tako kot incidenti kategorizirajo glede na njihovo resnost in prednost, da bi jim bilo mogoče lažje slediti, pri tem pa se upoštevata vpliv z njimi povezanih incidentov in pogostost njihovega pojavljanja.

5.3. Preiskava in diagnoza težav

Vsaka pogodbenica lahko opozori na težavo, naloga storitvenega centra pogodbenice, ki je odprla postopek za odpravljanje težav, pa je zabeležiti težavo, njeno reševanje dodeliti primernemu viru in slediti njenemu splošnemu statusu.

Skupina za reševanje, na katero je bila težava prenesena, je odgovorna za pravočasno obravnavo težave in komuniciranje s storitvenim centrom.

Obe pogodbenici morata na zahtevo zagotoviti izvedbo dodeljenih nalog in povratne informacije svojemu storitvenemu centru.

5.4. Reševanje

Skupina za reševanje, ki ji je bila težava dodeljena, je odgovorna za rešitev težave in zagotavljanje ustreznih informacij svojemu storitvenemu centru.

Ugotovitve, pridobljene pri obdelavi težave, se evidentirajo za prihodnjo uporabo.

5.5. Zaključek težave

Težava se uradno zaključi, ko se odpravi z izvedbo spremembe. Fazo zaključka težave izvede storitveni center, ki je težavo zabeležil in o tem obvestil storitveni center druge pogodbenice.

6. IZPOLNJEVANJE ZAHTEVKOV

Postopek izpolnjevanja zahtevkov je celovito upravljanje zahtevka za novo ali obstoječo storitev od trenutka, ko je evidentiran in odobren, do njegovega zaključka. Zahtevki za storitve so običajno majhni, vnaprej opredeljeni, ponavljajoči se, pogosti, vnaprej odobreni in postopkovni zahtevki.

Glavni koraki, ki jih je treba upoštevati, so opisani v nadaljevanju:

6.1. Vlaganje zahtevkov

Informacije v zvezi z zahtevkom za storitev se predložijo storitvenemu centru EU ali CH po elektronski pošti, telefonu ali z orodjem za upravljanje storitev IT (ITSM) oziroma po katerem koli drugem dogovorjenem komunikacijskem kanalu.

6.2. Evidentiranje in analiza zahtevkov

Kontaktna točka za vse zahtevke za storitve bi moral biti storitveni center EU ali CH, odvisno od tega, katera pogodbenica je vložila zahtevek za storitev. Ta storitveni center bo odgovoren za beleženje in primerno skrbno analizo zahtevka za storitev.

6.3. Odobritev zahtevkov

Zastopnik storitvenega centra pogodbenice, ki je vložila zahtevek za storitev, preveri, ali je potrebna kakršna koli odobritev druge pogodbenice, in če je, to odobritev pridobi. Če zahtevek za storitev ni odobren, storitveni center zabeležko posodobi in zapre.

6.4. Izpolnjevanje zahtevkov

Ta korak zajema učinkovito in uspešno obravnavo zahtevkov za storitve. Razlikovati je treba med naslednjimi primeri:

— izpolnjevanje zahtevka za storitev vpliva samo na eno pogodbenico. V tem primeru ta pogodbenica izdaja delovne naloge in usklajuje izvedbo.

— Izpolnjevanje zahtevka za storitev vpliva na EU in CH. V tem primeru vsak storitveni center izdaja delovne naloge na svojem področju odgovornosti. Obravnava za izpolnitev zahtevka za storitev se usklajuje med obema storitvenima centroma. Splošno odgovornost nosi tisti storitveni center, ki je prejel zahtevek za storitev in sprožil postopek za njegovo reševanje.

Ko je zahtevek za storitev izpolnjen, se mu mora dodeliti status rešenega zahtevka.

6.5. Prenos zahtevkov na višjo raven

Storitveni center lahko po potrebi prenese nerešeni zahtevek za storitev na višjo raven k primernemu viru (tretjo stran).

Zahtevki se prenesejo na višjo raven k ustreznim tretjim stranem, kar pomeni, da bo storitveni center EU moral prenos na švicarsko tretjo stran opraviti prek švicarskega storitvenega centra in obratno.

Tretja stran, na katero je bil zahtevek za storitev prenesen, je odgovorna za pravočasno obravnavo zahtevka za storitev in komuniciranje s storitvenim centrom, ki je prenesel zahtevek na višjo raven.

Storitveni center, ki je zabeležil zahtevek za storitev, je odgovoren za sledenje splošnemu statusu in dodelitev zahtevka za storitev.

6.6. Pregled izpolnjevanja zahtevkov

Preden se postopek zaključi, odgovorni storitveni center predloži dokumentacijo, povezano z zahtevkom za storitev, za končen nadzor kakovosti. Cilj je zagotoviti, da je zahtevek za storitev dejansko obdelan in da so zagotovljene dovolj podrobne informacije za opis celotnega poteka reševanja zahtevka. Poleg tega se ugotovitve, pridobljene pri obdelavi zahtevka, evidentirajo za prihodnjo uporabo.

6.7. Zaključek zahtevka

Če se strani, ki jim je bil zahtevek dodeljen, strinjajo, da je zahtevek za storitev izpolnjen, in če vlagatelj zahtevka meni, da je primer rešen, je naslednji status, ki se zahtevku določi, status „Zaključeno“.

Zahtevek za storitev je uradno zaključen, ko storitveni center, ki je zabeležil zahtevek za storitev, izvede fazo zaključka zahtevka in o tem obvesti storitveni center druge pogodbenice.

7. UPRAVLJANJE SPREMEMB

Cilj je zagotoviti uporabo standardiziranih metod in postopkov za učinkovito in hitro obravnavo vseh sprememb za nadzor infrastrukture IT, da bi se čim bolj zmanjšala število in vpliv vseh povezanih incidentov na storitev. Spremembe infrastrukture IT se lahko pojavijo reaktivno kot odziv na težave ali zunanje zahteve, npr. zakonodajne spremembe, ali proaktivno v prizadevanju za boljšo učinkovitost in uspešnost oziroma da bi se omogočile ali upoštevale poslovne pobude.

Postopek upravljanja sprememb vključuje različne korake, ki zajemajo vsako podrobnost v zvezi z zahtevkom za spremembe za prihodnje sledenje. Ti postopki zagotavljajo, da se sprememba pred uvedbo potrdi in preskusi. Postopek upravljanja izdaj zagotavlja uspešno uvedbo.

7.1. Zahtevek za spremembo

Zahtevek za spremembo se predloži skupini za upravljanje sprememb v potrditev in odobritev. Kontaktna točka za vse zahtevke za spremembe bi moral biti storitveni center EU ali CH, odvisno od tega, katera pogodbenica je vložila zahtevek. Ta storitveni center bo odgovoren za beleženje in primerno skrbno analizo zahtevka za spremembo.

Zahtevki za spremembe lahko izvirajo iz:

— incidenta, ki povzroči spremembo,

— obstoječe težave, ki povzroči spremembo,

— zahtevka končnega uporabnika za novo spremembo,

— spremembe zaradi tekočega vzdrževanja,

— zakonodajne spremembe.

7.2. Ocenjevanje in načrtovanje spremembe

V tej fazi se izvajajo dejavnosti ocenjevanja in načrtovanja spremembe. Vključuje dejavnosti prednostnega razvrščanja in načrtovanja za zmanjšanje tveganja in vpliva.

Če izvajanje postopka obravnave zahtevka za spremembo vpliva na EU in CH, pogodbenica, ki je zabeležila zahtevek za spremembo, preveri ocenjevanje in načrtovanje spremembe skupaj z drugo pogodbenico.

7.3. Odobritve sprememb

Vsak evidentirani zahtevek za spremembo je treba potrditi na ustrezni ravni prenosa.

7.4. Izvedba sprememb

Spremembe se izvedejo v okviru postopka upravljanja izdaj. Skupini za upravljanje izdaj obeh pogodbenic upoštevata lastne postopke, ki vključujejo načrtovanje in preskušanje. Ko je izvedba končana, se spremembe pregledajo. Za zagotovitev, da je vse izvedeno v skladu z načrtom, se postopek upravljanja spremembe redno pregleduje in po potrebi posodablja.

8. UPRAVLJANJE IZDAJ

Izdaja predstavlja eno ali več sprememb storitve IT, zbranih v načrtu izdaje, ki jo bo treba odobriti, pripraviti, zgraditi, preskusiti in uvesti. Izdaja lahko predstavlja odpravljanje programske napake, spremembo strojne opreme ali drugih sestavnih delov, spremembe programske opreme, posodobitve različic aplikacij, spremembe dokumentacije in/ali postopkov. Vsebina vsake izdaje se upravlja, preskuša in uvede kot ena entiteta.

Namen upravljanja izdaj je načrtovati, zgraditi, preskusiti in odobriti ter uresničiti zmogljivost za zagotovitev načrtovanih storitev, s katero bodo izpolnjene zahteve deležnikov in doseženi zastavljeni cilji. Merila za sprejemljivost vseh sprememb storitve se opredelijo in dokumentirajo med usklajevanjem zasnove ter zagotovijo skupinama za upravljanje izdaj.

Izdaja običajno vsebuje več rešitev težav in izboljšav storitve. Vsebuje zahtevano novo ali spremenjeno programsko opremo in vso novo ali spremenjeno strojno opremo, potrebno za izvedbo odobrenih sprememb.

8.1. Načrtovanje izdaje

Prvi korak v postopku vsebuje dodelitev odobrenih sprememb svežnjem izdaj ter opredelitev obsega in vsebine izdaj. Na podlagi teh informacij se v okviru načrtovanja izdaje pripravi časovni razpored priprave, preskušanja in uvedbe izdaje.

Pri načrtovanju bi bilo treba opredeliti:

— obseg in vsebino izdaje,

— oceno in profil tveganja za izdajo,

— stranke/uporabnike, na katere izdaja vpliva,

— skupino, odgovorno za izdajo,

— strategijo izročitve in uvedbe,

— vire za izdajo in njihovo uvedbo.

Pogodbenici se medsebojno obvestita o načrtovanih izdajah in obdobjih vzdrževanja. Če izdaja vpliva na EU in CH, obe usklajujeta načrtovanje in določita skupno obdobje vzdrževanja.

8.2. Priprava in preskus svežnja izdaje

Med pripravo in preskusom v okviru postopka upravljanja izdaje se določi pristop izvajanja izdaje ali svežnja izdaje ter vzdrževanja nadzorovanih okolij pred spremembo produkcije in preskušanja vseh sprememb v vseh izdanih okoljih.

Če izdaja vpliva na EU in CH, obe usklajujeta načrte izročitve in preskuse. To vključuje naslednje vidike:

— kako in kdaj bodo izročene enote izdaje in sestavni deli storitve,

— kakšen je potreben čas za izvedbo, kaj se zgodi v primeru zamude,

— kako slediti napredku izročitve in pridobiti potrditev,

— metriko za spremljanje in določanje uspeha pri uvedbi izdaje,

— skupne primere preskušanja ustreznih funkcij in sprememb.

Na koncu tega dela postopka so vsi zahtevani sestavni deli izdaje pripravljeni na fazo dejanske uvedbe.

8.3. Priprava na uvedbo

V okviru postopka priprave se zagotavlja, da so komunikacijski načrti pravilno opredeljeni, da so obvestila pripravljena za pošiljanje vsem deležnikom in končnim uporabnikom, na katere to vpliva, ter da je izdaja vključena v postopek upravljanja sprememb, s čimer se zagotovi, da se vse spremembe izvedejo nadzorovano in so odobrene v ustreznih forumih.

Če izdaja vpliva na EU in CH, obe usklajujeta naslednje dejavnosti:

— evidentiranje zahtevkov za spremembe za časovni razpored in pripravo uvedbe v produkcijskem okolju,

— pripravo načrta izvedbe,

— postopek povrnitve zaradi ponovne vzpostavitve prejšnjega stanja v primeru napake pri uvedbi,

— pošiljanje obvestil vsem zadevnim stranem,

— zahtevanje odobritve za izvedbo izdaje na ustrezni ravni prenosa.

8.4. Povrnitev izdaje

Če uvedba ni bila uspešno izvedena ali če je bilo pri preskušanju ugotovljeno, da ni bila uspešna ali da niso bila izpolnjena dogovorjena merila za sprejemljivost/kakovost, morata skupini za upravljanje izdaje obeh pogodbenic povrniti prejšnje stanje. Obvestiti je treba vse zadevne deležnike, vključno s končnimi uporabniki, na katere je to vplivalo/ki jim je bila izdaja namenjena. Postopek se lahko v čakanju na odobritev ponovno začne na kateri koli od prejšnjih ravni.

8.5. Pregled in zaključek izdaje

Pregled uvedbe bi moral vključevati naslednje dejavnosti:

— zajemanje povratnih informacij o zadovoljstvu stranke, uporabnika in dobavitelja storitve z uvedbo (zbiranje povratnih informacij in njihovo upoštevanje za nenehno izboljševanje storitve),

— pregled vseh meril kakovosti, ki niso bila izpolnjena,

— preverjanje, da so končane vse dejavnosti ter opravljene potrebne odprave napak in spremembe,

— zagotavljanje, da ob koncu postavitve ni nobenih težav, povezanih z zmožnostjo, virom, zmogljivostjo ali učinkovitostjo,

— preverjanje, da so stranka, končni uporabniki, izvajalci operativne podpore in druge zadevne strani dokumentirali in sprejeli vse težave, znane napake in alternativne rešitve,

— spremljanje incidentov in težav, ki nastanejo zaradi uvedbe (zagotavljanje zgodnje podpore operativnim skupinam, kadar se zaradi izdaje poveča obseg dela),

— posodabljanje podporne dokumentacije (tj. dokumentov s tehničnimi informacijami),

— uraden prenos uvedbe izdaje na operativne naloge storitve,

— dokumentiranje pridobljenih izkušenj,

— pridobivanje zbirnih dokumentov o izdaji pri izvajalskih skupinah,

— uraden zaključek izdaje po preverjanju dokumentacije, povezane z zahtevkom za spremembe.

9. OBVLADOVANJE VARNOSTNIH INCIDENTOV

Obvladovanje varnostnih incidentov je postopek za obravnavo varnostnih incidentov, da bi se omogočilo obveščanje vseh deležnikov, na katere bi incidenti lahko vplivali, o teh incidentih, ocenjevanje in prednostno razvrščanje incidentov ter odziv na incident za odpravo vseh dejanskih kršitev zaupnosti, razpoložljivosti ali celovitosti občutljivih informacijskih sredstev, suma teh kršitev ali potencialnih kršitev.

9.1. Kategorizacija incidentov v zvezi z informacijsko varnostjo

Za opredelitev možne kršitve zaupnosti, celovitosti ali razpoložljivosti katerih koli občutljivih informacij, evidentiranih v seznamu občutljivih informacij (SIL), se analizirajo vsi incidenti, ki vplivajo na povezavo med registrom Unije in švicarskim registrom.

V tem primeru se incident označi kot incident v zvezi z informacijsko varnostjo, nemudoma evidentira v orodju za upravljanje storitev IT (ITSM) ter obravnava kot tak.

9.2. Ravnanje v primeru incidentov v zvezi z informacijsko varnostjo

Odgovornost za varnostne incidente je na tretji ravni prenosa, za reševanje pa je pristojna posebna skupina za obvladovanje incidentov (IMT).

Skupina IMT je odgovorna za:

— izvedbo prve analize, kategorizacijo in oceno resnosti incidenta,

— usklajevanje ukrepov med vsemi zainteresiranimi stranmi, vključno s popolno dokumentacijo o analizi incidenta, sprejetimi odločitvami za obravnavo incidenta in katerimi koli možnimi opredeljenimi pomanjkljivostmi,

— odvisno od resnosti varnostnega incidenta, pravočasen prenos incidenta na primerno raven v vednost in/ali za sprejetje odločitve.

V postopku obvladovanja incidentov v zvezi z informacijsko varnostjo se vse informacije o incidentih razvrstijo na najvišjo raven občutljivosti informacij, nikakor pa ne nižje od OBČUTLJIVA: *ETS*.

V primeru preiskav, ki potekajo, in/ali pomanjkljivosti, ki bi jo bilo mogoče izkoristiti, se do njene odprave informacije označijo kot POSEBNA OBRAVNAVA: *ETS kritična*.

9.3. Opredelitev varnostnega incidenta

Na podlagi vrste varnostnega dogodka uradnik za informacijsko varnost določi ustrezne organizacije, ki se vključijo in so del skupine IMT.

9.4. Analiza varnostnega incidenta

Skupina IMT se za pregled incidenta poveže z vsemi vključenimi organizacijami in ustreznimi člani njihovih skupin, kakor je ustrezno. Med analizo se opredeli obseg izgube zaupnosti, celovitosti ali razpoložljivosti sredstva ter ocenijo posledice za vse organizacije, na katere je to vplivalo. Nato se opredelijo začetni in nadaljnji ukrepi za rešitev incidenta in obvladovanje njegovega vpliva, vključno z vplivom teh ukrepov na vir.

9.5. Ocenjevanje resnosti varnostnega incidenta, prenos na višjo raven in poročanje

Skupina IMT oceni resnost vseh novih varnostnih incidentov po njihovi opredelitvi kot varnostih incidentov in začne izvajati takojšnje potrebne ukrepe v skladu z resnostjo incidenta.

9.6. Poročanje o odzivu na varnostni incident

Skupina IMT v poročilo o odzivu na incident v zvezi z informacijsko varnostjo vključi rezultate zajezitve incidenta in obnovitve. Poročilo se tretji ravni reševanja pošlje po varni elektronski pošti ali z drugim medsebojno sprejetim sredstvom varnega komuniciranja.

Odgovorna pogodbenica pregleda rezultate zajezitve in obnovitve ter:

— ponovno vzpostavi povezavo med registroma v primeru predhodne prekinitve povezave,

— pošlje sporočila o incidentu skupinam registrov,

— zaključi incident.

Skupina IMT bi morala v poročilo o incidentu v zvezi z informacijsko varnostjo varno vključiti ustrezne podrobnosti, da bi zagotovila dosledno evidentiranje in komuniciranje ter omogočila hitro in ustrezno ukrepanje za zajezitev incidenta. Po zaključku postopka skupina IMT pravočasno pošlje končno poročilo o incidentu v zvezi z informacijsko varnostjo.

9.7. Spremljanje, krepitev zmogljivosti in nenehno izboljševanje

Skupina IMT bo zagotovila poročila o vseh varnostnih incidentih tretji ravni prenosa. Poročila bodo na tej ravni prenosa uporabljena za določitev:

— pomanjkljivosti v varnostnem nadzoru in/ali dejavnostih, ki jih je treba okrepiti,

— možne potrebe po okrepitvi tega postopka, da bi se izboljšala učinkovitost pri odzivanju na incidente,

— možnosti za usposabljanje in krepitev zmogljivosti za nadaljnjo krepitev odpornosti sistemov registra z vidika informacijske varnosti ter zmanjšanje tveganja prihodnjih incidentov in njihovega vpliva.

10. UPRAVLJANJE INFORMACIJSKE VARNOSTI

Namen upravljanja informacijske varnosti je zagotoviti zaupnost, celovitost in razpoložljivost zaupnih informacij, podatkov in storitev IT organizacije. Poleg tehničnih sestavnih delov, vključno z njihovo zasnovo in preskušanjem (glej LTS), so za izpolnjevanje varnostnih zahtev za stalno povezavo med registroma potrebni naslednji skupni delovni postopki.

10.1. Opredelitev občutljivih informacij

Občutljivost informacije se oceni tako, da se določi, kakšen vpliv na podjetje (npr. finančne izgube, poslabšanje podobe, kršitev prava …) bi lahko imela kršitev varnostnih predpisov, povezana s to informacijo.

Občutljiva informacijska sredstva se opredelijo na podlagi njihovega vpliva na povezavo.

Raven občutljivosti teh informacij se oceni v skladu z lestvico občutljivosti, ki se uporablja za to povezavo, in opredeli v oddelku „Ravnanje v primeru incidentov v zvezi z informacijsko varnostjo“ tega dokumenta.

10.2. Ravni občutljivosti informacijskih sredstev

Informacijska sredstva se ob opredelitvi razvrstijo na podlagi naslednjih pravil:

— če je opredeljena vsaj ena VISOKA raven zaupnosti, celovitosti ali razpoložljivosti, se sredstvo označi kot POSEBNA OBRAVNAVA: *ETS kritična*;

— če je opredeljena vsaj ena SREDNJA raven zaupnosti, celovitosti ali razpoložljivosti, se sredstvo označi kot OBČUTLJIVA: *ETS*;

— če je opredeljena samo NIZKA raven zaupnosti, celovitosti ali razpoložljivosti, se sredstvo označi kot oznaka EU: OBČUTLJIVA: *ETS skupno javno naročanje;* oznaka CH: OMEJENA: *ETS*.

10.3. Določitev lastnika informacijskih sredstev

Vsa informacijska sredstva bi morala imeti določenega lastnika. Informacijska sredstva sistema za trgovanje z emisijami, ki pripadajo EUTL in SSTL ali so povezana s povezavo med EUTL in SSTL, bi morala biti vključena v skupni seznam sredstev, ki ga vodita obe pogodbenici. Informacijska sredstva sistema za trgovanje z emisijami zunaj povezave med EUTL in SSTL bi morala biti vključena v seznam sredstev, ki ga vodi zadevna pogodbenica.

Pogodbenici se dogovorita o lastništvu vseh informacijskih sredstev, ki pripadajo EUTL in SSTL ali so povezana s povezavo med EUTL in SSTL. Lastnik informacijskega sredstva je odgovoren za oceno njegove občutljivosti.

Lastnik bi moral imeti primerne izkušnje glede na vrednost dodeljenih sredstev. O odgovornosti lastnika za sredstva in njegovi obveznosti ohranjanja zahtevane ravni zaupnosti, celovitosti in razpoložljivosti bi se bilo treba dogovoriti in ta dogovor formalizirati.

10.4. Evidentiranje občutljivih informacij

Vse občutljive informacije se evidentirajo v seznamu občutljivih informacij (SIL).

Kjer je to ustrezno, se upošteva združevanje občutljivih informacij, ki bi lahko povzročilo večji vpliv od vpliva ene same informacije, to pa se nato evidentira v seznam SIL (npr. sklop informacij, shranjenih v podatkovni zbirki sistema).

Seznam SIL se nenehno spreminja. Grožnje, ranljivosti, verjetnost ali posledice varnostnih incidentov, povezanih s sredstvi, se lahko spremenijo brez kakršnega koli namiga, v delovanje sistemov registra pa se lahko vnesejo nova sredstva.

Zato se seznam SIL redno pregleduje, vse nove informacije, opredeljene kot občutljive, pa se nemudoma evidentirajo v seznamu SIL.

Seznam SIL za vsak vnos vsebuje vsaj naslednje informacije:

— opis informacije,

— lastnika informacije,

— raven občutljivosti,

— oznako, če informacije vključujejo osebne podatke,

— dodatne informacije, če se zahtevajo.

10.5. Ravnanje z občutljivimi informacijami

Kadar se občutljive informacije obdelujejo zunaj povezave med registrom Unije in švicarskim registrom, se z njimi ravna v skladu z navodili za ravnanje.

Z občutljivimi informacijami, ki se obdelujejo s povezavo med registrom Unije in švicarskim registrom, se ravna v skladu z varnostnimi zahtevami pogodbenic.

10.6. Upravljanje dostopa

Namen upravljanja dostopa je dodeliti pooblaščenim uporabnikom pravico do uporabe storitve in obenem preprečiti dostop nepooblaščenim uporabnikom. Upravljanje dostopa se včasih imenuje tudi „upravljanje pravic“ ali „upravljanje identitete“.

Za stalno povezavo med registroma in njeno operacionalizacijo morata imeti obe pogodbenici dostop do naslednjih sestavnih delov:

— okolja Wiki: sodelovalno okolje za izmenjavo splošnih informacij, kot je načrtovanje izdaje,

— orodja za upravljanje storitve IT (ITSM) za obvladovanje incidentov in odpravljanje težav (glej poglavje 3 „Pristopi in standardi“),

— sistema za izmenjavo sporočil: vsaka pogodbenica zagotovi varen sistem za prenos za izmenjavo sporočil, ki vsebujejo podatke o transakciji.

Administrator švicarskega registra in centralni administrator Unije zagotovita, da so dostopi posodobljeni in delujejo kot kontaktne točke za pogodbenici za dejavnosti upravljanja dostopa. Zahtevki za dostop se obravnavajo v skladu s postopki izpolnjevanja zahtevkov.

10.7. Upravljanje potrdil/ključev

Vsaka pogodbenica je odgovorna za svoje upravljanje potrdila/ključa (ustvarjanje, evidentiranje, hramba, namestitev, uporaba, obnovitev, preklic, varnostno kopijo in obnovitev potrdil/ključev). Kot je pojasnjeno v tehničnih standardih za povezavo (LTS), se uporabljajo samo digitalna potrdila, ki jih izda overitelj potrdil, ki mu zaupata obe pogodbenici. Pri ravnanju s potrdili/ključi in njihovi hrambi je treba upoštevati določbe iz navodil za ravnanje.

Vsak preklic in/ali obnovitev potrdil in ključev usklajujeta obe pogodbenici. Izvaja se v skladu s postopki izpolnjevanja zahtevkov.

Administrator švicarskega registra in centralni administrator Unije si bosta izmenjevala potrdila/ključe po varnih komunikacijskih sredstvih v skladu z določbami iz navodil za ravnanje.

Vsako preverjanje potrdil/ključev v katerem koli sredstvu med pogodbenicama se opravi po drugi poti.

*PRILOGA III*

**TEHNIČNI STANDARDI ZA POVEZAVO NA PODLAGI ČLENA 3(7) SPORAZUMA MED EVROPSKO UNIJO IN ŠVICARSKO KONFEDERACIJO O POVEZAVI NJUNIH SISTEMOV TRGOVANJA Z EMISIJAMI TOPLOGREDNIH PLINOV**

**Standardi za stalno povezavo med registroma**

Kazalo


| | | |
|---|---|---|
| 1. | GLOSAR | 23 |
| 2. | UVOD | 25 |
| 2.1. | Obseg | 25 |
| 2.2. | Naslovniki | 25 |
| 3. | SPLOŠNE DOLOČBE | 25 |
| 3.1. | Zgradba komunikacijske vezi | 25 |
| 3.1.1. | Izmenjava sporočil | 26 |
| 3.1.2. | Sporočilo XML – visokoravenski opis | 26 |
| 3.1.3. | Zajemna okna | 26 |
| 3.1.4. | Promet sporočil o transakcijah | 27 |
| 3.2. | Varnost prenosa podatkov | 29 |
| 3.2.1. | Požarni zid in medomrežna povezava | 29 |
| 3.2.2. | Navidezno zasebno omrežje (VPN) | 29 |
| 3.2.3. | Izvajanje IPSec | 29 |
| 3.2.4. | Varen protokol za prenos za izmenjavo sporočil | 30 |
| 3.2.5. | Šifriranje in podpis XML | 30 |
| 3.2.6. | Kriptografski ključi | 30 |
| 3.3. | Seznam funkcij znotraj povezave | 30 |
| 3.3.1. | Poslovne transakcije | 30 |
| 3.3.2. | Protokol usklajevanja | 31 |
| 3.3.3. | Poskusno sporočilo | 31 |
| 3.4. | Zahteve glede zapisovanja podatkov | 31 |
| 3.5. | Operativne zahteve | 32 |
| 4. | DOLOČBE GLEDE RAZPOLOŽLJIVOSTI | 32 |
| 4.1. | Načrt razpoložljivosti komunikacij | 32 |
| 4.2. | Načrt inicializacije, komunikacije, ponovne aktivacije in testiranja | 33 |
| 4.2.1. | Interni testi infrastrukture IKT | 33 |
| 4.2.2. | Testi komunikacije | 33 |
| 4.2.3. | Testi celotnega sistema (med koncema) | 33 |
| 4.2.4. | Testi varnosti | 33 |
| 4.3. | Okolja sprejemanja/testiranja | 34 |
| 5. | DOLOČBE O ZAUPNOSTI IN CELOVITOSTI | 34 |
| 5.1. | Infrastruktura za testiranje varnosti | 34 |
| 5.2. | Določbe o prekinitvi povezave in ponovni aktivaciji | 35 |

5.3. Določbe o kršitvah varnostnih predpisov . . . . . 35
5.4. Smernice za testiranje varnosti . . . . . 35
5.4.1. Programska oprema . . . . . 35
5.4.2. Infrastruktura . . . . . 36
5.5. Določbe o oceni tveganja . . . . . 36

1. GLOSAR

**Preglednica 1-1 Poslovne kratice in opredelitve pojmov**

| Kratica/pojem | Opredelitev |
|---|---|
| Pravica | Pravica do emisij ene tone ekvivalenta ogljikovega dioksida v določenem obdobju, ki velja samo za izpolnjevanje zahtev v okviru ETS katerega koli subjekta. |
| CH | Švicarska konfederacija. |
| CHU | Vrsta švicarskih splošnih pravic, imenovanih tudi CHU2 (glede na ciljno obdobje 2 Kjotskega protokola), ki jih izda CH. |
| CHUA | Švicarske pravice za letalstvo. |
| COP | Skupni delovni postopki. Skupaj razviti postopki za operacionalizacijo povezave med EU ETS in švicarskim ETS. |
| ETR | Register za trgovanje z emisijami. |
| ETS | Sistem za trgovanje z emisijami. |
| EU | Evropska unija. |
| EUA | Splošne pravice EU. |
| EUAA | Pravice za letalstvo EU. |
| EUCR | Konsolidirani register Evropske unije. |
| EUTL | Evidenca transakcij Evropske unije. |
| Register | Sistem obračunavanja za pravice, izdane v ETS, s katerim se vodi evidenca o lastništvu pravic na elektronskih računih. |
| SSTL | Švicarska dopolnilna evidenca transakcij. |
| Transakcija | Postopek v registru, ki vključuje prenos pravice z enega računa na drugega. |
| Sistem evidence transakcij | Evidenca transakcij vsebuje zapis vsake predlagane transakcije, poslane iz enega registra v drugega. |

**Preglednica 1-2 Tehnične kratice in opredelitve pojmov**

| Kratica | Opredelitev |
|---|---|
| Asimetrična kriptografija | Uporablja javne in zasebne ključe za šifriranje in dešifriranje podatkov. |
| Overitelj potrdil | Subjekt, ki izdaja digitalna potrdila. |
| Kriptografski ključ | Del informacije, ki determinira funkcionalni izhod kriptografskega algoritma. |
| Dešifriranje | Postopek, ki poteka v obratni smeri od šifriranja. |
| Digitalni podpis | Matematična tehnika, ki se uporablja za potrditev avtentičnosti in celovitosti sporočila, programske opreme ali digitalnega dokumenta. |
| Šifriranje | Postopek pretvarjanja informacij ali podatkov v šifro, zlasti za preprečevanje nepooblaščenega dostopa. |
| Zajem datotek | Postopek branja datoteke. |
| Požarni zid | Izdelek s področja omrežne varnosti ali programska oprema, ki spremlja in nadzoruje vhodni in izhodni omrežni promet na podlagi vnaprej določenih pravil. |
| Spremljanje „utripa“ | Periodičen signal, ki ga ustvari in spremlja strojna ali programska oprema, da označi normalno delovanje ali sinhronizira druge dele računalniškega sistema. |
| IPSec | Varnostni protokol za zaščito komunikacije. Nabor omrežnih protokolov za avtentikacijo in šifriranje podatkovnih paketov, ki zagotavlja varno šifrirano komunikacijo med dvema računalnikoma prek omrežja internetnega protokola. |
| Penetracijsko testiranje | Testiranje računalniškega sistema, omrežja ali spletne aplikacije, pri katerem se iščejo varnostne ranljivosti, ki bi jih napadalci lahko izkoristili. |
| Postopek usklajevanja | Zagotavljanje usklajenosti dveh sklopov zapisov. |
| VPN | Navidezno zasebno omrežje. |
| XML | Razširljivi označevalni jezik. Načrtovalcem omogoča, da ustvarijo svoje prilagojene značke, ki omogočajo opredelitev, prenos, potrditev in tolmačenje podatkov med aplikacijami in organizacijami. |

## 2. UVOD

Sporazum med Evropsko unijo in Švicarsko konfederacijo o povezavi njunih sistemov trgovanja z emisijami toplogrednih plinov z dne 23. novembra 2017 (v nadaljnjem besedilu: Sporazum) določa medsebojno priznavanje pravic do emisije, ki se lahko uporabljajo za skladnost v okviru sistema Evropske unije za trgovanje z emisijami (v nadaljnjem besedilu: EU ETS) ali sistema Švice za trgovanje z emisijami (v nadaljnjem besedilu: švicarski ETS). Za operacionalizacijo povezave med EU ETS in švicarskim ETS bo vzpostavljena neposredna povezava med evidenco transakcij Evropske unije (EUTL) registra Unije in švicarsko dopolnilno evidenco transakcij (SSTL) švicarskega registra, s čimer bo omogočen prenos pravic do emisije, izdanih v katerem koli ETS, med registroma (člen 3(2) Sporazuma). Za operacionalizacijo povezave med EU ETS in švicarskim ETS je bila leta 2020 vzpostavljena začasna rešitev. Od leta 2023 dalje bo povezava med registroma dveh sistemov trgovanja z emisijami postopoma postajala stalna povezava med registroma, za katero se pričakuje, da se bo začela izvajati najpozneje leta 2024 in bo omogočila delovanje povezanih trgov v smislu koristi od likvidnosti trga ter izvajanje transakcij med obema povezanima sistemoma na način, ki je enakovreden enemu trgu, sestavljenemu iz dveh sistemov, in ki udeležencem na trgu omogoča, da delujejo, kot da bi bili na enem trgu, ob upoštevanju samo posameznih regulativnih določb pogodbenic (Priloga II k Sporazumu).

Na podlagi člena 3(7) Sporazuma administrator švicarskega registra in centralni administrator registra Unije pripravita tehnične standarde za povezavo na podlagi načel iz Priloge II k Sporazumu, v kateri so navedene podrobne zahteve za vzpostavitev trdne in varne povezave med SSTL in EUTL. Tehnični standardi za povezavo, ki jih oblikujeta administratorja, začnejo učinkovati, ko jih Skupni odbor sprejme s sklepom.

Skupni odbor je tehnične standarde za povezavo sprejel s Sklepom št. 2/2020. Skupni odbor bo posodobljene tehnične standarde za povezavo, navedene v tem dokumentu, sprejel s Sklepom št. 1/2024. V skladu s tem sklepom in zahtevami Skupnega odbora sta administrator švicarskega registra in centralni administrator Unije razvila dodatne tehnične smernice, ki jih bosta dodatno posodabljala, za operacionalizacijo povezave zagotovitev stalnega prilagajanja teh smernic tehničnemu napredku in novim zahtevam v zvezi z varnostjo in zaščito povezave ter njenim uspešnim in učinkovitim delovanjem.

### 2.1. Obseg

Ta dokument predstavlja skupno stališče pogodbenic Sporazuma v zvezi z vzpostavitvijo tehnične podlage za povezavo med registroma EU ETS in švicarskega ETS. V njem je opisano izhodišče za tehnične specifikacije z vidika zahtev, povezanih z zgradbo, storitvami in varnostjo, za operacionalizacijo povezave pa bo treba pripraviti nekatere dodatne podrobne smernice.

Za zagotovitev pravilnega delovanja povezave bo treba za nadaljnjo operacionalizacijo povezave določiti procese in postopke. Na podlagi člena 3(6) Sporazuma so navedene zadeve podrobno opredeljene v ločenem dokumentu o skupnih delovnih postopkih, ki bo sprejet ločeno s sklepom Skupnega odbora.

### 2.2. Naslovniki

Ta dokument je naslovljen na administratorja švicarskega registra in centralnega administratorja registra Unije.

## 3. SPLOŠNE DOLOČBE

### 3.1. Zgradba komunikacijske vezi

Namen tega oddelka je zagotoviti opis splošne zgradbe operacionalizacije povezave med EU ETS in švicarskim ETS ter različnih sestavnih delov, ki so vanjo vključeni.

Ker je varnost ključni del opredelitve zgradbe povezave med registroma, se šteje, da imajo vsi ukrepi trdno zgradbo. Za stalno povezavo med registroma se uporablja mehanizem za izmenjavo datotek, pri čemer se izvaja varna povezava z zračnim zidom.

Tehnična rešitev uporablja:

— protokol za prenos za varno izmenjavo sporočil;

— sporočila XML;

— digitalni podpis in šifriranje XML;

— VPN.

3.1.1. Izmenjava sporočil

Komunikacija med registrom Unije in švicarskim registrom temelji na mehanizmu za izmenjavo sporočil po varnih kanalih. Vsak konec se zanaša na svoj lasten repozitorij prejetih sporočil.

Pogodbenici vodita evidenco prejetih sporočil, vključno s podrobnostmi o obdelavi.

Napake ali nepričakovano stanje je treba sporočiti v obliki opozoril, člani podpornih skupin pa bi morali vzpostaviti osebni stik.

| |
|---|
| Napake in nepričakovani dogodki se obravnavajo ob upoštevanju delovnih postopkov, določenih v postopku obvladovanja incidentov, ki je del skupnih delovnih postopkov. |

3.1.2. Sporočilo XML – visokoravenski opis

Sporočilo XML vsebuje eno od naslednjega:

— enega ali več zahtevkov za transakcijo in/ali enega ali več odgovorov v zvezi s transakcijo;

— eno dejavnost/odgovor, povezan z usklajevanjem;

— eno testno sporočilo.

Vsako sporočilo vsebuje glavo, v kateri sta navedena:

— izvorni ETS;

— zaporedna številka.

3.1.3. Zajemna okna

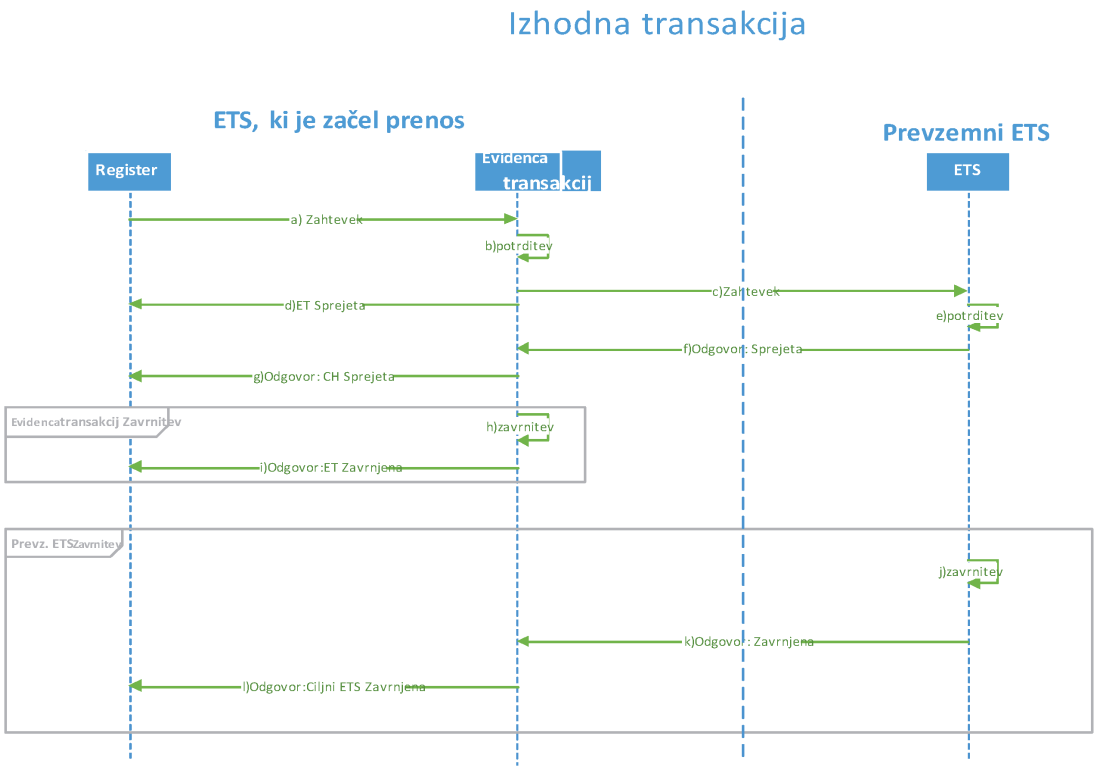
Stalna povezava med registroma temelji na vnaprej določenih zajemnih oknih, ki jim sledi sklop poimenovanih dogodkov. Zahtevki za transakcije, prejeti prek povezave, se bodo združevali samo v skladu z vnaprej določenimi intervali. Zajemna okna vključejo tehnično potrjevanje izhodnih in vhodnih transakcij. Poleg tega se usklajevanja lahko izvajajo vsak dan in se lahko sprožijo ročno.

| |
|---|
| Spremembe pogostosti in/ali časovne razporeditve katerih koli od teh dogodkov se bodo obravnavale ob upoštevanju delovnih postopkov, določenih v postopku izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov. |

3.1.4. Promet sporočil o transakcijah

Izhodne transakcije

Ta del obravnava vidik ETS, ki je začel prenos. Zadevni promet je prikazan na naslednjem diagramu zaporedja:




Glavni promet prikazuje naslednje korake (kot na zgornji sliki):

(a) pri ETS, ki je začel prenos, se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno);

(b) evidenca transakcij potrdi zahtevek za transakcijo;

(c) zahtevek za transakcijo se pošlje v ciljni ETS;

(d) odgovor o sprejetju se pošlje v register izvornega ETS;

(e) ciljni ETS potrdi zahtevek za transakcijo;

(f) ciljni ETS pošlje odgovor o sprejetju nazaj v evidenco transakcij izvornega ETS;

(g) evidenca transakcij pošlje odgovor o sprejetju v register.

Alternativni promet „Zavrnitev evidence transakcij“ (kot na zgornji sliki, začenši s točko (a) v glavnem prometu):

(a) v izvornem sistemu se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno);

(b) evidenca transakcij ne potrdi zahtevka;

(c) sporočilo o zavrnitvi se pošlje v izvorni register.

Alternativni promet „Zavrnitev ETS“ (kot na zgornji sliki, začenši s točko (d) v glavnem prometu):

(a) v izvornem ETS se zahtevek za transakcijo pošlje iz registra v evidenco transakcij, ko pretečejo vsi poslovni roki (24-urni rok, kjer je primerno);

(b) evidenca transakcij potrdi transakcijo;

(c) zahtevek za transakcijo se pošlje v ciljni ETS;

(d) sporočilo o sprejetju se pošlje v register izvornega ETS;

(e) evidenca transakcij prevzemnega ETS ne potrdi transakcije;

(f) prevzemni ETS pošlje odgovor o zavrnitvi v evidenco transakcij ETS, ki je začel prenos;

(g) evidenca transakcij pošlje zavrnitev v register.

Vhodne transakcije

Ta del obravnava vidik prevzemnega ETS. Zadevni promet je prikazan na naslednjem diagramu zaporedja:

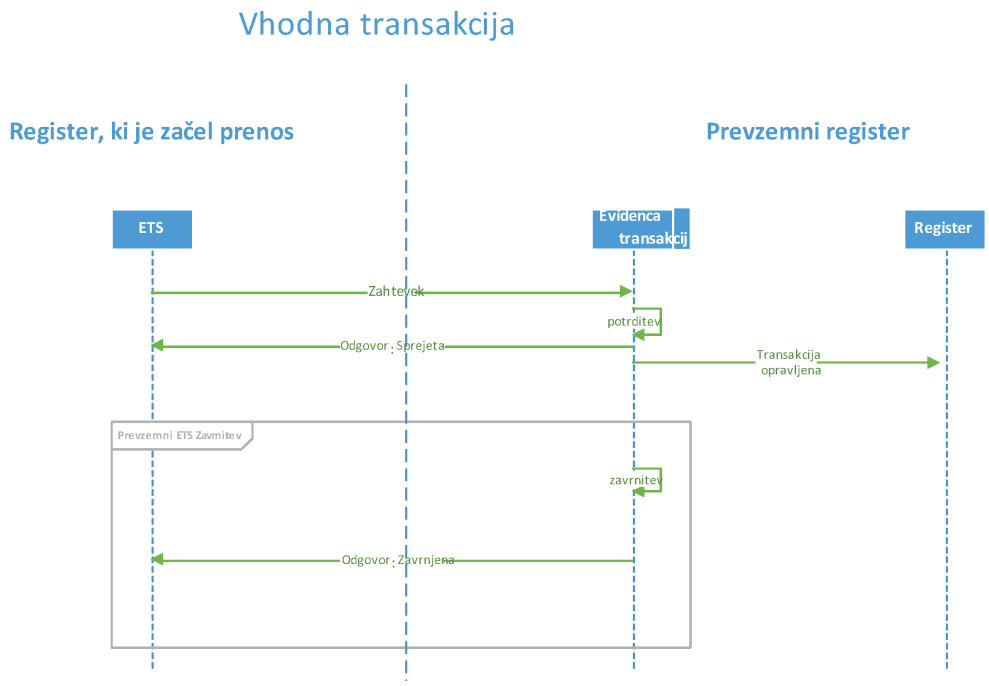



Diagram prikazuje naslednje:

(1) kadar evidenca transakcij prevzemnega ETS potrdi zahtevek, pošlje sporočilo o sprejetju v ETS, ki je začel prenos, in sporočilo o „opravljeni transakciji“ v register prevzemnega ETS;

(2) kadar prevzemna evidenca transakcij zavrne vhodni zahtevek za transakcijo, se ta ne pošlje v register prevzemnega ETS.

Protokol

Ciklus sporočil o transakciji vključuje samo dve sporočili:

— predlog za transakcijo – ETS, ki je začel prenos à prevzemni ETS;

— odgovor za transakcijo – prevzemni ETS à ETS, ki je začel prenos: sprejeta ali zavrnjena (vključno z razlogi za zavrnitev).

  — Sprejeta: transakcija je opravljena.

  — Zavrnjena: transakcija je prekinjena.

Stanje transakcije

— Stanje transakcije v ETS, ki izvaja prenos, se nastavi na „predlagana“, ko se zahtevek pošlje.

— Stanje transakcije v prevzemnem ETS se nastavi na „predlagana“, ko je zahtevek prejet in ko poteka njegova obdelava.

— Stanje transakcije v prevzemnem ETS se nastavi na „opravljena“/„prekinjena“, ko se predlog obdela. Prevzemni ETS nato pošlje ustrezno sporočilo o sprejetju/zavrnitvi.

— Stanje transakcije v ETS, ki je začel prenos, se nastavi na opravljena/prekinjena, ko je sporočilo o sprejetju/zavrnitvi prejeto in obdelano.

— Če ni bil prejet noben odgovor, se stanje transakcije v ETS, ki je začel prenos, ohrani v obliki predloga.

— Stanje transakcije v prevzemnem ETS se nastavi na „prekinjena“, če se katera koli predlagana transakcija ohrani v stanju „predlagana“ za več kot 30 minut.

| |
|---|
| Incidenti, povezani s transakcijami, se bodo obravnavali ob upoštevanju delovnih postopkov, določenih v postopku obvladovanja incidentov, ki je del skupnih delovnih postopkov. |

3.2. Varnost prenosa podatkov

Varnost podatkov, ki se prenašajo, se zagotovi na štirih ravneh:

(1) nadzor nad dostopom do omrežja: požarni zid in plast medomrežne povezave;

(2) šifriranje na ravni prenosa: VPN;

(3) šifriranje na ravni seje: varen protokol za prenos za izmenjavo sporočil;

(4) šifriranje na ravni aplikacije: šifriranje in podpis vsebine XML.

3.2.1. Požarni zid in medomrežna povezava

Vzpostavi se povezava v omrežju, zaščitenem s strojnim požarnim zidom. Požarni zid je konfiguriran na podlagi pravil tako, da se v strežnik VPN lahko povežejo samo „registrirani“ odjemalci.

3.2.2. Navidezno zasebno omrežje (VPN)

Vse komunikacije med pogodbenicama so zaščitene s tehnologijo navideznega zasebnega omrežja (VPN). Tehnologije VPN zagotavljajo možnost „tuneliranja“ skozi omrežje, kot je internet, ki pelje od ene točke do druge, pri čemer so zaščitene vse komunikacije. Pred vzpostavljanjem tunela VPN se izda digitalno potrdilo potencialni končni točki odjemalca, s katerim odjemalec lahko zagotovi dokazilo o identiteti med pogajanjem o povezavi. Vsaka pogodbenica je odgovorna za namestitev potrdila v svojo končno točko VPN. Strežnik VPN na vsakem koncu bo imel z digitalnim potrdilom dostop do centralnega overitelja zaradi pogajanja o avtentikacijskih poverilnicah. Med vzpostavljanjem tunela poteka pogajanje o šifriranju, s čimer se zagotovi zaščita vseh komunikacij, ki potekajo po tunelu.

Konfigurirajo se končne točke odjemalcev v VPN, da tunel VPN ohrani za stalno, s tem pa omogoči, da med pogodbenicama ves čas poteka zanesljiva, dvosmerna komunikacija v realnem času.

Evropska unija na splošno uporablja varne vseevropske telematske storitve med upravami (STESTA) kot zasebno omrežje, ki temelji na IP. Zato je to omrežje primerno tudi za stalno povezavo med registroma.

3.2.3. Izvajanje IPSec

Uporaba protokola IPSec za vzpostavitev infrastrukture VPN od spletnega mesta do spletnega mesta bo omogočila avtentikacijo od spletne strani do spletne strani, celovitost podatkov in šifriranje podatkov. Konfiguracije VPN IPSec omogočajo pravilno avtentikacijo med dvema končnima točkama v povezavi VPN. Pogodbenici ugotovita istovetnost in opravita avtentikacijo oddaljenega odjemalca prek povezave IPSec z digitalnim potrdilom overitelja potrdil, ki ga priznava nasprotna končna točka.

IPSec zagotavlja tudi celovitost vseh komunikacij, ki potekajo skozi tunel VPN. Podatkovni paketi so razpršeni in podpisani z avtentikacijsko informacijo, ki jo določi VPN. Zaupnost podatkov se prav tako zagotovi z omogočanjem šifriranja z IPSec.

3.2.4. Varen protokol za prenos za izmenjavo sporočil

Stalna povezava med registroma je odvisna od več plasti šifriranja za varno izmenjavo podatkov med pogodbenicama. Oba sistema in njuni različni okolji so medsebojno povezani na ravni omrežja s tuneli VPN. Na ravni aplikacije se datoteke prenašajo s pomočjo protokola za prenos za varno izmenjavo sporočil na ravni seje.

3.2.5. Šifriranje in podpis XML

Podpisovanje in šifriranje v datotekah XML poteka na dveh ravneh. Vsak zahtevek za transakcijo, odgovor v zvezi s transakcijo in sporočilo o usklajevanju se digitalno podpiše.

V drugem koraku se šifrira vsak podrejeni element elementa „sporočila“.

Poleg tega se v tretjem koraku za zagotovitev celovitosti in preprečevanja izpodbijanja celotnega sporočila digitalno podpiše korenski element sporočila. S tem se zagotovi visoka raven zaščite vgrajenih podatkov XML. Pri tehničnem izvajanju se upoštevajo standardi Konzorcija za svetovni splet.

Da bi se sporočilo dešifriralo in preverilo, se izvede postopek, ki poteka v obratni smeri.

3.2.6. Kriptografski ključi

Za šifriranje in podpisovanje se uporablja kriptografija javnih ključev.

V posebnem primeru IPSec se uporabi digitalno potrdilo, ki ga izda overitelj potrdil, ki mu zaupata obe pogodbenici. Ta overitelj potrdil preveri identiteto imetnika certifikata in izda potrdila, ki se uporabljajo za pozitivno identifikacijo organizacije in vzpostavitev varnih kanalov za podatkovne komunikacije med pogodbenicama.

| |
|---|
| Za podpisovanje in šifriranje komunikacijskih kanalov in podatkovnih datotek se uporabljajo kriptografski ključi. Pogodbenici digitalno izmenjujeta javna potrdila prek varnih kanalov in jih preverjata po drugi poti. Ta postopek je sestavni del postopka upravljanja informacijske varnosti, ki je del skupnih delovnih postopkov. |

3.3. Seznam funkcij znotraj povezave

Povezava določa sistem prenosa za niz funkcij, s katerimi se izvajajo poslovni postopki, ki izhajajo iz Sporazuma. Vključuje tudi specifikacijo za postopek usklajevanja in testna sporočila, ki bodo omogočili izvajanje spremljanja „utripa“.

3.3.1. Poslovne transakcije

Povezava s poslovnega vidika predvideva štiri (4) vrste zahtevkov za transakcije:

— zunanji prenos:

  — po začetku veljavnosti povezave med ETS so pravice EU in CH med pogodbenicama zamenljive in s tem tudi v celoti prenosljive;

  — v prenos prek povezave sta vključena račun, ki je začel prenos, v enem ETS in prevzemni račun v drugem ETS;

  — prenos lahko vključuje kakršno koli količino štirih (4) vrst pravic:

    — švicarskih splošnih pravic (CHU),

    — švicarskih pravic za letalstvo (CHUA),

    — splošnih pravic EU (EUA),

    — pravic za letalstvo EU (EUAA);

— mednarodna dodelitev:

  operaterji zrakoplovov, ki jih upravlja en ETS z obveznostmi do drugega ETS in ki so upravičeni do brezplačnih pravic iz navedenega drugega ETS, prejmejo od drugega ETS brezplačne pravice za letalstvo v okviru transakcije za mednarodno dodelitev;

— razveljavitev mednarodne dodelitve:

ta transakcija se izvede, če je treba brezplačne pravice, ki jih je drug ETS dodelil imetniškemu računu operaterja zrakoplova, v celoti razveljaviti;

— vračilo prevelikega števila dodeljenih pravic:

podobno razveljavitvi, vendar če dodelitve ni treba v celoti zavrniti, temveč le vrniti odvečno število dodeljenih pravic v ETS, iz katerega se opravi dodelitev.

3.3.2. Protokol usklajevanja

Usklajevanja se izvajajo po zaprtju oken za zajemanje, potrjevanje in obdelavo sporočil.

Usklajevanja so sestavni del ukrepov za zagotavljanje varnosti in skladnosti znotraj povezave. Pogodbenici sprejmeta točno časovno razporeditev usklajevanja, preden pripravita kakršen koli časovni načrt. Dnevno načrtovano usklajevanje se lahko izvede, če se tako dogovorita obe pogodbenici. Po vsakem postopku zajemanja se bo opravilo vsaj eno načrtovano usklajevanje.

V vsakem primeru lahko katera koli pogodbenica temu sproži postopek ročnega usklajevanja.

| |
|---|
| Spremembe časovne razporeditve in pogostosti načrtovanega usklajevanja se bodo obravnavale ob upoštevanju delovnih postopkov, določenih v postopku izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov. |

3.3.3. Poskusno sporočilo

Namen testnega sporočila je testirati komunikacijo med koncema. Sporočilo bo vsebovalo podatke, ki ga bodo opredelili kot testno sporočilo, nanj pa se odgovori, ko je prejeto na drugem koncu.

3.4. Zahteve glede zapisovanja podatkov

V podporo potrebi obeh pogodbenic po ohranitvi točnih in doslednih informacij ter za zagotovitev orodij, ki se uporabljajo v postopku usklajevanja za odpravo neskladnosti, pogodbenici vodita štiri (4) vrste evidenc podatkov:

— evidence transakcij;

— evidence usklajevanja;

— arhiv sporočil;

— evidence notranjih revizij.

Vsi podatki v teh evidencah se hranijo najmanj tri (3) mesece za odpravljanje težav, njihova nadaljnja hramba na vsakem koncu za revizijo pa je odvisna od veljavne zakonodaje. Zapisi, starejši od treh (3) mesecev, se lahko arhivirajo na varni lokaciji v neodvisnem sistemu IT, dokler se lahko v razumnem obdobju prikličejo ali se lahko do njih v razumnem obdobju dostopa.

Evidence transakcij

Oba podrejena sistema EUTL in SSTL sta izvajanje evidenc transakcij.

Natančneje, v evidencah transakcij se hranijo zapisi o vsaki predlagani transakciji, poslani v drugi ETS. Vsak zapis vsebuje vsa polja vsebine transakcije in poznejši rezultat transakcije (odgovor prevzemnega ETS). V evidencah transakcij se hranijo tudi zapisi v zvezi z vhodnimi transakcijami in odgovor, poslan izvornemu ETS.

Evidence usklajevanja

Evidenca usklajevanja vsebuje zapis o vseh sporočilih o usklajevanju, ki sta si jih izmenjali pogodbenici, vključno z identifikacijsko oznako usklajevanja, časovnim žigom in rezultatom usklajevanja: stanjem usklajevanja „Uspešno“ ali „Neskladnosti“. Sporočila o usklajevanju stalne povezave med registroma so sestavni del izmenjanih sporočil in so zato shranjena, kot je opisano v razdelku „Arhiv sporočil“.

Pogodbenici v evidenco usklajevanja shranita vsak zahtevek in odgovor nanj. Čeprav se informacije iz evidence usklajevanja ne posredujejo neposredno kot del samega usklajevanja, bo za odpravo neskladnosti morda potreben dostop do teh informacij.

Arhiv sporočil

Pogodbenici morata arhivirati kopijo izmenjanih podatkov (datoteke XML), tj. poslanih in prejetih, ter navesti, ali je bil format navedenih podatkov ali sporočil XML pravilen ali ne.

Arhiv je predvsem namenjen za revizijo, tj. da se zagotovijo dokazi o tem, kaj je druga pogodbenica poslala in prejela. V tem smislu je treba poleg datotek arhivirati tudi z njimi povezana potrdila.

Te datoteke vsebujejo tudi dodatne informacije za odpravljanje težav.

Evidenca notranje revizije

Te evidence opredeli in uporablja vsaka pogodbenica zase.

3.5. Operativne zahteve

Izmenjava podatkov med sistemoma pri stalni povezavi med registroma ni v celoti avtonomna, kar pomeni, da so za operacionalizacijo povezave potrebni upravljavci in postopki. V tem procesu je zato podrobno opisanih več vlog in orodij.

4. DOLOČBE GLEDE RAZPOLOŽLJIVOSTI

4.1. Načrt razpoložljivosti komunikacij

Zgradba za stalno povezavo med registroma je v osnovi infrastruktura IKT in programska oprema, ki omogoča komunikacijo med švicarskim ETS in EU ETS. Zagotavljanje visokih ravni razpoložljivosti, celovitosti in zaupnosti tega pretoka podatkov zato postane bistven vidik, ki ga je treba upoštevati pri načrtovanju stalne povezave med registroma. Ker gre za projekt, v katerem imajo ključno vlogo infrastruktura IKT, prilagojena programska oprema in postopki, je treba upoštevati vse tri elemente, da bi se lahko oblikoval odporen sistem.

Odpornost infrastrukture IKT

V poglavju o splošnih določbah v tem dokumentu so podrobno opisani gradniki zgradbe. Na področju infrastrukture IKT stalna povezava med registroma vzpostavlja odporno omrežje VPN, ki ustvarja varne komunikacijske tunele, skozi katere lahko poteka varna izmenjava sporočil. Drugi infrastrukturni elementi so konfigurirani kot visoko razpoložljivi in/ali se zanašajo na nadomestne mehanizme.

Odpornost prilagojene programske opreme

Moduli prilagojene programske opreme povečujejo odpornost z večkratnim poskušanjem vzpostavitve komunikacije z drugim koncem v določenem času, če ta iz katerega koli razloga ni na voljo.

Odpornost storitve

V stalni povezavi med registroma izmenjave podatkov med pogodbenicama potekajo v vnaprej določenih časovnih presledkih. V nekaterih korakih je bilo pri vnaprej načrtovanih izmenjavah podatkov potrebno ročno posredovanje upravljavcev sistemov in/ali administratorjev registrov. Ob upoštevanju tega vidika ter zaradi povečanja razpoložljivosti in uspešnosti izmenjav:

— so v delovnih postopkih predvidena časovna okna za izvajanje vsakega koraka;

— moduli programske opreme za stalno povezavo med registroma izvajajo asinhrono komunikacijo;

— samodejni postopek usklajevanja odkrije morebitne težave pri zajemu podatkovnih datotek na katerem koli koncu;

— postopek spremljanja (infrastrukture IKT in modulov prilagojene programske opreme) velja za enega od postopkov upravljanja incidentov, ki jih tudi sproži (kot je opredeljeno v dokumentu o skupnih delovnih postopkih). Navedeni postopki, katerih cilj je skrajšati čas za obnovitev normalnega delovanja po incidentih, so bistveni za zagotovitev visokih ravni razpoložljivosti.

4.2. Načrt inicializacije, komunikacije, ponovne aktivacije in testiranja

Vsi različni elementi, vključeni v zgradbo stalne povezave med registroma, opravijo niz posameznih in skupinskih testov za potrditev pripravljenosti platforme na ravni infrastrukture IKT in informacijskega sistema. Ti operativni testi so obvezen predpogoj pri vsakem prehodu stalne povezave med registroma na platformi iz stanja prekinitve v stanje delovanja.

Za aktivacijo stanja delovanja povezave se nato zahteva uspešna izvedba vnaprej določenega načrta testiranja. S tem se potrdi, da je bil v vsakem registru najprej opravljen niz notranjih testov, čemur je sledila potrditev povezljivosti med koncema pred začetkom pošiljanja produkcijskih transakcij med pogodbenicama.

Načrt testiranja bi moral vključevati celotno strategijo za testiranje in podrobnosti o testni infrastrukturi. Za vsak posamezen element v vsakem testnem bloku bi moral predvsem vključevati:

— testna merila in orodja;

— dodeljene vloge za izvajanje testa;

— pričakovane rezultate (pozitivne in negativne);

— časovni načrt testiranja;

— zahteve glede zapisovanja rezultatov testa;

— dokumentacijo o odpravljanju težav;

— določbe o prenosu reševanja.

Testi za aktivacijo stanja delovanja bi se kot postopek lahko razdelili na štiri (4) konceptualne bloke ali faze:

4.2.1. Interni testi infrastrukture IKT

Te teste naj bi izvajali in/ali preverjali administratorji registrov na vsakem koncu.

Posebej se testira vsak element infrastrukture IKT na vsakem koncu. To vključuje vsak posamezen sestavni del infrastrukture. Ti testi se lahko izvajajo samodejno ali ročno, v obeh primerih pa preverjajo, ali deluje vsak element infrastrukture.

4.2.2. Testi komunikacije

Te teste sproži katera koli od pogodbenic posamično, za zaključek teh testov pa je potrebno sodelovanje z drugim koncem.

Ko posamezni elementi začnejo delovati, je treba testirati komunikacijske kanale med obema registroma. V ta namen vsaka pogodbenica preveri, ali internetni dostop deluje, ali so vzpostavljeni tuneli VPN in ali obstaja IP-povezljivost od spletnega mesta do spletnega mesta. Nato je treba na drugem koncu potrditi dosegljivost elementov lokalne in oddaljene infrastrukture ter IP-povezljivost.

4.2.3. Testi celotnega sistema (med koncema)

Ti testi naj bi se izvajali na vsakem koncu, rezultati pa bi se delili z drugo pogodbenico.

Ko se opravi testiranje komunikacijskih kanalov in vsakega posameznega sestavnega dela obeh registrov, vsak konec pripravi niz simuliranih transakcij in usklajevanj, ki predstavljajo vse funkcije, ki naj bi se izvajale v okviru povezave.

4.2.4. Testi varnosti

Te teste naj bi izvajali in/ali sprožili administratorji registrov na vsakem koncu v skladu s podrobnimi navodili v oddelkih 5.4 „Smernice za testiranje varnosti“ in 5.5 „Določbe o oceni tveganja“.

Šele ko se vsaka od štirih faz/blokov konča s predvidljivim rezultatom, se lahko šteje, da je stalna povezava med registroma v stanju delovanja.

Viri testiranja

Vsaka pogodbenica ima na voljo določene vire testiranja (določeno programsko in strojno opremo infrastrukture IKT) ter v svojih sistemih razvije testne funkcije, ki zagotavljajo podporo ročni in neprekinjeni potrditvi platforme. Administratorji registrov lahko te postopke sami ali v sodelovanju z drugimi administratorji kadar koli izvajajo ročno. Aktivacija stanja delovanja je sama po sebi postopek, ki se izvaja ročno.

Prav tako je zagotovljeno, da platforma izvaja redna samodejna preverjanja. Namen navedenih preverjanj je povečati dostopnost platforme z zgodnjim odkrivanjem potencialnih težav pri infrastrukturi ali programski opremi. Ta načrt spremljanja platforme sestavljata dva elementa:

— spremljanje infrastrukture IKT: infrastrukturo na obeh koncih spremljajo ponudniki storitev infrastrukture IKT. Samodejni testi zajemajo različne elemente infrastrukture in razpoložljivost komunikacijskih kanalov;

— spremljanje aplikacije: moduli programske opreme stalne povezave med registroma izvajajo sistem spremljanja komunikacije na ravni aplikacije (ročno in/ali redno), s čimer se testira razpoložljivost povezave na obeh koncih s simulacijo nekaterih transakcij prek povezave.

4.3. Okolja sprejemanja/testiranja

Zgradba registra Unije in švicarskega registra vsebuje naslednja tri okolja:

— produkcija (PROD): to okolje vsebuje realne podatke in obdeluje realne transakcije;

— sprejemanje (ACC): to okolje vsebuje nerealne ali anonimizirane, reprezentativne podatke. V tem okolju upravljavci sistemov obeh pogodbenic potrjujejo nove izdaje;

— test (TEST): to okolje vsebuje nerealne ali anonimizirane, reprezentativne podatke. To okolje je omejeno na administratorje registrov in je namenjeno izvajanju integracijskih testov pri obeh pogodbenicah.

Razen v primeru VPN so tri okolja povsem neodvisna drugo od drugega, kar pomeni, da se strojna in programska oprema, podatkovne zbirke, navidezna okolja, IP-naslovi in vhodi vzpostavljajo in delujejo neodvisno drug od drugega.

Pri postavitvi VPN mora biti komunikacija med tremi okolji popolnoma neodvisna, kar zagotavlja uporaba STESTA.

5. DOLOČBE O ZAUPNOSTI IN CELOVITOSTI

Varnostni mehanizmi in postopki vsebujejo metodo dveh oseb (načelo štirih oči) za delovanje v povezavi med registrom Unije in švicarskim registrom. Metoda dveh oseb se uporabi, kadar koli je to potrebno, vendar se morda ne bo uporabila za vse korake, ki jih izvajajo administratorji registrov.

Varnostne zahteve so upoštevane in obravnavane v načrtu upravljanja varnosti, ki vključuje tudi postopke, povezane z obravnavo varnostnih incidentov, ki sledi morebitni kršitvi varnostnih predpisov. Del teh postopkov, ki se nanaša na delovanje, je opisan v dokumentu o skupnih delovnih postopkih.

5.1 Infrastruktura za testiranje varnosti

Vsaka pogodbenica se zaveže, da bo vzpostavila infrastrukturo za testiranje varnosti (z uporabo skupnega sklopa programske in strojne opreme, ki se uporablja pri odkrivanju ranljivosti v fazi razvoja in delovanja):

— ločeno od produkcijskega okolja;

— kadar varnost analizira skupina, in sicer neodvisno od razvoja in delovanja sistema.

Vsaka pogodbenica se zaveže, da bo opravila statično in dinamično analizo.

Pri dinamični analizi (kot je penetracijsko testiranje) se obe pogodbenici zavežeta, da bosta omejili ocene večinoma na okolja testiranja in sprejemanja (kot je opredeljeno v oddelku 4.3 „Okolja sprejemanja/testiranja“). Izjeme pri tej politiki morata odobriti obe pogodbenici.

Pred postavitvijo v produkcijsko okolje se testira varnost pri vsakem modulu programske opreme v povezavi (kot je opredeljeno v oddelku 3.1 „Zgradba komunikacijske vezi“).

Infrastruktura za testiranje mora biti na ravni omrežja in na ravni infrastrukture ločena od produkcijske infrastrukture. Testi varnosti, potrebni za preverjanje skladnosti z varnostnimi zahtevami, se izvajajo v infrastrukturi za testiranje.

5.2 Določbe o prekinitvi povezave in ponovni aktivaciji

Kadar obstaja sum, da je varnost švicarskega registra, SSTL, registra Unije ali EUTL ogrožena, se pogodbenici takoj medsebojno obvestita o tem ter prekineta povezavo med SSTL in EUTL.

| |
|---|
| Postopki izmenjave informacij ter postopki za odločitev o prekinitvi in odločitev o ponovni aktivaciji so del postopka izpolnjevanja zahtevkov, ki je del skupnih delovnih postopkov. |

Prekinitve

Prekinitev povezave med registroma v skladu s Prilogo II k Sporazumu se lahko zgodi zaradi:

— razlogov, povezanih z upravljanjem (npr. vzdrževanje …), ki so načrtovani;

— varnostnih razlogov (ali okvar infrastrukture IT), ki niso načrtovani.

V nujnih primerih pogodbenica o tem obvesti drugo pogodbenico in enostransko prekine povezavo med registroma.

Če je sprejeta odločitev o prekinitvi povezave med registroma, vsaka pogodbenica zagotovi, da se povezava prekine na ravni omrežja (z delnim ali celotnim blokiranjem vhodnih in izhodnih povezav).

| |
|---|
| Odločitev o prekinitvi povezave med registroma, bodisi načrtovani ali nenačrtovani, bo sprejeta v skladu s postopkom upravljanja sprememb ali postopkom obvladovanja varnostnih incidentov, ki sta del skupnih delovnih postopkov. |

Ponovna aktivacija komunikacije

Odločitev o ponovni aktivaciji povezave med registroma se sprejme na način, kot je podrobno opisano v skupnih delovnih postopkih, nikakor pa ne pred uspešnim dokončanjem postopkov testiranja varnosti, kot je navedeno v oddelkih 5.4 „Smernice za testiranje varnosti“ in 4.2 „Načrt inicializacije, komunikacije, ponovne aktivacije in testiranja“.

5.3 Določbe o kršitvah varnostnih predpisov

Kršitev varnostih predpisov velja za varnostni incident, ki vpliva na zaupnost in celovitost vseh občutljivih informacij in/ali razpoložljivost sistema, ki jih obdeluje.

Občutljive informacije so opredeljene na seznamu občutljivih informacij in se lahko obdelujejo v sistemu ali katerem koli povezanem delu sistema.

Informacije, ki so neposredno povezane s kršitvijo varnostnih predpisov, se bodo štele za občutljive z oznako „POSEBNA OBRAVNAVA: *ETS kritična*“ in bodo obdelane v skladu z navodili za ravnanje, razen če je določeno drugače.

| |
|---|
| Vsaka kršitev varnostnih predpisov se obravnava v skladu s poglavjem o obvladovanju varnostnih incidentov v dokumentu o skupnih delovnih postopkih. |

5.4 Smernice za testiranje varnosti

5.4.1 Programska oprema

Pri vseh večjih novih izdajah programske opreme se v skladu z varnostnimi zahtevami, ki jih določajo tehnični standardi za povezavo, opravita testiranje varnosti, po potrebi vključno s penetracijskim testiranjem, da bi se ocenili varnost povezave in povezana tveganja.

Če v zadnjih 12 mesecih ni bila pripravljena nobena večja izdaja, se testiranje varnosti izvede v trenutnem sistemu ob upoštevanju razvoja kibernetskih groženj v zadnjih 12 mesecih.

Testiranje varnosti povezave med registroma se izvede v okolju sprejemanja in po potrebi v produkcijskem okolju ter z usklajevanjem in na podlagi medsebojnega dogovora obeh pogodbenic.

Pri testiranju spletne aplikacije se upoštevajo mednarodni odprti standardi, kot so standardi, razviti v okviru projekta o varnosti odprtih spletnih aplikacij (Open Web Application Security Project – OWASP).

5.4.2 Infrastruktura

Infrastruktura, ki podpira produkcijski sistem, se redno pregleduje zaradi morebitnih ranljivosti (vsaj enkrat na mesec), odkrite ranljivosti pa se popravijo na podlagi istega načela, ki je opredeljeno v prejšnjem oddelku, z uporabo posodobljene podatkovne zbirke o ranljivosti.

5.5 Določbe o oceni tveganja

Če je penetracijsko testiranje mogoče uporabiti, ga je treba vključiti v testiranje varnosti.

Vsaka pogodbenica mora skleniti pogodbo s specializiranim podjetjem za izvajanje testiranja varnosti, če to podjetje:

— ima znanje in izkušnje v zvezi s takim testiranjem varnosti;

— ne poroča neposredno razvijalcu in/ali svojemu izvajalcu in če ni vključeno v razvoj programske opreme za povezavo ali če ni podizvajalec razvijalca;

— podpiše sporazum o zaupnosti, da bi ohranilo zaupnost rezultatov in jih obravnavalo na ravni „POSEBNA OBRAVNAVA: *ETS kritična*“ v skladu z navodili za ravnanje.