ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 20.3.2024
COM(2024) 125 final

ANNEX

ΠΑΡΑΡΤΗΜΑ

της

πρότασης απόφασης του Συμβουλίου

σχετικά με τη θέση που πρέπει να ληφθεί εξ ονόματος της Ευρωπαϊκής Ένωσης στο πλαίσιο της μεικτής επιτροπής που συστάθηκε από τη συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας εκπομπών αερίων θερμοκηπίου, όσον αφορά την τροποποίηση του παραρτήματος II της συμφωνίας, των κοινών επιχειρησιακών διαδικασιών και των τεχνικών προτύπων σύνδεσης

ΑΠΟΦΑΣΗ ΑΡΙΘ. 1/2024 ΤΗΣ ΜΕΙΚΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΟΥ ΣΥΣΤΑΘΗΚΕ ΜΕ ΤΗ ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΚΑΙ ΤΗΣ ΕΛΒΕΤΙΚΗΣ ΣΥΝΟΜΟΣΠΟΝΔΙΑΣ ΓΙΑ ΤΗ ΣΥΝΔΕΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΟΥΣ ΕΜΠΟΡΙΑΣ ΔΙΚΑΙΩΜΑΤΩΝ ΕΚΠΟΜΠΩΝ ΑΕΡΙΩΝ ΘΕΡΜΟΚΗΠΙΟΥ

της.....

όσον αφορά την τροποποίηση του παραρτήματος ΙΙ της συμφωνίας, των κοινών επιχειρησιακών διαδικασιών και των τεχνικών προτύπων σύνδεσης

Η ΜΕΙΚΤΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας εκπομπών αερίων θερμοκηπίου[1] (στο εξής: συμφωνία), και ιδίως το άρθρο 9 και το άρθρο 13 παράγραφος 2,

Εκτιμώντας τα ακόλουθα:

(1) Η απόφαση αριθ. 2/2019 της μεικτής επιτροπής[2] προέβλεπε μια προσωρινή λύση για την επιχειρησιακή εφαρμογή της σύνδεσης μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας.

(2) Κατά την τρίτη συνεδρίασή της, η μεικτή επιτροπή συμφώνησε ως προς την ανάγκη ανάλυσης της σχέσης κόστους-αποτελεσματικότητας της μόνιμης σύνδεσης μεταξύ του ενωσιακού μητρώου και του μητρώου της Ελβετίας.

(3) Κατά την 5η συνεδρίασή της, η μεικτή επιτροπή ενέκρινε την έκθεση που υπέβαλε η ομάδα εργασίας που συστάθηκε με τις αποφάσεις 1/2020[3] και 2/2020[4] της μεικτής επιτροπής και στην οποία η εν λόγω ομάδα εργασίας ανέλυσε και συνέστησε μια προσέγγιση για την εφαρμογή της μόνιμης σύνδεσης του ενωσιακού μητρώου και του μητρώου της Ελβετίας.

(4) Για να αντικατοπτρίζονται οι τεχνικές απαιτήσεις της μόνιμης σύνδεσης του ενωσιακού μητρώου και του μητρώου της Ελβετίας, καθώς και για να εξορθολογιστούν οι διατάξεις του παραρτήματος ΙΙ της συμφωνίας υπό το πρίσμα των τεχνολογικών εξελίξεων, το παράρτημα ΙΙ της συμφωνίας θα πρέπει να τροποποιηθεί.

(5) Για να διασφαλιστεί η συνοχή των κοινών επιχειρησιακών διαδικασιών και των τεχνικών προτύπων σύνδεσης με το παράρτημα ΙΙ της συμφωνίας, τα εν λόγω έγγραφα θα πρέπει επίσης να τροποποιηθούν,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

1. Το παράρτημα ΙΙ της συμφωνίας αντικαθίσταται από το κείμενο του παραρτήματος Ι της παρούσας απόφασης.

2. Οι κοινές επιχειρησιακές διαδικασίες που αναφέρονται στο άρθρο 3 παράγραφος 6 της συμφωνίας παρατίθενται στο παράρτημα ΙΙ της παρούσας απόφασης.

3. Τα τεχνικά πρότυπα σύνδεσης που αναφέρονται στο άρθρο 3 παράγραφος 7 της συμφωνίας παρατίθενται στο παράρτημα ΙΙΙ της παρούσας απόφασης.

---

1 ΕΕ L 322 της 7.12.2017, σ. 3.
2 ΕΕ L 314 της 29.9.2020, σ. 68.
3 ΕΕ L 226 της 25.6.2021, σ. 2.
4 ΕΕ L 226 της 25.6.2021, σ. 16.

Άρθρο 2

Η παρούσα απόφαση αρχίζει να ισχύει την ημέρα της έκδοσής της.

Συντάχθηκε στην αγγλική γλώσσα στ... [Βρυξέλλες] [Βέρνη] στις/την [xx 2024].

Για τη μεικτή επιτροπή

Η γραμματέας για την Ευρωπαϊκή Ένωση	*Η πρόεδρος*	*Η γραμματέας για την Ελβετία*

ΠΑΡΑΡΤΗΜΑ Ι

«ΠΑΡΑΡΤΗΜΑ ΙΙ

ΤΕΧΝΙΚΑ ΠΡΟΤΥΠΑ ΣΥΝΔΕΣΗΣ

Για να καταστεί λειτουργική η σύνδεση μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας, το 2020 εφαρμόστηκε προσωρινή λύση. Από το 2023 η σύνδεση των μητρώων των δύο συστημάτων εμπορίας δικαιωμάτων εκπομπών θα εξελιχθεί σταδιακά σε μόνιμη σύνδεση των μητρώων η οποία αναμένεται να υλοποιηθεί το αργότερο το 2024 και η οποία θα καταστήσει δυνατή τη λειτουργία των συνδεδεμένων αγορών όσον αφορά τα οφέλη από τη ρευστότητα της αγοράς και την εκτέλεση των συναλλαγών μεταξύ των δύο συνδεδεμένων συστημάτων κατά τρόπο που ισοδυναμεί με μία αγορά που αποτελείται από δύο συστήματα και επιτρέπει στους συμμετέχοντες στην αγορά να ενεργούν σαν να ήταν σε μία αγορά, με την επιφύλαξη μόνο των επιμέρους κανονιστικών διατάξεων των συμβαλλόμενων μερών. Τα τεχνικά πρότυπα σύνδεσης (ΤΠΣ) ορίζουν συγκεκριμένα:

– την αρχιτεκτονική της σύνδεσης επικοινωνίας

– τις επικοινωνίες μεταξύ του SSTL και του EUTL

– την ασφάλεια της διαβίβασης δεδομένων

– τον κατάλογο καθηκόντων (συναλλαγές, αντιπαραβολή...)

– τον ορισμό του επιπέδου μεταφοράς

– τις απαιτήσεις καταγραφής δεδομένων

– τις ρυθμίσεις λειτουργίας (τηλεφωνική γραμμή βοήθειας, υποστήριξη)

– το σχέδιο ενεργοποίησης της σύνδεσης επικοινωνίας και τη διαδικασία δοκιμών

– τη διαδικασία δοκιμών ασφαλείας.

Τα ΤΠΣ ορίζουν συγκεκριμένα ότι οι διαχειριστές οφείλουν να λαμβάνουν όλα τα εύλογα μέτρα για να διασφαλίσουν τη λειτουργία του SSTL, του EUTL και της σύνδεσης σε εικοσιτετράωρη βάση, επτά ημέρες την εβδομάδα, και να περιορίζουν στο ελάχιστο δυνατό τις όποιες διακοπές λειτουργίας του SSTL, του EUTL και της σύνδεσης.

Τα ΤΠΣ ορίζουν πρόσθετες απαιτήσεις ασφαλείας για το ελβετικό μητρώο, το SSTL, το ενωσιακό μητρώο και το EUTL, οι οποίες καταγράφονται σε «σχέδιο διαχείρισης της ασφάλειας». Τα ΤΠΣ ορίζουν συγκεκριμένα ότι:

– αν υπάρχει υπόνοια ότι έχει διακυβευτεί η ασφάλεια του ελβετικού μητρώου, του SSTL, του ενωσιακού μητρώου ή του EUTL, αμφότερα τα συμβαλλόμενα μέρη αλληλοενημερώνονται αμέσως και αναστέλλουν τη σύνδεση μεταξύ του SSTL και του EUTL

– σε περίπτωση παραβίασης της ασφάλειας, τα συμβαλλόμενα μέρη δεσμεύονται να ανταλλάξουν άμεσα τις σχετικές πληροφορίες μεταξύ τους χωρίς καθυστέρηση. Εφόσον είναι διαθέσιμες οι τεχνικές λεπτομέρειες, εντός 24 ωρών από τον προσδιορισμό περιστατικού ασφάλειας ως παραβίασης της ασφάλειας, ανταλλάσσεται μεταξύ του διαχειριστή του ελβετικού μητρώου και του κεντρικού διαχειριστή της Ένωσης έκθεση στην οποία περιγράφεται το περιστατικό (ημερομηνία, αιτία, επιπτώσεις, διορθωτικά μέτρα).

Η διαδικασία δοκιμών ασφαλείας που ορίζεται στα ΤΠΣ ολοκληρώνεται πριν από την εγκατάσταση της σύνδεσης επικοινωνίας μεταξύ του SSTL και του EUTL και όταν απαιτείται νέα έκδοση ή κυκλοφορία του SSTL ή του EUTL.

Τα ΤΠΣ παρέχουν δύο περιβάλλοντα δοκιμών επιπροσθέτως του περιβάλλοντος παραγωγής: ένα περιβάλλον δοκιμών κατασκευαστή και ένα περιβάλλον αποδοχής.

Μέσω του διαχειριστή του ελβετικού μητρώου και του κεντρικού διαχειριστή της Ένωσης, τα συμβαλλόμενα μέρη υποβάλλουν στοιχεία από τα οποία αποδεικνύεται ότι τα συστήματά τους έχουν υποβληθεί σε ανεξάρτητη εκτίμηση ασφαλείας τους τελευταίους 12 μήνες σύμφωνα με τις απαιτήσεις ασφαλείας που ορίζονται στα ΤΠΣ. Οι δοκιμές ασφαλείας και συγκεκριμένα οι δοκιμές διείσδυσης διενεργούνται σε όλες τις νέες σημαντικές κυκλοφορίες του λογισμικού σύμφωνα με τις απαιτήσεις ασφαλείας που ορίζονται στα ΤΠΣ. Δεν επιτρέπεται η διενέργεια των δοκιμών διείσδυσης από τον κατασκευαστή του λογισμικού ή από υπεργολάβο του κατασκευαστή του λογισμικού».

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΚΟΙΝΕΣ ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ (ΚΕΔ)

σύμφωνα με το άρθρο 3 παράγραφος 6 της συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας εκπομπών αερίων θερμοκηπίου

Διαδικασίες για τη μόνιμη σύνδεση των μητρώων

Περιεχόμενα

1. Γλωσσάριο 10
2. Εισαγωγή 11
2.1. Πεδίο εφαρμογής 11
2.2. Αποδέκτες 12
3. Προσέγγιση και πρότυπα 12
4. Διαχείριση περιστατικών 13
4.1. Ανίχνευση και καταγραφή περιστατικών 13
4.2. Ταξινόμηση και αρχική υποστήριξη 14
4.3. Διερεύνηση και διάγνωση 14
4.4. Επίλυση και ανάκαμψη 15
4.5. Κλείσιμο του περιστατικού 15
5. Διαχείριση προβλημάτων 16
5.1. Προσδιορισμός και καταγραφή του προβλήματος 16
5.2. Κατάταξη των προβλημάτων ανά προτεραιότητα 16
5.3. Διερεύνηση και διάγνωση προβλημάτων 16
5.4. Επίλυση 16
5.5. Κλείσιμο του προβλήματος 17
6. Ικανοποίηση αιτημάτων 17
6.1. Υποβολή αιτήματος 17
6.2. Καταγραφή και ανάλυση του αιτήματος 17
6.3. Έγκριση αιτήματος 17
6.4. Ικανοποίηση αιτήματος 17
6.5. Κλιμάκωση αιτήματος 18
6.6. Επανεξέταση της ικανοποίησης του αιτήματος 18
6.7. Κλείσιμο του αιτήματος 18
7. Διαχείριση αλλαγών 19

7.1. Αίτημα αλλαγής 19
7.2. Αξιολόγηση και προγραμματισμός αλλαγής 19
7.3. Εγκρίσεις αλλαγής 19
7.4. Υλοποίηση της αλλαγής 19
8. Διαχείριση εκδόσεων 20
8.1. Προγραμματισμός της έκδοσης 20
8.2. Οικοδόμηση και δοκιμή του πακέτου της έκδοσης 20
8.3. Προετοιμασία της εγκατάστασης 21
8.4. Επαναφορά στην προηγούμενη έκδοση 21
8.5. Επανεξέταση και κλείσιμο έκδοσης 21
9. Διαχείριση περιστατικών ασφάλειας 22
9.1. Κατάταξη περιστατικών ασφάλειας πληροφοριών 22
9.2. Διαχείριση περιστατικών ασφάλειας πληροφοριών 22
9.3. Αναγνώριση περιστατικών ασφάλειας 23
9.4. Ανάλυση περιστατικών ασφάλειας 23
9.5. Εκτίμηση της σοβαρότητας περιστατικού ασφάλειας, κλιμάκωση και υποβολή εκθέσεων 23
9.6. Υποβολή εκθέσεων σχετικά με την αντιμετώπιση περιστατικών ασφάλειας 23
9.7. Παρακολούθηση, δημιουργία ικανοτήτων και συνεχής βελτίωση 23
10. Διαχείριση της ασφάλειας των πληροφοριών 24
10.1. Αναγνώριση των ευαίσθητων πληροφοριών 24
10.2. Επίπεδα ευαισθησίας των πληροφορικών πόρων 24
10.3. Καθορισμός του ιδιοκτήτη των πληροφορικών πόρων 24
10.4. Καταχώριση ευαίσθητων πληροφοριών 25
10.5. Χειρισμός ευαίσθητων πληροφοριών 25
10.6. Διαχείριση πρόσβασης 25
10.7. Διαχείριση πιστοποιητικών/κλειδιών 26
1. Γλωσσάριο 29
2. Εισαγωγή 32
2.1. Πεδίο εφαρμογής 33
2.2. Αποδέκτες 33
3. Γενικές διατάξεις 33
3.1. Αρχιτεκτονική της σύνδεσης επικοινωνίας 33

3.1.1. Ανταλλαγή μηνυμάτων 33
3.1.2. Μήνυμα XML — Περιγραφή υψηλού επιπέδου 34
3.1.3. Παράθυρα πρόσληψης (ingestion windows) 34
3.1.4. Ροές μηνυμάτων συναλλαγής 34
3.2. Ασφάλεια της μεταφοράς δεδομένων 37
3.2.1. Τείχος προστασίας και διασύνδεση δικτύων 38
3.2.2. Εικονικό ιδιωτικό δίκτυο (VPN) 38
3.2.3. Εφαρμογή της IPsec 38
3.2.4. Πρωτόκολλο ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων 38
3.2.5. Κρυπτογράφηση και υπογραφή XML 39
3.2.6. Κρυπτογραφικά κλειδιά 39
3.3. Κατάλογος λειτουργιών στο πλαίσιο της σύνδεσης 39
3.3.1. Συναλλαγές σχετικές με δραστηριότητες εμπορίας δικαιωμάτων εκπομπών 39
3.3.2. Πρωτόκολλο αντιπαραβολής 40
3.3.3. Δοκιμαστικό μήνυμα 40
3.4. Απαιτήσεις καταγραφής δεδομένων 41
3.5. Επιχειρησιακές απαιτήσεις 42
4. Διατάξεις περί διαθεσιμότητας 43
4.1. Σχεδιασμός της επικοινωνιακής διαθεσιμότητας 43
4.2. Αρχικοποίηση, επικοινωνία, επανενεργοποίηση και σχέδιο δοκιμών 43
4.2.1. Εσωτερικές δοκιμές υποδομής ΤΠΕ 44
4.2.2. Δοκιμές επικοινωνίας 44
4.2.3. Δοκιμές πλήρους συστήματος (διατερματικά) 44
4.2.4. Δοκιμές ασφαλείας 45
4.3. Περιβάλλοντα αποδοχής / δοκιμών 45
5. Διατάξεις για την εμπιστευτικότητα και την ακεραιότητα 46
5.1. Υποδομή για τους ελέγχους της ασφάλειας 46
5.2. Αναστολή της σύνδεσης και διατάξεις για την επανενεργοποίηση 46
5.3. Διατάξεις για την παραβίαση της ασφάλειας 47
5.4. Κατευθυντήριες γραμμές για τους ελέγχους της ασφάλειας 47
5.4.1. Λογισμικό 47
5.4.2. Υποδομές 48
5.5. Διατάξεις αξιολόγησης κινδύνου 48

1. ΓΛΩΣΣΑΡΙΟ

Πίνακας 1-1 Αρκτικόλεξα και ορισμοί

Αρκτικόλεξο/Όρος	Ορισμός
Αρχή πιστοποίησης (ΑΠ)	Οντότητα που εκδίδει ψηφιακά πιστοποιητικά
CH	Ελβετική Συνομοσπονδία
ΣΕΔΕ	Σύστημα Εμπορίας Δικαιωμάτων Εκπομπών
ΕΕ	Ευρωπαϊκή Ένωση
ΟΔΠ	Ομάδα Διαχείρισης Περιστατικών
Πληροφορικός πόρος	Πληροφορία που έχει αξία για μια εταιρεία ή έναν οργανισμό
ΤΠ	Τεχνολογία πληροφοριών
ITIL	Βιβλιοθήκη υποδομής τεχνολογίας των πληροφοριών (Information Technology Infrastructure Library)
ITSM	Διαχείριση υπηρεσιών ΤΠ (IT Service Management)
ΤΠΣ	Τεχνικά πρότυπα σύνδεσης
Μητρώο	Λογιστικό σύστημα για τα δικαιώματα που εκχωρούνται στο πλαίσιο του ΣΕΔΕ, το οποίο καταγράφει την κυριότητα των δικαιωμάτων που τηρούνται σε ηλεκτρονικούς λογαριασμούς.
RFC	Αίτημα αλλαγής (Request For Change)
SIL	Κατάλογος ευαίσθητων πληροφοριών (Sensitive Information List)
SR	Αίτημα παροχής υπηρεσιών (Service Request)
Wiki	Ιστότοπος που δίνει τη δυνατότητα στους χρήστες να ανταλλάσσουν πληροφορίες και γνώσεις προσθέτοντας ή προσαρμόζοντας περιεχόμενο απευθείας μέσω προγράμματος διαδικτυακής περιήγησης.

2. ΕΙΣΑΓΩΓΗ

Η συμφωνία της 23ης Νοεμβρίου 2017 μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας δικαιωμάτων εκπομπών αερίων θερμοκηπίου (στο εξής: συμφωνία) προβλέπει την αμοιβαία αναγνώριση δικαιωμάτων εκπομπών τα οποία μπορούν να χρησιμοποιηθούν για συμμόρφωση στο πλαίσιο του συστήματος εμπορίας δικαιωμάτων εκπομπών της Ευρωπαϊκής Ένωσης (στο εξής: ΣΕΔΕ της ΕΕ) ή του συστήματος εμπορίας δικαιωμάτων εκπομπών της Ελβετίας (στο εξής: ΣΕΔΕ της Ελβετίας). Για να καταστεί λειτουργική η σύνδεση ανάμεσα στο ΣΕΔΕ της ΕΕ και το ΣΕΔΕ της Ελβετίας, θα εγκαθιδρυθεί άμεση σύνδεση ανάμεσα στο ημερολόγιο συναλλαγών της ΕΕ (European Union Transaction Log – EUTL) του ενωσιακού μητρώου και στο ελβετικό συμπληρωματικό ημερολόγιο συναλλαγών (Swiss Supplementary Transaction Log – SSTL) του ελβετικού μητρώου, η οποία θα επιτρέψει τη μεταξύ των μητρώων μεταφορά δικαιωμάτων εκπομπών που εκχωρούνται από οποιοδήποτε εκ των δύο ΣΕΔΕ (άρθρο 3 παράγραφος 2 της συμφωνίας). Για να καταστεί λειτουργική η σύνδεση μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας, το 2020 εφαρμόστηκε προσωρινή λύση. Από το 2023 η σύνδεση των μητρώων των δύο συστημάτων εμπορίας δικαιωμάτων εκπομπών θα εξελιχθεί σταδιακά σε μόνιμη σύνδεση των μητρώων η οποία αναμένεται να υλοποιηθεί το αργότερο το 2024 και η οποία θα καταστήσει δυνατή τη λειτουργία των συνδεδεμένων αγορών όσον αφορά τα οφέλη από τη ρευστότητα της αγοράς και την εκτέλεση των συναλλαγών μεταξύ των δύο συνδεδεμένων συστημάτων κατά τρόπο που ισοδυναμεί με μία αγορά που αποτελείται από δύο συστήματα και επιτρέπει στους συμμετέχοντες στην αγορά να ενεργούν σαν να ήταν σε μία αγορά, με την επιφύλαξη μόνο των επιμέρους κανονιστικών διατάξεων των συμβαλλόμενων μερών. (Παράρτημα ΙΙ της συμφωνίας).

Σύμφωνα με το άρθρο 3 παράγραφος 6 της συμφωνίας, ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής της Ένωσης καθορίζουν κοινές επιχειρησιακές διαδικασίες (ΚΕΔ) οι οποίες αφορούν τεχνικά ή άλλα ζητήματα απαραίτητα για τη λειτουργία της σύνδεσης και λαμβάνουν υπόψη τις προτεραιότητες της εθνικής νομοθεσίας. Οι ΚΕΔ που αναπτύσσουν οι διαχειριστές παράγουν αποτελέσματα αφού εγκριθούν με απόφαση της μεικτής επιτροπής.

Οι ΚΕΔ εγκρίθηκαν από τη μεικτή επιτροπή με την απόφαση αριθ. 1/2020. Οι επικαιροποιημένες ΚΕΔ, όπως καταγράφονται στο παρόν έγγραφο, θα εγκριθούν από τη μεικτή επιτροπή με την απόφαση αριθ. 1/2024. Σύμφωνα με την παρούσα απόφαση και τα αιτήματα της μεικτής επιτροπής, ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής της Ένωσης έχουν αναπτύξει και θα επικαιροποιούν περαιτέρω τεχνικές κατευθυντήριες γραμμές ώστε να καταστεί λειτουργική η σύνδεση και να εξασφαλιστεί ότι αυτές οι κατευθυντήριες γραμμές προσαρμόζονται συνεχώς στην τεχνική πρόοδο και στις νέες απαιτήσεις που αφορούν την ασφάλεια και την προστασία της σύνδεσης, καθώς και την αποτελεσματική και αποδοτική λειτουργία της.

2.1. Πεδίο εφαρμογής

Το παρόν έγγραφο αποτελεί την κοινή συμφωνία μεταξύ των συμβαλλόμενων μερών όσον αφορά την καθιέρωση των διαδικαστικών θεμελίων για τη σύνδεση μεταξύ των μητρώων του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας. Σκιαγραφεί μεν τις συνολικές διαδικαστικές απαιτήσεις όσον αφορά τις λειτουργίες, αλλά θα χρειαστούν ορισμένες περαιτέρω τεχνικές κατευθυντήριες γραμμές για να καταστεί λειτουργική η σύνδεση.

Για την ορθή λειτουργία της σύνδεσης θα χρειαστούν τεχνικές προδιαγραφές οι οποίες θα βελτιώσουν την επιχειρησιακή λειτουργία της. Σύμφωνα με το άρθρο 3 παράγραφος 7 της

συμφωνίας, τα θέματα αυτά περιγράφονται λεπτομερώς στα τεχνικά πρότυπα σύνδεσης (ΤΠΣ), έγγραφο το οποίο θα εγκριθεί χωριστά με απόφαση της μεικτής επιτροπής.

Σκοπός των ΚΕΔ είναι να εξασφαλίσουν ότι οι υπηρεσίες ΤΠ που σχετίζονται με τη λειτουργία της σύνδεσης μεταξύ των μητρώων του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας παρέχονται αποτελεσματικά και αποδοτικά, ιδίως όσον αφορά την ικανοποίηση των αιτημάτων παροχής υπηρεσιών, την επίλυση των βλαβών υπηρεσίας, τη διόρθωση των προβλημάτων, καθώς και την εκτέλεση των συνήθων επιχειρησιακών καθηκόντων σύμφωνα με τα διεθνή πρότυπα για τη διαχείριση υπηρεσιών ΤΠ.

Για τη μόνιμη σύνδεση των μητρώων, θα χρειαστούν μόνο οι ακόλουθες ΚΕΔ, οι οποίες αποτελούν μέρος του παρόντος εγγράφου:

- Διαχείριση περιστατικών·
- Διαχείριση προβλημάτων·
- Ικανοποίηση αιτημάτων·
- Διαχείριση αλλαγών·
- Διαχείριση εκδόσεων·
- Διαχείριση περιστατικών ασφάλειας·
- Διαχείριση της ασφάλειας των πληροφοριών.

2.2. Αποδέκτες

Το στοχευόμενο κοινό αυτών των ΚΕΔ είναι οι ομάδες υποστήριξης του ενωσιακού και του ελβετικού μητρώου.

3. ΠΡΟΣΕΓΓΙΣΗ ΚΑΙ ΠΡΟΤΥΠΑ

Η ακόλουθη αρχή εφαρμόζεται σε όλες τις ΚΕΔ:

- Η ΕΕ και η Ελβετία συμφωνούν να ορίσουν τις ΚΕΔ με βάση την ITIL (Βιβλιοθήκη υποδομής τεχνολογίας των πληροφοριών, έκδοση 4). Πρακτικές του προτύπου αυτού επαναχρησιμοποιούνται και προσαρμόζονται στις ειδικές ανάγκες που σχετίζονται με τη μόνιμη σύνδεση των μητρώων·
- Η επικοινωνία και ο συντονισμός που απαιτούνται για την επεξεργασία των ΚΕΔ μεταξύ των δύο συμβαλλόμενων μερών λαμβάνουν χώρα μέσω των υπηρεσιών υποστήριξης μητρώου της Ελβετίας και της ΕΕ. Τα καθήκοντα ανατίθενται πάντοτε εντός ενός συμβαλλόμενου μέρους·
- Εάν υπάρχει διαφωνία σχετικά με τον χειρισμό μιας ΚΕΔ, αυτή θα αναλυθεί και θα επιλυθεί από κοινού από τις δύο υπηρεσίες υποστήριξης. Εάν δεν επιτευχθεί συμφωνία, η εύρεση κοινής λύσης κλιμακώνεται στο επόμενο επίπεδο.

Επίπεδα κλιμάκωσης	**ΕΕ**	**CH**
1ο επίπεδο	Υπηρεσία υποστήριξης ΕΕ	Υπηρεσία υποστήριξης Ελβετίας
2ο επίπεδο	Επιχειρησιακός διαχειριστής της ΕΕ	Διαχειριστής εφαρμογής μητρώου της Ελβετίας

3ο επίπεδο	Μεικτή επιτροπή (η οποία μπορεί να αναθέσει αυτή την αρμοδιότητα σε άλλους, λαμβάνοντας υπόψη το άρθρο 12 παράγραφος 5 της συμφωνίας για τη σύνδεση)
4ο επίπεδο	Μεικτή επιτροπή, εάν το 3ο επίπεδο ανατεθεί σε άλλους

- Κάθε συμβαλλόμενο μέρος μπορεί να καθορίσει τις διαδικασίες για τη λειτουργία του δικού του συστήματος μητρώου, λαμβάνοντας υπόψη τις απαιτήσεις και τις διεπαφές που συνδέονται με τις εν λόγω ΚΕΔ.
- Για την υποστήριξη των ΚΕΔ χρησιμοποιείται το εργαλείο διαχείρισης υπηρεσιών ΤΠ (ITSM), και ιδίως η διαχείριση περιστατικών, η διαχείριση προβλημάτων και η ικανοποίηση αιτημάτων, καθώς και η επικοινωνία μεταξύ των δύο συμβαλλόμενων μερών.
- Επιπλέον, επιτρέπεται η ανταλλαγή πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου.
- Τα δύο συμβαλλόμενα μέρη εξασφαλίζουν ότι πληρούνται οι απαιτήσεις ασφάλειας των πληροφοριών, σύμφωνα με τις οδηγίες χειρισμού.

4. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Στόχος της διαδικασίας διαχείρισης περιστατικών είναι να επαναφέρει τις υπηρεσίες ΤΠ σε κανονικό επίπεδο υπηρεσιών το συντομότερο δυνατόν μετά το περιστατικό, με την ελάχιστη διαταραχή των επιχειρησιακών δραστηριοτήτων.

Η διαχείριση περιστατικών θα πρέπει επίσης να τηρεί αρχείο περιστατικών για σκοπούς λογοδοσίας και να συμβαδίζει με άλλες διαδικασίες ώστε να είναι δυνατή η συνεχής βελτίωση.

Σε γενικό επίπεδο, η διαχείριση περιστατικών περιλαμβάνει τις ακόλουθες δραστηριότητες:

- Ανίχνευση και καταγραφή περιστατικών
- Ταξινόμηση και αρχική υποστήριξη
- Διερεύνηση και διάγνωση
- Επίλυση και ανάκαμψη
- Κλείσιμο του περιστατικού.

Σε όλη τη διάρκεια του κύκλου ζωής ενός περιστατικού, η διαδικασία διαχείρισης περιστατικών είναι αρμόδια για τη συνεχή διαχείριση της ιδιοκτησίας, της επίβλεψης, της παρακολούθησης και της επικοινωνίας.

4.1. Ανίχνευση και καταγραφή περιστατικών

Ένα περιστατικό μπορεί να ανιχνευθεί από ομάδα υποστήριξης, από αυτόματα εργαλεία παρακολούθησης ή από τεχνικό προσωπικό που εκτελεί τακτική επιτήρηση.

Όταν ανιχνευθεί, το περιστατικό πρέπει να καταγραφεί και να του αποδοθεί ένας μοναδικός αναγνωριστικός κωδικός ο οποίος να επιτρέπει την ορθή παρακολούθηση και επίβλεψή του. Ο μοναδικός αναγνωριστικός κωδικός περιστατικού είναι ο κωδικός που αποδίδεται στο κοινό σύστημα δήλωσης περιστατικών από την υπηρεσία υποστήριξης του συμβαλλόμενου μέρους (της ΕΕ ή της Ελβετίας) που δήλωσε το περιστατικό· ο εν λόγω κωδικός πρέπει να χρησιμοποιείται σε κάθε επικοινωνία που συνδέεται με το εν λόγω περιστατικό.

Για όλα τα περιστατικά, το σημείο επαφής θα πρέπει να είναι η υπηρεσία υποστήριξης του συμβαλλόμενου μέρους που κατέγραψε τη δήλωση του περιστατικού.

4.2. Ταξινόμηση και αρχική υποστήριξη

Η ταξινόμηση των περιστατικών αποσκοπεί στην κατανόηση και στον προσδιορισμό του συστήματος και/ή της υπηρεσίας που έχει πληγεί από ένα περιστατικό και του βαθμού στον οποίο έχει πληγεί. Η ταξινόμηση, για να είναι αποτελεσματική, θα πρέπει να δρομολογεί το συμβάν στον σωστό πόρο από την πρώτη αντίδραση, ώστε να επιταχύνεται η επίλυση του περιστατικού.

Κατά τη φάση της ταξινόμησης, θα πρέπει το περιστατικό να κατατάσσεται σε κατηγορία και να του αποδίδεται προτεραιότητα ανάλογα με τον αντίκτυπο και τον επείγοντα χαρακτήρα του, έτσι ώστε να αντιμετωπίζεται σύμφωνα με το σχετικό χρονοδιάγραμμα ανά βαθμό προτεραιότητας.

Εάν το περιστατικό έχει δυνητικό αντίκτυπο στην εμπιστευτικότητα ή την ακεραιότητα ευαίσθητων δεδομένων, και/ή αντίκτυπο στη διαθεσιμότητα του συστήματος, τότε θα πρέπει να χαρακτηρίζεται και ως περιστατικό ασφάλειας και να αντιμετωπίζεται σύμφωνα με τη διαδικασία που ορίζεται στο κεφάλαιο «Διαχείριση περιστατικών ασφάλειας» του παρόντος εγγράφου.

Εάν είναι δυνατόν, η υπηρεσία υποστήριξης που κατέγραψε τη δήλωση του περιστατικού προβαίνει σε αρχική διάγνωση. Για τον σκοπό αυτόν, η υπηρεσία υποστήριξης διαπιστώνει αν το περιστατικό αποτελεί γνωστό σφάλμα. Εάν ναι, τότε η διαδικασία επίλυσης ή παράκαμψης του προβλήματος είναι ήδη γνωστή και τεκμηριωμένη.

Εάν η υπηρεσία υποστήριξης καταφέρει να αντιμετωπίσει επιτυχώς το περιστατικό, τότε θα κλείσει το αρχείο καταγραφής του, καθώς θα έχει εκπληρωθεί ο πρωταρχικός σκοπός της διαχείρισης περιστατικών (δηλαδή η ταχεία αποκατάσταση της υπηρεσίας για τον τελικό χρήστη). Εάν όχι, η υπηρεσία υποστήριξης θα παραπέμψει το περιστατικό στην κατάλληλη ομάδα επίλυσης για περαιτέρω διερεύνηση και διάγνωση.

4.3. Διερεύνηση και διάγνωση

Η διερεύνηση και διάγνωση των περιστατικών διενεργείται όταν έναν περιστατικό δεν μπορεί να επιλυθεί από την υπηρεσία υποστήριξης ως μέρος της αρχικής διάγνωσης, και, συνεπώς, παραπέμπεται στο κατάλληλο επίπεδο. Η παραπομπή των περιστατικών στο κατάλληλο επίπεδο αποτελεί πλήρες μέρος της διαδικασίας διερεύνησης και διάγνωσης.

Μια κοινή πρακτική στο στάδιο της διερεύνησης και διάγνωσης είναι η προσπάθεια αναπαραγωγής του περιστατικού υπό ελεγχόμενες συνθήκες. Κατά τη διερεύνηση και διάγνωση του περιστατικού, είναι σημαντικό να γίνεται κατανοητή η ορθή σειρά των γεγονότων που οδήγησαν σε αυτό.

Κλιμάκωση είναι η διαπίστωση ότι ένα περιστατικό δεν μπορεί να επιλυθεί στο τρέχον επίπεδο στήριξης και ότι πρέπει να παραπεμφθεί σε ομάδα υποστήριξης υψηλότερου επιπέδου ή στο άλλο συμβαλλόμενο μέρος. Η κλιμάκωση μπορεί να ακολουθήσει δύο πορείες: την οριζόντια (λειτουργική) ή την κάθετη (ιεραρχική).

Η υπηρεσία υποστήριξης που κατέγραψε και δρομολόγησε το περιστατικό είναι υπεύθυνη για την κλιμάκωσή του στον κατάλληλο πόρο και για την παρακολούθηση της συνολικής κατάστασης και της ανάθεσης του περιστατικού.

Το συμβαλλόμενο μέρος στο οποίο έχει ανατεθεί το περιστατικό είναι υπεύθυνο για την έγκαιρη εκτέλεση των απαιτούμενων ενεργειών και για την παροχή ανατροφοδότησης στη δική του υπηρεσία υποστήριξης.

4.4. Επίλυση και ανάκαμψη

Η επίλυση του περιστατικού και η ανάκαμψη λαμβάνουν χώρα αφότου το περιστατικό έχει γίνει πλήρως κατανοητό. Η επίλυση περιστατικού σημαίνει ότι έχει βρεθεί τρόπος διόρθωσης του προβλήματος. Η διεργασία επίλυσης αποτελεί το στάδιο της ανάκαμψης.

Μόλις οι κατάλληλοι πόροι επιλύσουν τη βλάβη υπηρεσίας, το περιστατικό επιστρέφεται στην αρμόδια υπηρεσία υποστήριξης η οποία το κατέγραψε και η οποία επιβεβαιώνει με τον χρήστη που δήλωσε το περιστατικό ότι το σφάλμα έχει διορθωθεί και ότι το περιστατικό μπορεί να κλείσει. Τα πορίσματα που εξάγονται από την επεξεργασία του περιστατικού πρέπει να καταγράφονται για μελλοντική χρήση.

Η ανάκαμψη μπορεί να εκτελεστεί από το προσωπικό υποστήριξης της ΤΠ ή με την παροχή στον τελικό χρήστη σειράς οδηγιών προς εκτέλεση.

4.5. Κλείσιμο του περιστατικού

Το κλείσιμο είναι το τελευταίο βήμα στη διαδικασία διαχείρισης περιστατικών και πραγματοποιείται σύντομα μετά την επίλυση του περιστατικού.

Από τον κατάλογο των δραστηριοτήτων που πρέπει να εκτελεστούν κατά το στάδιο του κλεισίματος, τονίζονται οι εξής:

- Η επαλήθευση της αρχικής κατηγορίας στην οποία είχε καταταχθεί το περιστατικό·
- Η ορθή αποτύπωση όλων των πληροφοριών που περιβάλλουν το περιστατικό·
- Η ορθή τεκμηρίωση του περιστατικού και η επικαιροποίηση της βάσης γνώσεων·
- Η κατάλληλη επικοινωνία με κάθε ενδιαφερόμενο που επηρεάζεται άμεσα ή έμμεσα από το περιστατικό.

Ένα περιστατικό κλείνει επισήμως όταν το στάδιο του κλεισίματος έχει ολοκληρωθεί από την υπηρεσία υποστήριξης και έχει κοινοποιηθεί στο άλλο συμβαλλόμενο μέρος.

Από τη στιγμή που ένα περιστατικό έχει κλείσει, δεν ανοίγει εκ νέου. Εάν ένα περιστατικό εμφανιστεί εκ νέου εντός σύντομου χρονικού διαστήματος, δεν ανοίγει εκ νέου το αρχικό περιστατικό αλλά καταγράφεται νέο περιστατικό.

Εάν το περιστατικό παρακολουθείται τόσο από την υπηρεσία υποστήριξης της ΕΕ όσο και από την υπηρεσία υποστήριξης της Ελβετίας, το τελικό κλείσιμο αποτελεί ευθύνη της υπηρεσίας υποστήριξης που κατέγραψε τη δήλωση περιστατικού.

5. ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΒΛΗΜΑΤΩΝ

Αυτή η διαδικασία πρέπει να ακολουθείται όποτε εντοπίζεται ένα πρόβλημα, το οποίο δρομολογεί την έναρξη διαδικασίας διαχείρισης προβλημάτων. Η διαχείριση προβλημάτων εστιάζεται στην ενίσχυση της ποιότητας και στη μείωση του αριθμού των περιστατικών. Ένα πρόβλημα μπορεί να είναι αιτία ενός ή περισσότερων περιστατικών. Όταν δηλώνεται περιστατικό, ο στόχος της διαχείρισης προβλημάτων είναι να αποκαταστήσει την υπηρεσία το συντομότερο δυνατόν, πιθανώς μέσω μεθόδων που παρακάμπτουν το πρόβλημα. Όταν προκύπτει ένα πρόβλημα, στόχος είναι να διερευνηθεί η βασική αιτία του, ώστε να προσδιοριστεί κάποια αλλαγή που θα εξασφαλίσει ότι το συγκεκριμένο πρόβλημα και τα συναφή μ' αυτό περιστατικά δεν θα προκύψουν εκ νέου.

5.1. Προσδιορισμός και καταγραφή του προβλήματος

Το σημείο επαφής για ό,τι αφορά ένα συγκεκριμένο πρόβλημα είναι είτε η υπηρεσία υποστήριξης της ΕΕ είτε η υπηρεσία υποστήριξης της Ελβετίας, ανάλογα με το ποιο είναι το συμβαλλόμενο μέρος που δήλωσε την ύπαρξη προβλήματος.

Ο μοναδικός αναγνωριστικός κωδικός ενός προβλήματος είναι ο κωδικός που αποδίδεται από την ομάδα διαχείρισης υπηρεσιών ΤΠ (ITSM). Πρέπει να χρησιμοποιείται σε κάθε επικοινωνία σχετικά με το πρόβλημα αυτό.

Η διαδικασία διαχείρισης προβλημάτων μπορεί να ξεκινήσει από ένα περιστατικό ή να δρομολογηθεί εσκεμμένα με σκοπό την επίλυση ζητημάτων που εντοπίζονται στο σύστημα οποιαδήποτε χρονική στιγμή.

5.2. Κατάταξη των προβλημάτων ανά προτεραιότητα

Τα προβλήματα μπορούν να καταταγούν σε κατηγορίες ανάλογα με τη σοβαρότητα και την προτεραιότητά τους, κατά τον ίδιο τρόπο όπως και τα περιστατικά, ώστε να διευκολύνεται η παρακολούθησή τους· για τον σκοπό αυτόν, πρέπει να λαμβάνονται υπόψη ο αντίκτυπος των περιστατικών που συνδέονται μ' αυτά και η συχνότητα εμφάνισής τους.

5.3. Διερεύνηση και διάγνωση προβλημάτων

Κάθε συμβαλλόμενο μέρος μπορεί να δηλώσει ένα πρόβλημα και η υπηρεσία υποστήριξης του μέρους που έκανε τη δήλωση θα είναι υπεύθυνη για την καταγραφή του προβλήματος, την ανάθεσή του στον κατάλληλο πόρο και την παρακολούθηση της συνολικής κατάστασης όσον αφορά το πρόβλημα.

Η ομάδα επίλυσης στην οποία ανατέθηκε τελικά το πρόβλημα είναι υπεύθυνη για την έγκαιρη διευθέτησή του και για την επικοινωνία με την υπηρεσία υποστήριξης.

Κατόπιν αιτήματος, και τα δύο συμβαλλόμενα μέρη έχουν την ευθύνη να εξασφαλίσουν ότι εκτελούνται οι ανατεθείσες ενέργειες και να παράσχουν ανατροφοδότηση στη δική τους υπηρεσία υποστήριξης.

5.4. Επίλυση

Η ομάδα επίλυσης στην οποία ανατέθηκε τελικά το πρόβλημα είναι υπεύθυνη για την επίλυσή του και για την παροχή των σχετικών πληροφοριών στο γραφείο υποστήριξης του δικού της συμβαλλόμενου μέρους.

Τα πορίσματα που εξάγονται από την επεξεργασία του προβλήματος πρέπει να καταγράφονται για μελλοντική χρήση.

5.5. Κλείσιμο του προβλήματος

Ένα πρόβλημα κλείνει επισήμως όταν αποκατασταθεί με την υλοποίηση της αλλαγής. Το κλείσιμο του προβλήματος εκτελείται από την υπηρεσία υποστήριξης που κατέγραψε το πρόβλημα και ενημέρωσε την υπηρεσία υποστήριξης του άλλου συμβαλλόμενου μέρους.

6. ΙΚΑΝΟΠΟΙΗΣΗ ΑΙΤΗΜΑΤΩΝ

Η διαδικασία ικανοποίησης αιτημάτων είναι η διατερματική διαχείριση αιτήματος για νέα ή υπάρχουσα υπηρεσία, από τη στιγμή που το αίτημα καταγράφεται και εγκρίνεται έως το κλείσιμό του. Τα αιτήματα παροχής υπηρεσιών συνήθως είναι μικρά, προκαθορισμένα, επαναλαμβανόμενα, συχνά, προεγκεκριμένα και διαδικαστικά.

Τα κύρια βήματα που πρέπει να ακολουθούνται είναι τα ακόλουθα:

6.1. Υποβολή αιτήματος

Οι πληροφορίες που συνδέονται με αίτημα παροχής υπηρεσιών υποβάλλονται στην υπηρεσία υποστήριξης της ΕΕ ή της Ελβετίας με ηλεκτρονικό ταχυδρομείο, τηλέφωνο, μέσω του εργαλείου διαχείρισης υπηρεσιών (ITSM) ή οποιουδήποτε άλλου συμφωνημένου διαύλου επικοινωνίας.

6.2. Καταγραφή και ανάλυση του αιτήματος

Για όλα τα αιτήματα παροχής υπηρεσιών, το σημείο επαφής θα πρέπει να είναι η υπηρεσία υποστήριξης της ΕΕ ή της Ελβετίας, ανάλογα με το ποιο από τα συμβαλλόμενα μέρη υπέβαλε το συγκεκριμένο αίτημα. Αυτή η υπηρεσία υποστήριξης θα είναι υπεύθυνη για την καταγραφή και την ανάλυση του αιτήματος παροχής υπηρεσιών με την κατάλληλη επιμέλεια.

6.3. Έγκριση αιτήματος

Ο υπάλληλος της υπηρεσίας υποστήριξης του συμβαλλόμενου μέρους που υπέβαλε το αίτημα παροχής υπηρεσιών ελέγχει αν απαιτούνται τυχόν εγκρίσεις από το άλλο μέρος και, στην περίπτωση αυτή, ζητά τη χορήγησή τους. Εάν ένα αίτημα παροχής υπηρεσιών δεν εγκριθεί, η υπηρεσία υποστήριξης επικαιροποιεί και κλείνει το αίτημα.

6.4. Ικανοποίηση αιτήματος

Σ' αυτό το βήμα εξασφαλίζεται η αποτελεσματική και αποδοτική διεκπεραίωση των αιτημάτων παροχής υπηρεσιών. Πρέπει να γίνεται διάκριση μεταξύ των ακόλουθων περιπτώσεων:

- Η ικανοποίηση αιτήματος παροχής υπηρεσιών αφορά μόνο ένα συμβαλλόμενο μέρος. Σ' αυτή την περίπτωση, το εν λόγω μέρος εκδίδει τις οδηγίες εργασίας και συντονίζει την εκτέλεση της εργασίας.
- Η ικανοποίηση αιτήματος παροχής υπηρεσιών αφορά τόσο την ΕΕ όσο και την Ελβετία. Σ' αυτή την περίπτωση, οι υπηρεσίες υποστήριξης εκδίδουν τις οδηγίες εργασίας καθεμία στον τομέα της αρμοδιότητάς της. Την επεξεργασία του αιτήματος παροχής υπηρεσιών συντονίζουν μαζί και οι δύο υπηρεσίες υποστήριξης. Τη συνολική ευθύνη φέρει η υπηρεσία υποστήριξης που δέχθηκε και κατέγραψε το αίτημα παροχής υπηρεσιών.

Όταν ικανοποιηθεί το αίτημα παροχής υπηρεσιών, πρέπει να αρχειοθετείται στην κατηγορία «Επιλυθέντα».

6.5. Κλιμάκωση αιτήματος

Η υπηρεσία υποστήριξης μπορεί να παραπέμψει το εκκρεμές αίτημα παροχής υπηρεσιών στον κατάλληλο πόρο (τρίτο μέρος) εάν χρειάζεται.

Οι κλιμακούμενες παραπομπές γίνονται προς το αντίστοιχο τρίτο μέρος, δηλ. η υπηρεσία υποστήριξης της ΕΕ πρέπει να παραπέμπει το αίτημα σε τρίτο μέρος της Ελβετίας, πάντα με τη μεσολάβηση της υπηρεσίας υποστήριξης της Ελβετίας, και αντιστρόφως.

Το τρίτο μέρος στο οποίο ανατέθηκε τελικά το αίτημα παροχής υπηρεσιών είναι υπεύθυνο για την έγκαιρη διευθέτησή του και για την επικοινωνία με την υπηρεσία υποστήριξης που το παρέπεμψε.

Η υπηρεσία υποστήριξης που κατέγραψε το αίτημα παροχής υπηρεσιών είναι υπεύθυνη για την παρακολούθηση της συνολικής κατάστασης και της ανάθεσής του.

6.6. Επανεξέταση της ικανοποίησης του αιτήματος

Η υπεύθυνη υπηρεσία υποστήριξης υποβάλλει το αρχείο του αιτήματος παροχής υπηρεσιών σε τελικό έλεγχο ποιότητας πριν από το κλείσιμό του. Σκοπός είναι να εξασφαλιστεί ότι το αίτημα παροχής υπηρεσιών έχει όντως διεκπεραιωθεί και ότι όλες οι πληροφορίες που απαιτούνται για την περιγραφή του κύκλου ζωής του αιτήματος παρέχονται με επαρκή λεπτομέρεια. Επιπλέον, τα πορίσματα που εξάγονται από την επεξεργασία του αιτήματος πρέπει να καταγράφονται για μελλοντική χρήση.

6.7. Κλείσιμο του αιτήματος

Εάν τα μέρη στα οποία έχει ανατεθεί το αίτημα συμφωνούν ότι αυτό έχει ικανοποιηθεί και ο χρήστης που το υπέβαλε κρίνει ότι η παρεχόμενη υπηρεσία έχει ολοκληρωθεί, τότε το αίτημα αρχειοθετείται στην κατηγορία «Κλεισμένα».

Ένα αίτημα παροχής υπηρεσιών κλείνει επισήμως όταν η υπηρεσία υποστήριξης που κατέγραψε το εν λόγω αίτημα έχει ολοκληρώσει τη διαδικασία κλεισίματος και έχει ενημερώσει την υπηρεσία υποστήριξης του άλλου συμβαλλόμενου μέρους.

7. ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ

Στόχος είναι να εξασφαλιστεί ότι εφαρμόζονται τυποποιημένες μέθοδοι και διαδικασίες για την αποδοτική και έγκαιρη διεκπεραίωση όλων των αλλαγών που αφορούν την υποδομή ΤΠ, ώστε να ελαχιστοποιηθεί ο αριθμός και ο αντίκτυπος τυχόν σχετικών περιστατικών κατά την παροχή υπηρεσιών. Αλλαγές στην υποδομή ΤΠ μπορούν να προκύψουν ως αντίδραση σε προβλήματα ή σε απαιτήσεις που επιβάλλονται από το μη ηλεκτρονικό περιβάλλον —π.χ. νομοθετικές αλλαγές—, ή, προδραστικά, όταν επιδιώκεται η βελτίωση της αποτελεσματικότητας και της αποδοτικότητας ή η αποτύπωση επιχειρηματικών πρωτοβουλιών.

Η διαδικασία διαχείρισης αλλαγών περιλαμβάνει διάφορα βήματα, κατά τα οποία καταγράφεται κάθε λεπτομέρεια σχετικά με το αίτημα αλλαγής για σκοπούς μελλοντικής παρακολούθησης. Τα βήματα αυτά εξασφαλίζουν ότι η αλλαγή επικυρώνεται και δοκιμάζεται πριν από τη μετάβασή της στο στάδιο της πλήρους εγκατάστασης. Η διαδικασία διαχείρισης των εκδόσεων είναι υπεύθυνη για την επιτυχή εγκατάσταση της αλλαγής.

7.1. Αίτημα αλλαγής

Τα αιτήματα αλλαγής (RFC) υποβάλλονται στην ομάδα διαχείρισης των αλλαγών για επικύρωση και έγκριση. Για όλα τα αιτήματα αλλαγής, το σημείο επαφής θα πρέπει να είναι η υπηρεσία υποστήριξης της ΕΕ ή της Ελβετίας, ανάλογα με το ποιο από τα συμβαλλόμενα μέρη υπέβαλε το συγκεκριμένο αίτημα. Αυτή η υπηρεσία υποστήριξης θα είναι υπεύθυνη για την καταγραφή και την ανάλυση του αιτήματος με την κατάλληλη επιμέλεια.

Τα αιτήματα αλλαγής μπορεί να προκύψουν λόγω:

- περιστατικού που επέφερε κάποια αλλαγή·
- υπάρχοντος προβλήματος που έχει ως αποτέλεσμα κάποια αλλαγή·
- τελικού χρήστη που ζητά νέα αλλαγή·
- αλλαγή ως απόρροια συνεχιζόμενης συντήρησης·
- νομοθετική αλλαγή.

7.2. Αξιολόγηση και προγραμματισμός αλλαγής

Σ’ αυτό το στάδιο πραγματοποιούνται δραστηριότητες εκτίμησης και προγραμματισμού. Μεταξύ αυτών συγκαταλέγονται η απόδοση προτεραιότητας και ο προγραμματισμός έτσι ώστε να ελαχιστοποιηθούν οι κίνδυνοι και οι επιπτώσεις.

Εάν η διεκπεραίωση των αιτημάτων αλλαγής επηρεάζει τόσο την ΕΕ όσο και την Ελβετία, το συμβαλλόμενο μέρος που κατέγραψε ένα συγκεκριμένο αίτημα αλλαγής επαληθεύει την αξιολόγηση και τον προγραμματισμό της αλλαγής με το άλλο μέρος.

7.3. Εγκρίσεις αλλαγής

Κάθε καταγεγραμμένο αίτημα αλλαγής πρέπει να εγκρίνεται από το σχετικό επίπεδο κλιμάκωσης.

7.4. Υλοποίηση της αλλαγής

Η υλοποίηση της αλλαγής γίνεται μέσω της διαδικασίας διαχείρισης των εκδόσεων. Οι ομάδες διαχείρισης εκδόσεων και των δύο συμβαλλόμενων μερών ακολουθούν τις δικές τους διαδικασίες που περιλαμβάνουν τον προγραμματισμό και τις δοκιμές. Όταν ολοκληρωθεί η υλοποίηση της αλλαγής πραγματοποιείται επανεξέταση. Η υπάρχουσα διαδικασία διαχείρισης αλλαγών

επανεξετάζεται και επικαιροποιείται διαρκώς, ανάλογα με τις ανάγκες, ώστε να εξασφαλίζεται ότι όλα έχουν προχωρήσει σύμφωνα με το σχέδιο.

8. ΔΙΑΧΕΙΡΙΣΗ ΕΚΔΟΣΕΩΝ

Μια έκδοση συνίσταται σε μία ή περισσότερες αλλαγές υπηρεσίας ΤΠ, οι οποίες έχουν συγκεντρωθεί σ' ένα σχέδιο έκδοσης και θα πρέπει να εγκριθούν, να προετοιμαστούν, να υλοποιηθούν, να δοκιμαστούν και να εγκατασταθούν ταυτόχρονα. Μια έκδοση μπορεί να αποτελείται από διόρθωση σφάλματος προγραμματισμού, αλλαγή του υλισμικού ή άλλων δομικών συστατικών, αλλαγές λογισμικού, αναβαθμίσεις των εκδόσεων μιας εφαρμογής, αλλαγές στην τεκμηρίωση και/ή σε διαδικασίες. Το περιεχόμενο κάθε έκδοσης διεκπεραιώνεται, δοκιμάζεται και εγκαθίσταται ως ενιαία οντότητα.

Η διαχείριση εκδόσεων αποσκοπεί στον προγραμματισμό, την οικοδόμηση, τη διενέργεια δοκιμών και την επικύρωση, καθώς και στην ικανότητα παροχής των σχεδιασμένων υπηρεσιών, οι οποίες θα ικανοποιούν τις απαιτήσεις των ενδιαφερομένων και θα επιτυγχάνουν τους επιδιωκόμενους στόχους. Τα κριτήρια αποδοχής για όλες τις αλλαγές στην υπηρεσία θα καθορίζονται και θα τεκμηριώνονται κατά τον συντονισμό του σχεδιασμού και θα παρέχονται στις ομάδες διαχείρισης εκδόσεων.

Κατά κανόνα, η έκδοση αποτελείται από διάφορες διορθώσεις προβλημάτων και βελτιώσεις μιας υπηρεσίας. Περιέχει το νέο ή τροποποιημένο λογισμικό που απαιτείται και το τυχόν νέο ή τροποποιημένο υλισμικό που χρειάζεται για την υλοποίηση των εγκεκριμένων αλλαγών.

8.1. Προγραμματισμός της έκδοσης

Κατά το πρώτο βήμα της διαδικασίας οι εγκεκριμένες αλλαγές κατανέμονται σε πακέτα εκδόσεων και καθορίζεται το εύρος του πεδίου και το περιεχόμενο των εκδόσεων. Βάσει αυτών των πληροφοριών, καταρτίζεται χρονοδιάγραμμα, στο πλαίσιο της επιμέρους διαδικασίας του προγραμματισμού της έκδοσης, για την οικοδόμηση, δοκιμή και εγκατάσταση της έκδοσης.

Στον προγραμματισμό θα πρέπει να καθορίζονται τα εξής:

- Το εύρος του πεδίου και το περιεχόμενο της έκδοσης·
- Η εκτίμηση και τα χαρακτηριστικά του κινδύνου που συνδέεται με την έκδοση·
- Οι πελάτες/χρήστες που επηρεάζονται από την έκδοση·
- Η ομάδα που είναι υπεύθυνη για την έκδοση·
- Η στρατηγική παράδοσης και εγκατάστασης·
- Οι πόροι για την έκδοση και την εγκατάστασή της.

Τα δύο συμβαλλόμενα μέρη αλληλοενημερώνονται σχετικά με το χρονικό περιθώριο που έχουν ορίσει για τον προγραμματισμό της έκδοσης και τη συντήρηση. Εάν μια έκδοση επηρεάζει τόσο την ΕΕ όσο και την Ελβετία, τότε αυτές συντονίζουν το χρονοδιάγραμμα και καθορίζουν κοινό χρονικό περιθώριο για τη συντήρηση.

8.2. Οικοδόμηση και δοκιμή του πακέτου της έκδοσης

Το στάδιο της οικοδόμησης και της δοκιμής της διαδικασίας διαχείρισης των εκδόσεων συνίσταται στην εκτέλεση μια έκδοσης ή ενός πακέτου εκδόσεων και στη διατήρηση ελεγχόμενου περιβάλλοντος πριν από κάθε αλλαγή της παραγωγής, καθώς και στη δοκιμή όλων των αλλαγών σε όλα τα περιβάλλοντα που περιλαμβάνονται στη νέα έκδοση.

Εάν μια έκδοση επηρεάζει τόσο την ΕΕ όσο και την Ελβετία, τότε αυτές συντονίζουν τα σχεδιαγράμματα παράδοσης και τις δοκιμές. Αυτό περιλαμβάνει τις ακόλουθες πτυχές:

- Πότε και πώς θα παραδοθούν οι μονάδες της έκδοσης και οι συνιστώσες της υπηρεσίας·
- Ποιοι είναι οι τυπικοί χρόνοι παράδοσης· Τι συμβαίνει σε περίπτωση καθυστέρησης·
- Πώς να καταγραφεί η πρόοδος της παράδοσης και να επιτευχθεί η επιβεβαίωση·
- Μετρήσεις για την παρακολούθηση και τον προσδιορισμό της επιτυχίας των προσπαθειών για την εγκατάσταση της έκδοσης·
- Κοινές περιπτώσεις δοκιμών για τις σχετικές λειτουργίες και τις αλλαγές.

Στο τέλος αυτής της επιμέρους διαδικασίας, όλες οι απαιτούμενες συνιστώσες της έκδοσης είναι έτοιμες για το στάδιο της εγκατάστασης.

8.3. Προετοιμασία της εγκατάστασης

Με την επιμέρους διαδικασία προετοιμασίας εξασφαλίζεται, αφενός, ότι τα σχέδια επικοινωνίας καθορίζονται σωστά και ότι είναι έτοιμες οι κοινοποιήσεις που θα σταλούν σε όλους τους ενδιαφερομένους και τους τελικούς χρήστες, και, αφετέρου, ότι η έκδοση εντάσσεται στο πλαίσιο της διαδικασίας διαχείρισης αλλαγών, έτσι ώστε όλες οι αλλαγές να εφαρμόζονται με ελεγχόμενο τρόπο και να εγκρίνονται από τα απαιτούμενα φόρουμ.

Εάν μια έκδοση επηρεάζει τόσο την ΕΕ όσο και την Ελβετία, τότε αυτές συντονίζουν τις ακόλουθες δραστηριότητες:

- Καταγραφή του αιτήματος αλλαγής με σκοπό τον προγραμματισμό και την προετοιμασία της εγκατάστασης στο περιβάλλον παραγωγής·
- Κατάρτιση σχεδίου υλοποίησης·
- Πρόβλεψη για επαναφορά στην προηγούμενη έκδοση, σε περίπτωση αποτυχίας κατά την εγκατάσταση·
- Κοινοποιήσεις που θα αποσταλούν σε όλα τα ενδιαφερόμενα μέρη·
- Αίτημα έγκρισης για την υλοποίηση της έκδοσης από το κατάλληλο επίπεδο κλιμάκωσης.

8.4. Επαναφορά στην προηγούμενη έκδοση

Στην περίπτωση που η εγκατάσταση αποτύχει ή οι δοκιμές εντοπίσουν ότι η εγκατάσταση ήταν ανεπιτυχής ή ότι δεν ικανοποιεί τα συμφωνημένα κριτήρια αποδοχής/ποιότητας, οι ομάδες διαχείρισης εκδόσεων και των δύο συμβαλλόμενων μερών θα πρέπει να επαναφέρουν το λογισμικό στην προηγούμενη έκδοσή του. Θα πρέπει να ενημερωθούν όλοι οι απαραίτητοι ενδιαφερόμενοι, μεταξύ των οποίων και οι θιγόμενοι/στοχευόμενοι τελικοί χρήστες. Εν αναμονή έγκρισης, η διαδικασία μπορεί να αρχίσει εκ νέου σε οποιοδήποτε από τα προηγούμενα στάδια.

8.5. Επανεξέταση και κλείσιμο έκδοσης

Η επανεξέταση μιας εγκατάστασης πρέπει να περιλαμβάνει τις ακόλουθες δραστηριότητες:

- Καταγραφή της ανατροφοδότησης σχετικά με την ικανοποίηση των πελατών, των χρηστών και την παράδοση της υπηρεσίας (συλλογή των πληροφοριών και αξιοποίησή τους για συνεχή βελτίωση της υπηρεσίας)·
- Επανεξέταση τυχόν κριτηρίων ποιότητας που δεν ικανοποιήθηκαν·
- Έλεγχος ότι έχουν ολοκληρωθεί όλες οι ενέργειες, οι απαραίτητες διορθώσεις και οι αλλαγές·
- Εξασφάλιση ότι δεν υπάρχουν ζητήματα ικανότητας, πόρων, επάρκειας ή επιδόσεων στο τέλος της εγκατάστασης·

- Έλεγχος ότι τυχόν προβλήματα, γνωστά σφάλματα και εναλλακτικές λύσεις έχουν τεκμηριωθεί και γίνει δεκτά από τον πελάτη, τους τελικούς χρήστες, την επιχειρησιακή υποστήριξη και τα άλλα εμπλεκόμενα μέρη·
- Παρακολούθηση περιστατικών και προβλημάτων που προκαλούνται από την εγκατάσταση (πρέπει να παρασχεθεί έγκαιρη εργασιακή υποστήριξη στις επιχειρησιακές ομάδες στην περίπτωση που η έκδοση έχει προκαλέσει αύξηση του όγκου εργασίας)·
- Επικαιροποίηση των υποστηρικτικών εγγράφων τεκμηρίωσης (π.χ. των εγγράφων τεχνικής πληροφόρησης)·
- Επίσημη μεταβίβαση της εγκατεστημένης έκδοσης στην επιχειρησιακή υπηρεσία·
- Καταγραφή των διδαγμάτων που αποκομίστηκαν·
- Συλλογή του εγγράφου συνοπτικής περιγραφής της έκδοσης από τις ομάδες υλοποίησης·
- Επίσημο κλείσιμο της έκδοσης ύστερα από την επαλήθευση της καταγραφής του αιτήματος αλλαγής.

9. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η διαχείριση των περιστατικών ασφάλειας είναι διαδικασία για την αντιμετώπιση περιστατικών ασφάλειας έτσι ώστε να καταστεί δυνατή η επικοινωνία με τους δυνητικά πληγέντες ενδιαφερομένους· η αξιολόγηση του περιστατικού και η απόδοση προτεραιότητας· και η διευθέτηση τυχόν πραγματικής, εικαζόμενης ή δυνητικής παραβίασης της εμπιστευτικότητας, της διαθεσιμότητας ή της ακεραιότητας των ευαίσθητων πληροφορικών πόρων.

9.1. Κατάταξη περιστατικών ασφάλειας πληροφοριών

Όλα τα περιστατικά που επηρεάζουν τη σύνδεση μεταξύ του ενωσιακού μητρώου και του ελβετικού μητρώου πρέπει να αναλύονται, ώστε να εντοπίζεται πιθανή παραβίαση της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας κάθε ευαίσθητης πληροφορίας που έχει καταγραφεί στον κατάλογο ευαίσθητων πληροφοριών (SIL).

Εάν υπάρχει παραβίαση, το περιστατικό πρέπει να χαρακτηρίζεται ως περιστατικό ασφάλειας πληροφοριών, να καταχωρίζεται αμέσως στο εργαλείο διαχείρισης υπηρεσιών (ITSM) και να αντιμετωπίζεται ως τέτοιο.

9.2. Διαχείριση περιστατικών ασφάλειας πληροφοριών

Τα περιστατικά ασφάλειας τίθενται υπό την ευθύνη του τρίτου επιπέδου κλιμάκωσης, ενώ η επίλυσή τους διεκπεραιώνεται από ειδική ομάδα διαχείρισης περιστατικών (ΟΔΠ).

Η ΟΔΠ είναι υπεύθυνη για τα εξής:

- Τη διενέργεια μιας πρώτης ανάλυσης, την κατάταξη και την εκτίμηση της σοβαρότητας του περιστατικού·
- Τον συντονισμό των ενεργειών μεταξύ όλων των ενδιαφερομένων· μεταξύ αυτών συγκαταλέγονται η πλήρης τεκμηρίωση της ανάλυσης του περιστατικού, οι αποφάσεις που λαμβάνονται για την αντιμετώπισή του και πιθανές εντοπιζόμενες αδυναμίες·
- Την έγκαιρη παραπομπή στο κατάλληλο επίπεδο, ανάλογα με τη σοβαρότητα του περιστατικού ασφάλειας, προς ενημέρωση και/ή απόφαση.

Κατά τη διαδικασία διαχείρισης της ασφάλειας των πληροφοριών, όλες οι πληροφορίες που αφορούν περιστατικά διαβαθμίζονται στο υψηλότερο επίπεδο ευαισθησίας των πληροφοριών, και σε καμία περίπτωση χαμηλότερα από το επίπεδο SENSITIVE. *ΣΕΔΕ*.

Για τις έρευνες που βρίσκονται σε εξέλιξη και/ή για αδυναμία που θα μπορούσε να αποτελέσει αντικείμενο εκμετάλλευσης, και μέχρι την αποκατάστασή της, οι πληροφορίες πρέπει να διαβαθμίζονται ως SPECIAL HANDLING: *ETS Critical*.

9.3. Αναγνώριση περιστατικών ασφάλειας

Βάσει του είδους του περιστατικού ασφάλειας, ο υπεύθυνος ασφάλειας πληροφοριών καθορίζει τις κατάλληλες οργανώσεις που πρέπει να συμμετέχουν αποτελώντας μέρος της ΟΔΠ.

9.4. Ανάλυση περιστατικών ασφάλειας

Η ΟΔΠ συνεργάζεται με όλες τις συμμετέχουσες οργανώσεις και με τα αρμόδια μέλη των ομάδων τους, κατά περίπτωση, για να επανεξετάσει το περιστατικό. Κατά την ανάλυση, προσδιορίζεται η έκταση της απώλειας όσον αφορά την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα του πληροφορικού πόρου, και εκτιμούνται οι επιπτώσεις για όλες της πληγείσες οργανώσεις. Στη συνέχεια, καθορίζονται οι αρχικές και οι επακόλουθες ενέργειες για την επίλυση του περιστατικού και τη διαχείριση του αντικτύπου του, συμπεριλαμβανομένου του αντικτύπου των εν λόγω ενεργειών όσον αφορά τους πόρους.

9.5. Εκτίμηση της σοβαρότητας περιστατικού ασφάλειας, κλιμάκωση και υποβολή εκθέσεων

Η ΟΔΠ εκτιμά τη σοβαρότητα κάθε νέου περιστατικού ασφάλειας μετά τον χαρακτηρισμό του ως περιστατικό ασφάλειας και προβαίνει στις άμεσες ενέργειες που απαιτούνται ανάλογα με τη σοβαρότητα του περιστατικού.

9.6. Υποβολή εκθέσεων σχετικά με την αντιμετώπιση περιστατικών ασφάλειας

Η ΟΔΠ, στην έκθεση που υποβάλλει σχετικά με την αντιμετώπιση του περιστατικό ασφάλειας πληροφοριών, περιλαμβάνει την ανάσχεση του περιστατικού και τα αποτελέσματα της ανάκαμψης. Η έκθεση διαβιβάζεται στο τρίτο επίπεδο κλιμάκωσης μέσω ασφαλούς ηλεκτρονικού ταχυδρομείου ή άλλων αμοιβαία αποδεκτών μέσων ασφαλούς επικοινωνίας.

Το υπεύθυνο συμβαλλόμενο μέρος εξετάζει τα αποτελέσματα της ανάσχεσης και της ανάκαμψης και:

- επανασυνδέει το μητρώο, σε περίπτωση προηγούμενης αποσύνδεσης·
- παρέχει πληροφορίες σχετικά με το περιστατικό στις ομάδες των μητρώων·
- κλείνει το περιστατικό.

Η ΟΔΠ θα πρέπει να περιλαμβάνει —κατά τρόπο ασφαλή— τις σχετικές λεπτομέρειες στην έκθεσή της για το περιστατικό ασφάλειας των πληροφοριών, ώστε να εξασφαλίζεται η συνεπής καταγραφή και επικοινωνία και να γίνεται δυνατή η άμεση και κατάλληλη δράση για την ανάσχεση του περιστατικού. Μετά την ολοκλήρωσή του, η ΟΔΠ υποβάλλει την τελική έκθεση για το περιστατικό ασφάλειας πληροφοριών σε εύθετο χρόνο.

9.7. Παρακολούθηση, δημιουργία ικανοτήτων και συνεχής βελτίωση

Η ΟΔΠ υποβάλλει εκθέσεις για όλα τα περιστατικά ασφάλειας στο τρίτο επίπεδο κλιμάκωσης. Οι εκθέσεις χρησιμοποιούνται από αυτό το επίπεδο κλιμάκωσης για να καθοριστούν τα εξής:

- Αδύνατα σημεία όσον αφορά τους ελέγχους ασφάλειας και/ή τη λειτουργία, τα οποία πρέπει να ενισχυθούν·

- Ενδεχόμενη ανάγκη ενίσχυσης αυτής της διαδικασίας, ώστε να βελτιωθεί η αποτελεσματικότητα της αντιμετώπισης των περιστατικών·
- Ευκαιρίες για επιμόρφωση και δημιουργία ικανοτήτων, ώστε να ενισχυθεί περαιτέρω η ανθεκτικότητα των συστημάτων μητρώων όσον αφορά την ασφάλεια πληροφοριών, να μειωθεί ο κίνδυνος μελλοντικών περιστατικών και να ελαχιστοποιηθεί ο αντίκτυπός τους.

10. ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η διαχείριση της ασφάλειας των πληροφοριών αποσκοπεί στο να εξασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των διαβαθμισμένων πληροφοριών, δεδομένων και υπηρεσιών ΤΠ ενός φορέα. Πέρα από τις τεχνικές συνιστώσες, στις οποίες συμπεριλαμβάνονται ο σχεδιασμός τους και η διενέργεια δοκιμών (βλ. τα ΤΠΣ), είναι αναγκαίες οι ακόλουθες κοινές επιχειρησιακές διαδικασίες ώστε να ικανοποιηθούν οι απαιτήσεις ασφάλειας για τη μόνιμη σύνδεση των μητρώων.

10.1. Αναγνώριση των ευαίσθητων πληροφοριών

Για να εκτιμηθεί ο ευαίσθητος χαρακτήρας μιας πληροφορίας, καθορίζεται το επίπεδο του αντικτύπου που θα μπορούσε να έχει μια παραβίαση της ασφάλειας —η οποία σχετίζεται με την εν λόγω πληροφορία— στην επιχείρηση (π.χ. οικονομική ζημία, υποβάθμιση εικόνας, παράβαση της νομοθεσίας κ.λπ.).

Οι ευαίσθητοι πληροφορικοί πόροι αναγνωρίζονται με βάση τον αντίκτυπό τους στη σύνδεση.

Το επίπεδο ευαισθησίας της εκάστοτε πληροφορίας εκτιμάται σύμφωνα με την κλίμακα ευαισθησίας που εφαρμόζεται για τη σύνδεση και περιγράφεται λεπτομερώς στην ενότητα «Διαχείριση περιστατικών ασφάλειας πληροφοριών» του παρόντος εγγράφου.

10.2. Επίπεδα ευαισθησίας των πληροφορικών πόρων

Μόλις αναγνωριστεί ο πληροφορικός πόρος, διαβαθμίζεται με βάση τους ακόλουθους κανόνες:

- Εάν προσδιοριστεί έστω και μόνο ένα επίπεδο HIGH όσον αφορά την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα, ο πληροφορικός πόρος διαβαθμίζεται ως SPECIAL HANDLING: *ETS Critical*
- Εάν προσδιοριστεί έστω και μόνο ένα επίπεδο MEDIUM όσον αφορά την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα, ο πληροφορικός πόρος διαβαθμίζεται ως SENSITIVE: *ETS*
- Εάν προσδιοριστεί μόνο επίπεδο LOW όσον αφορά την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα, ο πληροφορικός πόρος διαβαθμίζεται ως Marking EU**:** SENSITIVE: *ETS Joint Procurement.* Χαρακτηρισμός CH: LIMITED: ETS.

10.3. Καθορισμός του ιδιοκτήτη των πληροφορικών πόρων

Όλοι οι πληροφορικοί πόροι πρέπει να έχουν έναν καθορισμένο ιδιοκτήτη. Οι πληροφορικοί πόροι του ΣΕΔΕ, οι οποίοι ανήκουν στη σύνδεση μεταξύ του EUTL και του SSTL ή συνδέονται με αυτήν, θα πρέπει να περιλαμβάνονται σε κοινό κατάλογο απογραφής πόρων, τηρούμενο και από τα δύο συμβαλλόμενα μέρη. Οι πληροφορικοί πόροι του ΣΕΔΕ, πέραν της σύνδεσης μεταξύ του EUTL και του SSTL θα πρέπει να περιλαμβάνονται σε κατάλογο απογραφής πόρων, τηρούμενο από το αντίστοιχο συμβαλλόμενο μέρος.

Η ιδιοκτησία κάθε πληροφορικού πόρου που ανήκει στη σύνδεση μεταξύ του EUTL και του SSTL, ή που συνδέεται με αυτήν, πρέπει να συμφωνείται από τα συμβαλλόμενα μέρη. Ο ιδιοκτήτης ενός πληροφορικού πόρου είναι υπεύθυνος για την εκτίμηση της ευαισθησίας του.

Ο ιδιοκτήτης θα πρέπει να διαθέτει το κατάλληλο επίπεδο αρχαιότητας για την αξία του πόρου / των πόρων που του έχει/-ουν ανατεθεί. Θα πρέπει να συμφωνηθεί και να επισημοποιηθεί η ευθύνη του ιδιοκτήτη για τον πόρο ή τους πόρους, καθώς και η υποχρέωσή του/της να διατηρεί το απαιτούμενο επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

10.4. Καταχώριση ευαίσθητων πληροφοριών

Όλες οι ευαίσθητες πληροφορίες καταχωρίζονται στον κατάλογο ευαίσθητων πληροφοριών (SIL).

Όπου είναι σκόπιμο, θα πρέπει να λαμβάνεται υπόψη η συγκέντρωση ευαίσθητων πληροφοριών που θα μπορούσε να έχει μεγαλύτερο αντίκτυπο από εκείνον που θα είχε μία μεμονωμένη πληροφορία, και να καταχωρίζεται στον SIL (π.χ. σειρά πληροφοριών που αποθηκεύεται στη βάση δεδομένων του συστήματος).

Ο SIL δεν είναι στατικός. Οι απειλές, τα ευάλωτα σημεία, η πιθανότητα ή οι συνέπειες των περιστατικών ασφάλειας που συνδέονται με τους πληροφορικούς πόρους μπορούν να μεταβληθούν χωρίς καμία ένδειξη, όπως επίσης ενδέχεται να εισαχθούν νέοι πληροφορικοί πόροι στη λειτουργία των συστημάτων μητρώων.

Συνεπώς, ο SIL πρέπει να επανεξετάζεται τακτικά και να καταχωρίζεται αμέσως κάθε νέα πληροφορία που αναγνωρίζεται ως ευαίσθητη.

Ο SIL πρέπει να περιέχει τουλάχιστον τις ακόλουθες πληροφορίες για κάθε καταχώριση:

- Περιγραφή της πληροφορίας
- Ιδιοκτήτης της πληροφορίας
- Επίπεδο ευαισθησίας
- Ένδειξη του κατά πόσον η πληροφορία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα
- Πρόσθετες πληροφορίες, εάν αυτό απαιτείται

10.5. Χειρισμός ευαίσθητων πληροφοριών

Όταν οι ευαίσθητες πληροφορίες υποβάλλονται σε επεξεργασία εκτός της σύνδεσης μεταξύ του ενωσιακού μητρώου και του ελβετικού μητρώου, ο χειρισμός τους πρέπει να ακολουθεί τις οδηγίες χειρισμού.

Ο χειρισμός των ευαίσθητων πληροφοριών που υποβάλλονται σε επεξεργασία στο πλαίσιο της σύνδεσης μεταξύ του ενωσιακού μητρώου και του ελβετικού μητρώου γίνεται σύμφωνα με τις απαιτήσεις ασφάλειας των συμβαλλόμενων μερών.

10.6. Διαχείριση πρόσβασης

Στόχος της διαχείρισης πρόσβασης είναι να παρέχει στους εξουσιοδοτημένους χρήστες το δικαίωμα να χρησιμοποιούν μια υπηρεσία, εμποδίζοντας παράλληλα την πρόσβαση για τους μη εξουσιοδοτημένους χρήστες. Η διαχείριση πρόσβασης καλείται μερικές φορές και «διαχείριση δικαιωμάτων» ή «διαχείριση ταυτότητας».

Για τη μόνιμη σύνδεση των μητρώων και τη λειτουργία της, και τα δύο συμβαλλόμενα μέρη χρειάζονται πρόσβαση στις ακόλουθες συνιστώσες:

- Wiki: συνεργατικό περιβάλλον για την ανταλλαγή κοινών πληροφοριών, όπως ο προγραμματισμός των εκδόσεων·
- εργαλείο διαχείρισης υπηρεσιών ΤΠ (ITSM) για τη διαχείριση των περιστατικών και των προβλημάτων (βλ. κεφάλαιο 3 «Προσέγγιση και πρότυπα»)·
- Σύστημα ανταλλαγής μηνυμάτων: κάθε συμβαλλόμενο μέρος παρέχει ένα ασφαλές σύστημα ανταλλαγής μηνυμάτων για τη διαβίβαση των μηνυμάτων που περιέχουν τα δεδομένα των συναλλαγών.

Ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής της Ένωσης εξασφαλίζουν ότι οι προσβάσεις είναι επικαιροποιημένες και λειτουργούν ως σημεία επαφής για το αντίστοιχο συμβαλλόμενο μέρος τους όσον αφορά τις δραστηριότητες διαχείρισης της πρόσβασης. Ο χειρισμός των αιτημάτων πρόσβασης γίνεται σύμφωνα με τις διαδικασίες ικανοποίησης αιτημάτων.

10.7. Διαχείριση πιστοποιητικών/κλειδιών

Κάθε συμβαλλόμενο μέρος είναι υπεύθυνο για τη διαχείριση του δικού του πιστοποιητικού / κλειδιού (παραγωγή, καταχώριση, αποθήκευση, εγκατάσταση, χρήση, ανανέωση, ανάκληση, δημιουργία εφεδρικού αντιγράφου και ανάκτηση πιστοποιητικών/κλειδιών). Όπως περιγράφεται στα τεχνικά πρότυπα σύνδεσης (ΤΠΣ), χρησιμοποιούνται μόνο ψηφιακά πιστοποιητικά που εκδίδονται από αρχή πιστοποίησης (ΑΠ) την οποία εμπιστεύονται και τα δύο συμβαλλόμενα μέρη. Ο χειρισμός και η αποθήκευση των πιστοποιητικών / των κλειδιών ακολουθεί τις διατάξεις που καθορίζονται στις οδηγίες χειρισμού.

Κάθε ανάκληση και/ή ανανέωση πιστοποιητικών και κλειδιών συντονίζεται και από τα δύο συμβαλλόμενα μέρη. Αυτό γίνεται σύμφωνα με τις διαδικασίες ικανοποίησης αιτημάτων.

Ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής της Ένωσης θα ανταλλάσσουν πιστοποιητικά / κλειδιά μέσω ασφαλών μέσων επικοινωνίας σύμφωνα με τις διατάξεις που καθορίζονται στις οδηγίες χειρισμού.

Κάθε επαλήθευση των πιστοποιητικών / των κλειδιών, με όποιον τρόπο και αν γίνεται μεταξύ των συμβαλλόμενων μερών, πραγματοποιείται εκτός ζώνης.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

ΤΕΧΝΙΚΑ ΠΡΟΤΥΠΑ ΣΥΝΔΕΣΗΣ (ΤΠΣ)

σύμφωνα με το άρθρο 3 παράγραφος 7 της συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας εκπομπών αερίων θερμοκηπίου

Πρότυπο για τη μόνιμη σύνδεση των μητρώων

Περιεχόμενα

1. Γλωσσάριο 10
2. Εισαγωγή 11
2.1. Πεδίο εφαρμογής 11
2.2. Αποδέκτες 12
3. Προσέγγιση και πρότυπα 12
4. Διαχείριση περιστατικών 13
4.1. Ανίχνευση και καταγραφή περιστατικών 13
4.2. Ταξινόμηση και αρχική υποστήριξη 14
4.3. Διερεύνηση και διάγνωση 14
4.4. Επίλυση και ανάκαμψη 15
4.5. Κλείσιμο του περιστατικού 15
5. Διαχείριση προβλημάτων 16
5.1. Προσδιορισμός και καταγραφή του προβλήματος 16
5.2. Κατάταξη των προβλημάτων ανά προτεραιότητα 16
5.3. Διερεύνηση και διάγνωση προβλημάτων 16
5.4. Επίλυση 16
5.5. Κλείσιμο του προβλήματος 17
6. Ικανοποίηση αιτημάτων 17
6.1. Υποβολή αιτήματος 17
6.2. Καταγραφή και ανάλυση του αιτήματος 17
6.3. Έγκριση αιτήματος 17
6.4. Ικανοποίηση αιτήματος 17
6.5. Κλιμάκωση αιτήματος 18
6.6. Επανεξέταση της ικανοποίησης του αιτήματος 18
6.7. Κλείσιμο του αιτήματος 18
7. Διαχείριση αλλαγών 19

7.1. Αίτημα αλλαγής 19
7.2. Αξιολόγηση και προγραμματισμός αλλαγής 19
7.3. Εγκρίσεις αλλαγής 19
7.4. Υλοποίηση της αλλαγής 19
8. Διαχείριση εκδόσεων 20
8.1. Προγραμματισμός της έκδοσης 20
8.2. Οικοδόμηση και δοκιμή του πακέτου της έκδοσης 20
8.3. Προετοιμασία της εγκατάστασης 21
8.4. Επαναφορά στην προηγούμενη έκδοση 21
8.5. Επανεξέταση και κλείσιμο έκδοσης 21
9. Διαχείριση περιστατικών ασφάλειας 22
9.1. Κατάταξη περιστατικών ασφάλειας πληροφοριών 22
9.2. Διαχείριση περιστατικών ασφάλειας πληροφοριών 22
9.3. Αναγνώριση περιστατικών ασφάλειας 23
9.4. Ανάλυση περιστατικών ασφάλειας 23
9.5. Εκτίμηση της σοβαρότητας περιστατικού ασφάλειας, κλιμάκωση και υποβολή εκθέσεων 23
9.6. Υποβολή εκθέσεων σχετικά με την αντιμετώπιση περιστατικών ασφάλειας 23
9.7. Παρακολούθηση, δημιουργία ικανοτήτων και συνεχής βελτίωση 23
10. Διαχείριση της ασφάλειας των πληροφοριών 24
10.1. Αναγνώριση των ευαίσθητων πληροφοριών 24
10.2. Επίπεδα ευαισθησίας των πληροφορικών πόρων 24
10.3. Καθορισμός του ιδιοκτήτη των πληροφορικών πόρων 24
10.4. Καταχώριση ευαίσθητων πληροφοριών 25
10.5. Χειρισμός ευαίσθητων πληροφοριών 25
10.6. Διαχείριση πρόσβασης 25
10.7. Διαχείριση πιστοποιητικών/κλειδιών 26
1. Γλωσσάριο 31
2. Εισαγωγή 34
2.1. Πεδίο εφαρμογής 35
2.2. Αποδέκτες 35
3. Γενικές διατάξεις 35
3.1. Αρχιτεκτονική της σύνδεσης επικοινωνίας 35

3.1.1. Ανταλλαγή μηνυμάτων 35
3.1.2. Μήνυμα XML — Περιγραφή υψηλού επιπέδου 36
3.1.3. Παράθυρα πρόσληψης (ingestion windows) 36
3.1.4. Ροές μηνυμάτων συναλλαγής 36
3.2. Ασφάλεια της μεταφοράς δεδομένων 39
3.2.1. Τείχος προστασίας και διασύνδεση δικτύων 40
3.2.2. Εικονικό ιδιωτικό δίκτυο (VPN) 40
3.2.3. Εφαρμογή της IPsec 40
3.2.4. Πρωτόκολλο ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων 40
3.2.5. Κρυπτογράφηση και υπογραφή XML 41
3.2.6. Κρυπτογραφικά κλειδιά 41
3.3. Κατάλογος λειτουργιών στο πλαίσιο της σύνδεσης 41
3.3.1. Συναλλαγές σχετικές με δραστηριότητες εμπορίας δικαιωμάτων εκπομπών 41
3.3.2. Πρωτόκολλο αντιπαραβολής 42
3.3.3. Δοκιμαστικό μήνυμα 42
3.4. Απαιτήσεις καταγραφής δεδομένων 43
3.5. Επιχειρησιακές απαιτήσεις 44
4. Διατάξεις περί διαθεσιμότητας 45
4.1. Σχεδιασμός της επικοινωνιακής διαθεσιμότητας 45
4.2. Αρχικοποίηση, επικοινωνία, επανενεργοποίηση και σχέδιο δοκιμών 45
4.2.1. Εσωτερικές δοκιμές υποδομής ΤΠΕ 46
4.2.2. Δοκιμές επικοινωνίας 46
4.2.3. Δοκιμές πλήρους συστήματος (διατερματικά) 46
4.2.4. Δοκιμές ασφαλείας 47
4.3. Περιβάλλοντα αποδοχής / δοκιμών 47
5. Διατάξεις για την εμπιστευτικότητα και την ακεραιότητα 48
5.1. Υποδομή για τους ελέγχους της ασφάλειας 48
5.2. Αναστολή της σύνδεσης και διατάξεις για την επανενεργοποίηση 48
5.3. Διατάξεις για την παραβίαση της ασφάλειας 49
5.4. Κατευθυντήριες γραμμές για τους ελέγχους της ασφάλειας 49
5.4.1. Λογισμικό 49
5.4.2. Υποδομές 50
5.5. Διατάξεις αξιολόγησης κινδύνου 50

1. ΓΛΩΣΣΑΡΙΟ

Πίνακας 1-1 Ακρωνύμια επιχειρησιακών δραστηριοτήτων και ορισμοί

Ακρωνύμιο/Όρος	Ορισμός
Δικαίωμα	Δικαίωμα εκπομπών ενός τόνου ισοδυνάμου διοξειδίου του άνθρακα κατά τη διάρκεια καθορισμένης περιόδου, το οποίο ισχύει μόνον για τους σκοπούς της τήρησης των απαιτήσεων του ΣΕΔΕ οποιασδήποτε οντότητας.
CH	Ελβετική Συνομοσπονδία
CHU	Είδος δικαιωμάτων εκπομπών από εγκαταστάσεις, που καλούνται επίσης CHU2 (αναφέρεται στην περίοδο δεσμεύσεων 2 του πρωτοκόλλου του Κιότο), που εκχωρούνται από την CH
CHUA	Δικαιώματα του κλάδου αερομεταφορών της Ελβετίας
ΚΕΔ	Κοινές επιχειρησιακές διαδικασίες. Διαδικασίες που έχουν αναπτυχθεί από κοινού για την επιχειρησιακή εφαρμογή της σύνδεσης μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας.
ΜΕΔΕ	Μητρώο Εμπορίας Δικαιωμάτων Εκπομπών
ΣΕΔΕ	Σύστημα Εμπορίας Δικαιωμάτων Εκπομπών
ΕΕ	Ευρωπαϊκή Ένωση
ΓΔΕΕ	Γενικά δικαιώματα της ΕΕ
ΔΚΑΕΕ	Δικαιώματα του κλάδου αερομεταφορών της ΕΕ
ΕΜΕΕ	Ενοποιημένο μητρώο της Ευρωπαϊκής Ένωσης
EUTL	Ημερολόγιο συναλλαγών της Ευρωπαϊκής Ένωσης
Μητρώο	Λογιστικό σύστημα για τα δικαιώματα που εκχωρούνται στο πλαίσιο του ΣΕΔΕ, το οποίο καταγράφει την κυριότητα των δικαιωμάτων που τηρούνται σε ηλεκτρονικούς λογαριασμούς.
SSTL	Συμπληρωματικό ημερολόγιο συναλλαγών της Ελβετίας
Συναλλαγή	Διαδικασία σε μητρώο που περιλαμβάνει τη μεταφορά δικαιώματος από έναν λογαριασμό σε άλλον.

Ακρωνύμιο/Όρος	Ορισμός
Σύστημα ημερολογίου συναλλαγών	Το ημερολόγιο συναλλαγών καταγράφει κάθε προτεινόμενη συναλλαγή που αποστέλλεται από το ένα μητρώο στο άλλο.

Πίνακας 1-2 Τεχνικά ακρωνύμια και ορισμοί

Ακρωνύμιο	Ορισμός
Ασύμμετρη κρυπτογράφηση	Χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.
Αρχή πιστοποίησης (ΑΠ)	Οντότητα που εκδίδει ψηφιακά πιστοποιητικά.
Κρυπτογραφικό κλειδί	Πληροφορία που καθορίζει τη λειτουργική παραγωγή ενός κρυπτογραφικού αλγορίθμου.
Αποκρυπτογράφηση	Αντίστροφη διαδικασία κρυπτογράφησης.
Ψηφιακή υπογραφή	Μαθηματική τεχνική που χρησιμοποιείται για τον έλεγχο της γνησιότητας και της ακεραιότητας μηνύματος, λογισμικού ή ψηφιακού εγγράφου.
Κρυπτογράφηση	Διαδικασία μετατροπής πληροφοριών ή δεδομένων σε κώδικα, ιδίως για την πρόληψη της άνευ αδείας πρόσβασης.
Πρόσληψη αρχείων (file ingestion)	Η διαδικασία ανάγνωσης ενός αρχείου.
Τείχος προστασίας (Firewall)	Συσκευή ή λογισμικό ασφάλειας δικτύου το οποίο παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κίνηση δικτύων βάσει προκαθορισμένων κανόνων.
Παρακολούθηση «χτύπων καρδιάς» (heartbeat)	Περιοδικό σήμα που δημιουργείται και παρακολουθείται από το υλισμικό ή το λογισμικό για την ένδειξη της κανονικής λειτουργίας ή για τον συγχρονισμό άλλων μερών του συστήματος ηλεκτρονικού υπολογιστή.
IPSEC	Ασφάλεια IP. Ακολουθία πρωτοκόλλου δικτύου, η οποία ελέγχει τη γνησιότητα και κρυπτογραφεί πακέτα δεδομένων με σκοπό την ασφαλή κρυπτοθετημένη επικοινωνία μεταξύ δύο υπολογιστών μέσω δικτύου πρωτοκόλλου διαδικτύου.
Δοκιμή διείσδυσης	Πρακτική της διεξαγωγής δοκιμών σε σύστημα ηλεκτρονικού υπολογιστή, δίκτυο ή διαδικτυακή εφαρμογή για να βρεθούν τα τρωτά σημεία στον τομέα της ασφάλειας που θα μπορούσαν να εκμεταλλευτούν οι επιτιθέμενοι.
Διαδικασία αντιπαραβολής	Διαδικασία με την οποία εξασφαλίζεται ότι δύο σειρές εγγραφών συμφωνούν μεταξύ τους.
VPN	Εικονικό ιδιωτικό δίκτυο (Virtual Private Network).

Ακρωνύμιο	Ορισμός
XML	Επεκτάσιμη γλώσσα σήμανσης (Extensible Mark-up Language). Επιτρέπει στους σχεδιαστές να δημιουργούν τις δικές τους εξατομικευμένες ετικέτες, ώστε να γίνεται δυνατός ο ορισμός, η διαβίβαση, η επικύρωση και η ερμηνεία των δεδομένων μεταξύ των εφαρμογών και μεταξύ των οργανισμών.

2. ΕΙΣΑΓΩΓΗ

Η συμφωνία της 23ης Νοεμβρίου 2017 μεταξύ της Ευρωπαϊκής Ένωσης και της Ελβετικής Συνομοσπονδίας για τη σύνδεση των συστημάτων τους εμπορίας δικαιωμάτων εκπομπών αερίων θερμοκηπίου (στο εξής: συμφωνία) προβλέπει την αμοιβαία αναγνώριση δικαιωμάτων εκπομπών τα οποία μπορούν να χρησιμοποιηθούν για συμμόρφωση στο πλαίσιο του συστήματος εμπορίας δικαιωμάτων εκπομπών της Ευρωπαϊκής Ένωσης (στο εξής: ΣΕΔΕ της ΕΕ) ή του συστήματος εμπορίας δικαιωμάτων εκπομπών της Ελβετίας (στο εξής: ΣΕΔΕ της Ελβετίας). Για να καταστεί λειτουργική η σύνδεση ανάμεσα στο ΣΕΔΕ της ΕΕ και το ΣΕΔΕ της Ελβετίας, εγκαθιδρύεται άμεση σύνδεση ανάμεσα στο ημερολόγιο συναλλαγών της ΕΕ (European Union Transaction Log – EUTL) του ενωσιακού μητρώου και στο ελβετικό συμπληρωματικό ημερολόγιο συναλλαγών (Swiss Supplementary Transaction Log – SSTL) του ελβετικού μητρώου, η οποία θα επιτρέψει τη μεταξύ των μητρώων μεταφορά δικαιωμάτων εκπομπών που εκχωρούνται από οποιοδήποτε εκ των δύο ΣΕΔΕ (άρθρο 3 παράγραφος 2 της συμφωνίας). Για να καταστεί λειτουργική η σύνδεση μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας, το 2020 εφαρμόστηκε προσωρινή λύση. Από το 2023 η σύνδεση των μητρώων μεταξύ των δύο συστημάτων εμπορίας δικαιωμάτων εκπομπών θα εξελιχθεί σταδιακά σε μόνιμη σύνδεση των μητρώων η οποία αναμένεται να υλοποιηθεί το αργότερο το 2024 και η οποία θα καταστήσει δυνατή τη λειτουργία των συνδεδεμένων αγορών όσον αφορά τα οφέλη από τη ρευστότητα της αγοράς και την εκτέλεση των συναλλαγών μεταξύ των δύο συνδεδεμένων συστημάτων κατά τρόπο που ισοδυναμεί με μία αγορά που αποτελείται από δύο συστήματα και επιτρέπει στους συμμετέχοντες στην αγορά να ενεργούν σαν να ήταν σε μία αγορά, με την επιφύλαξη μόνο των επιμέρους κανονιστικών διατάξεων των συμβαλλόμενων μερών (παράρτημα ΙΙ της συμφωνίας).

Σύμφωνα με το άρθρο 3 παράγραφος 7 της συμφωνίας, ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής του ενωσιακού μητρώου αναπτύσσουν τεχνικά πρότυπα σύνδεσης (στο εξής: ΤΠΣ) με βάση τις αρχές που ορίζονται στο παράρτημα ΙΙ της συμφωνίας, στα οποία περιγράφονται λεπτομερώς οι απαιτήσεις για τη θέσπιση αξιόπιστης και ασφαλούς σύνδεσης ανάμεσα στο SSTL και το EUTL. Τα ΤΠΣ που αναπτύσσουν οι διαχειριστές παράγουν αποτελέσματα αφού εγκριθούν με απόφαση της μεικτής επιτροπής.

Τα ΤΠΣ εγκρίθηκαν από τη μεικτή επιτροπή με την απόφαση αριθ. 2/2020. Τα επικαιροποιημένα ΤΠΣ, όπως καταγράφονται στο παρόν έγγραφο, πρόκειται να εγκριθούν από τη μεικτή επιτροπή με την απόφαση αριθ. 1/2024. Σύμφωνα με την παρούσα απόφαση και τα αιτήματα της μεικτής επιτροπής, ο διαχειριστής του ελβετικού μητρώου και ο κεντρικός διαχειριστής της Ένωσης έχουν αναπτύξει και θα επικαιροποιούν περαιτέρω τεχνικές κατευθυντήριες γραμμές ώστε να καταστεί λειτουργική η σύνδεση και να εξασφαλιστεί ότι αυτές οι κατευθυντήριες γραμμές προσαρμόζονται συνεχώς στην τεχνική πρόοδο και/ή στις νέες απαιτήσεις που αφορούν την ασφάλεια και την προστασία της σύνδεσης, καθώς και την αποτελεσματική και αποδοτική λειτουργία της.

2.1. Πεδίο εφαρμογής

Το παρόν έγγραφο αντιπροσωπεύει την κοινή αντίληψη μεταξύ των συμβαλλόμενων μερών της συμφωνίας όσον αφορά τη δημιουργία των τεχνικών θεμελίων της σύνδεσης των μητρώων του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας. Περιγράφει τη γραμμή βάσης για τις τεχνικές προδιαγραφές όσον αφορά τις απαιτήσεις αρχιτεκτονικής, παροχής υπηρεσιών και ασφάλειας, αλλά για την επιχειρησιακή λειτουργία της σύνδεσης θα χρειαστούν κάποιες περαιτέρω λεπτομερείς οδηγίες.

Για την ορθή λειτουργία της σύνδεσης θα χρειαστούν διεργασίες και διαδικασίες οι οποίες θα βελτιώσουν την επιχειρησιακή λειτουργία της. Σύμφωνα με το άρθρο 3 παράγραφος 6 της συμφωνίας, τα ζητήματα αυτά περιγράφονται λεπτομερώς σε χωριστό έγγραφο κοινών επιχειρησιακών διαδικασιών (ΚΕΔ), το οποίο εγκρίνεται χωριστά με απόφαση της μεικτής επιτροπής.

2.2. Αποδέκτες

Το παρόν έγγραφο απευθύνεται στον διαχειριστή του ελβετικού μητρώου και στον κεντρικό διαχειριστή της Ένωσης.

3. ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

3.1. Αρχιτεκτονική της σύνδεσης επικοινωνίας

Σκοπός του παρόντος τμήματος είναι να περιγράψει τη γενική αρχιτεκτονική της επιχειρησιακής λειτουργίας της σύνδεσης μεταξύ του ΣΕΔΕ της ΕΕ και του ΣΕΔΕ της Ελβετίας, καθώς και τα διάφορα στοιχεία που εμπλέκονται σε αυτήν.

Δεδομένου ότι η ασφάλεια αποτελεί βασικό στοιχείο για τον καθορισμό της αρχιτεκτονικής, έχουν ληφθεί όλα τα μέτρα για μια αξιόπιστη αρχιτεκτονική. Η μόνιμη σύνδεση των μητρώων χρησιμοποιεί μηχανισμό ανταλλαγής αρχείων ως εφαρμογή ασφαλούς σύνδεσης Air Gap.

Η τεχνική λύση χρησιμοποιεί:

- Πρωτόκολλο ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων.
- Μηνύματα XML.
- Ψηφιακή υπογραφή και κρυπτογράφηση με βάση την XML.
- VPN.

Το ακόλουθο γράφημα παρέχει μια συνολική εικόνα της αρχιτεκτονικής της μόνιμης σύνδεσης των μητρώων:

3.1.1. Ανταλλαγή μηνυμάτων

Η επικοινωνία μεταξύ του ενωσιακού μητρώου και του ελβετικού μητρώου βασίζεται σε μηχανισμό ανταλλαγής μηνυμάτων μέσω ασφαλών διαύλων. Κάθε άκρο βασίζεται στο δικό του αποθετήριο λαμβανόμενων μηνυμάτων.

Αμφότερα τα συμβαλλόμενα μέρη τηρούν ημερολόγιο των λαμβανόμενων μηνυμάτων, μαζί με τα λεπτομερή στοιχεία της επεξεργασίας.

Σφάλματα ή απροσδόκητες καταστάσεις πρέπει να αναφέρονται ως προειδοποιήσεις, ενώ πρέπει να πραγματοποιούνται επαφές μεταξύ των ατόμων που εργάζονται στις ομάδες υποστήριξης.

Τα σφάλματα και τα απρόβλεπτα γεγονότα αντιμετωπίζονται με τήρηση των επιχειρησιακών διαδικασιών που προβλέπονται στη διαδικασία διαχείρισης περιστατικών των ΚΕΔ.

3.1.2. Μήνυμα XML — Περιγραφή υψηλού επιπέδου

Ένα μήνυμα XML περιέχει ένα από τα ακόλουθα:

- Ένα ή περισσότερα αιτήματα συναλλαγής και/ή μία ή περισσότερες αποκρίσεις σε συναλλαγή·
- Μία πράξη / απόκριση που σχετίζεται με την αντιπαραβολή·
- Ένα δοκιμαστικό μήνυμα.

Κάθε μήνυμα περιλαμβάνει κεφαλίδα με:

- Το ΣΕΔΕ προέλευσης·
- Αύξοντα αριθμό.

3.1.3. Παράθυρα πρόσληψης (ingestion windows)

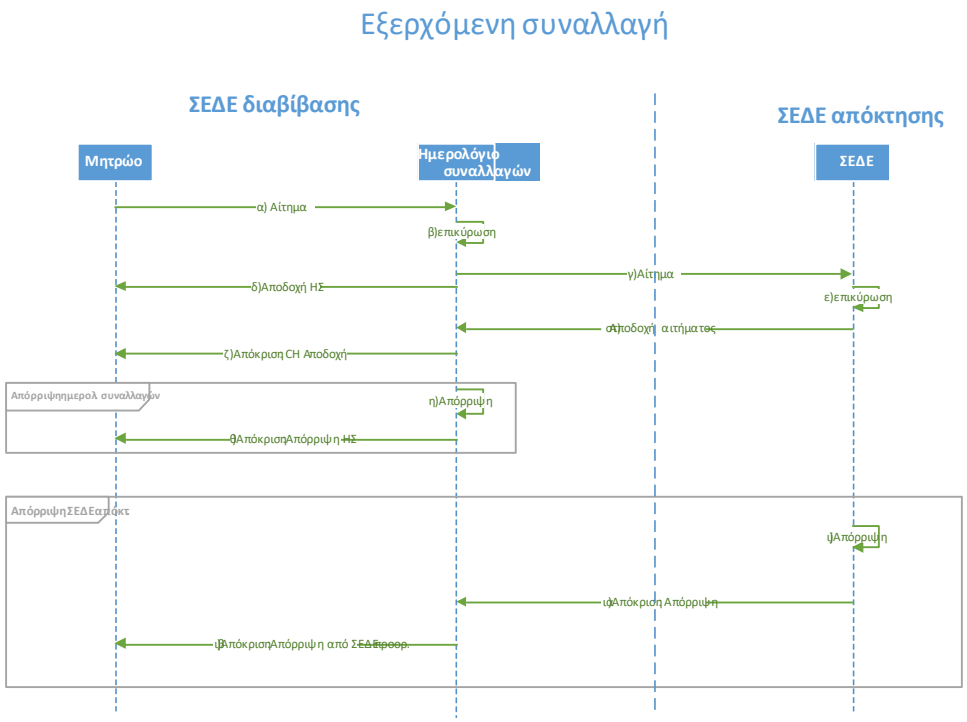
Η μόνιμη σύνδεση των μητρώων βασίζεται σε προκαθορισμένα παράθυρα πρόσληψης που ακολουθούνται από ένα σύνολο συγκεκριμένων συμβάντων. Τα αιτήματα συναλλαγής που λαμβάνονται μέσω της σύνδεσης θα προσλαμβάνονται μόνο σε προκαθορισμένα χρονικά διαστήματα και περιλαμβάνουν τεχνική επικύρωση για εξερχόμενες και εισερχόμενες συναλλαγές. Επιπλέον, οι αντιπαραβολές μπορούν να διεξάγονται σε καθημερινή βάση και μπορούν να ενεργοποιούνται χειρωνακτικά.

Οι αλλαγές στη συχνότητα και/ή στον χρόνο οποιουδήποτε από αυτά τα συμβάντα θα αντιμετωπίζονται με τήρηση των επιχειρησιακών διαδικασιών που προβλέπονται στη διαδικασία ικανοποίησης αιτημάτων των ΚΕΔ.

3.1.4. Ροές μηνυμάτων συναλλαγής

Εξερχόμενες συναλλαγές

Αντικατοπτρίζουν την άποψη του ΣΕΔΕ διαβίβασης. Η συγκεκριμένη ροή απεικονίζεται στο ακόλουθο διάγραμμα ακολουθίας:



Η κύρια ροή δείχνει τα ακόλουθα βήματα (όπως στο ανωτέρω σχήμα):

α) Στο ΣΕΔΕ διαβίβασης, το αίτημα συναλλαγής αποστέλλεται από το μητρώο στο ημερολόγιο συναλλαγών, μόλις ολοκληρωθούν όλες οι επιχειρησιακές καθυστερήσεις (24ωρη καθυστέρηση, κατά περίπτωση).

β) Το ημερολόγιο συναλλαγών επικυρώνει το αίτημα συναλλαγής.

γ) Το αίτημα συναλλαγής αποστέλλεται στο ΣΕΔΕ προορισμού.

δ) Η απόκριση αποδοχής αποστέλλεται στο μητρώο του ΣΕΔΕ προέλευσης.

ε) Το ΣΕΔΕ προορισμού επικυρώνει το αίτημα συναλλαγής.

στ) Το ΣΕΔΕ προορισμού αποστέλλει την απόκριση αποδοχής στο ημερολόγιο συναλλαγών του ΣΕΔΕ προέλευσης.

ζ) Το ημερολόγιο συναλλαγών αποστέλλει την απόκριση αποδοχής στο μητρώο.

Εναλλακτική ροή «Απόρριψη από το ημερολόγιο συναλλαγών» [όπως στο ανωτέρω σχήμα, αρχίζοντας από το α) στην κύρια ροή]:

α) Στο σύστημα προέλευσης, το αίτημα συναλλαγής αποστέλλεται από το μητρώο στο ημερολόγιο συναλλαγών, μόλις ολοκληρωθούν όλες οι επιχειρησιακές καθυστερήσεις (24ωρη καθυστέρηση, κατά περίπτωση).

β) Το ημερολόγιο συναλλαγών δεν επικυρώνει το αίτημα

γ) Το μήνυμα απόρριψης αποστέλλεται στο μητρώο προέλευσης.

Εναλλακτική ροή «απόρριψη του ΣΕΔΕ» [όπως στο ανωτέρω σχήμα, αρχίζοντας από το στοιχείο δ) στην κύρια ροή]:

α) Στο ΣΕΔΕ προέλευσης, το αίτημα συναλλαγής αποστέλλεται από το μητρώο στο ημερολόγιο συναλλαγών, μόλις ολοκληρωθούν όλες οι επιχειρησιακές καθυστερήσεις (24ωρη καθυστέρηση, κατά περίπτωση).

β) Το ημερολόγιο συναλλαγών επικυρώνει τη συναλλαγή.

γ) Το αίτημα συναλλαγής αποστέλλεται στο ΣΕΔΕ προορισμού.

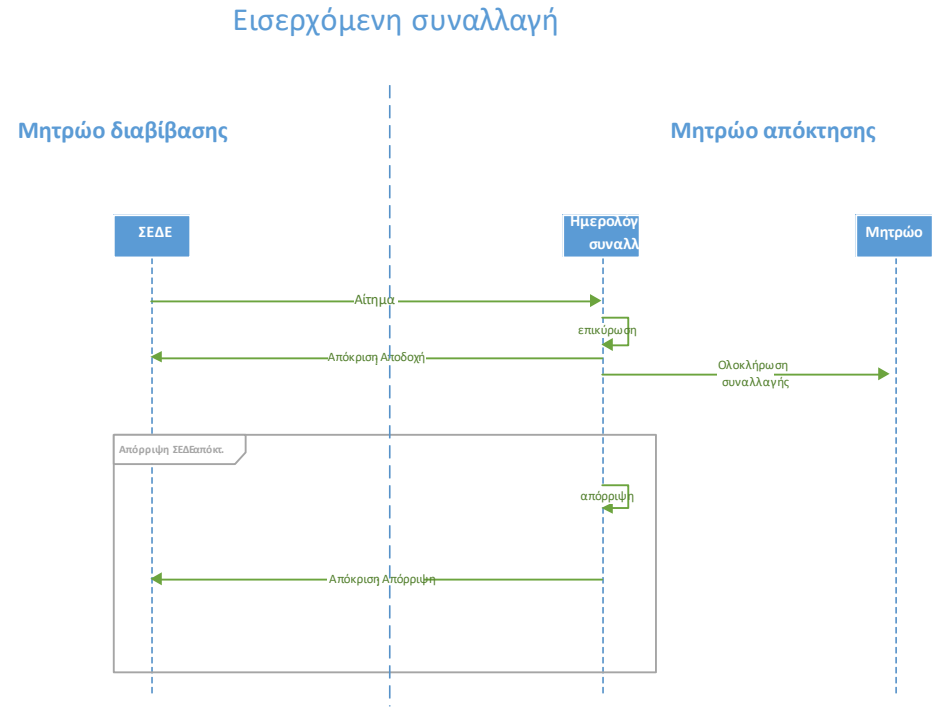
δ) Το μήνυμα αποδοχής αποστέλλεται στο μητρώο του ΣΕΔΕ προέλευσης.

ε) Το ημερολόγιο συναλλαγών του ΣΕΔΕ απόκτησης δεν επικυρώνει τη συναλλαγή.

στ) Το ΣΕΔΕ απόκτησης στέλνει την απάντηση απόρριψης στο ημερολόγιο συναλλαγών του ΣΕΔΕ διαβίβασης.

ζ) Το ημερολόγιο συναλλαγών στέλνει την απόρριψη στο μητρώο.

Εισερχόμενες συναλλαγές



Εδώ αντικατοπτρίζεται η οπτική του ΣΕΔΕ απόκτησης. Η συγκεκριμένη ροή απεικονίζεται στο ακόλουθο διάγραμμα ακολουθίας:

Το διάγραμμα δείχνει:

1) Όταν το ημερολόγιο συναλλαγών του ΣΕΔΕ απόκτησης επικυρώσει το αίτημα, αποστέλλει το μήνυμα αποδοχής στο ΣΕΔΕ διαβίβασης και μήνυμα «ολοκλήρωση συναλλαγής» στο μητρώο του ΣΕΔΕ απόκτησης.

2) Όταν ένα εισερχόμενο αίτημα απορρίπτεται στο ημερολόγιο συναλλαγών απόκτησης και απορρίπτεται, το αίτημα συναλλαγής δεν αποστέλλεται στο μητρώο του ΣΕΔΕ απόκτησης.

Πρωτόκολλο

Ο κύκλος των μηνυμάτων συναλλαγής περιλαμβάνει μόνο δύο μηνύματα:

- Την πρόταση συναλλαγής από το ΣΕΔΕ διαβίβασης → στο ΣΕΔΕ απόκτησης·
- Την απάντηση για τη συναλλαγή από το ΣΕΔΕ απόκτησης → στο ΣΕΔΕ διαβίβασης: Είτε αποδοχή είτε απόρριψη (συμπεριλαμβανομένου του λόγου της απόρριψης).
  - Αποδοχή: Η συναλλαγή ολοκληρώνεται.
  - Απόρριψη: Η συναλλαγή περατώνεται.

Καθεστώς συναλλαγής

- Όταν αποσταλεί το αίτημα, το καθεστώς συναλλαγής στο ΣΕΔΕ διαβίβασης θα ορίζεται ως «προτεινόμενη».
- Όταν ληφθεί το αίτημα και κατά τη διάρκεια της διεκπεραίωσής του, το καθεστώς συναλλαγής στο ΣΕΔΕ απόκτησης θα ορίζεται ως «προτεινόμενη».
- Μόλις ολοκληρωθεί η επεξεργασία του αιτήματος, το καθεστώς συναλλαγής στο ΣΕΔΕ απόκτησης θα ορίζεται ως «ολοκληρωμένη» / «περατωθείσα». Στη συνέχεια,το ΣΕΔΕ απόκτησης θα αποστείλει το αντίστοιχο μήνυμα αποδοχής / απόρριψης.
- Όταν η αποδοχή / η απόρριψη ληφθεί και υποστεί επεξεργασία, το καθεστώς συναλλαγής στο ΣΕΔΕ διαβίβασης θα ορίζεται ως «ολοκληρωμένη» / «περατωθείσα».
- Στο ΣΕΔΕ διαβίβασης, το καθεστώς συναλλαγής θα παραμείνει «προτεινόμενη» εάν δεν ληφθεί απάντηση.
- Το ΣΕΔΕ απόκτησης θα ορίσει ως «περατωθείσα» κάθε συναλλαγή που παραμένει «προτεινόμενη» για περισσότερα από 30 λεπτά.

Τα περιστατικά που σχετίζονται με συναλλαγές θα αντιμετωπίζονται με τήρηση των επιχειρησιακών διαδικασιών που προβλέπονται στη διαδικασία διαχείρισης περιστατικών των ΚΕΔ.

3.2. Ασφάλεια της μεταφοράς δεδομένων

Τα υπό διαμετακόμιση δεδομένα θα υπόκεινται σε τέσσερα επίπεδα ασφαλείας:

1) Έλεγχος πρόσβασης στο δίκτυο: Τείχος προστασίας και στρώμα διασύνδεσης δικτύων.

2) Κρυπτογράφηση στο επίπεδο της μεταφοράς: VPN.

3) Κρυπτογράφηση στο επίπεδο της συνεδρίας επικοινωνίας: Πρωτόκολλο ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων.

4) Κρυπτογράφηση στο επίπεδο της εφαρμογής: Κρυπτογράφηση περιεχομένου και υπογραφή XML.

3.2.1. Τείχος προστασίας και διασύνδεση δικτύων

Η σύνδεση πραγματοποιείται μέσω δικτύου που προστατεύεται από τείχος προστασίας υποστηριζόμενο από υλικό. Το τείχος προστασίας ρυθμίζεται με κανόνες, έτσι ώστε μόνον οι «καταχωρισμένοι» πελάτες να μπορούν να κάνουν συνδέσεις με τον εξυπηρετητή VPN.

3.2.2. Εικονικό ιδιωτικό δίκτυο (VPN)

Όλες οι επικοινωνίες μεταξύ των συμβαλλόμενων μερών προστατεύονται με τη χρήση τεχνολογίας εικονικού ιδιωτικού δικτύου (VPN). Οι τεχνολογίες VPN παρέχουν την ικανότητα «διοχέτευσης» μέσω δικτύου, όπως το διαδίκτυο, από ένα σημείο σε άλλο, προστατεύοντας όλες τις επικοινωνίες. Πριν από τη δημιουργία της διοχέτευσης VPN εκδίδεται ψηφιακό πιστοποιητικό στο άκρο του μελλοντικού πελάτη, που του επιτρέπει να παρέχει αποδεικτικό ταυτότητας κατά τη διάρκεια της διαπραγμάτευσης της σύνδεσης. Κάθε συμβαλλόμενο μέρος είναι υπεύθυνο για την εγκατάσταση του πιστοποιητικού στο δικό του άκρο VPN. Με τη χρήση ψηφιακών πιστοποιητικών, ο εξυπηρετητής VPN κάθε άκρου θα αποκτά πρόσβαση σε μια κεντρική αρχή για να διαπραγματευτεί διαπιστευτήρια για τον έλεγχο ταυτότητας. Κατά τη διαδικασία δημιουργίας της διοχέτευσης γίνεται διαπραγμάτευση κρυπτογράφησης, ώστε να εξασφαλίζεται η προστασία όλων των επικοινωνιών κατά τη διοχέτευση.

Τα άκρα VPN του πελάτη είναι κατάλληλα διαμορφωμένα για τη διατήρηση της σήραγγας VPN σε μόνιμη βάση, ώστε να είναι δυνατή ανά πάσα στιγμή η αξιόπιστη, αμφίδρομη και σε πραγματικό χρόνο επικοινωνία μεταξύ των συμβαλλόμενων μερών.

Γενικά, η Ευρωπαϊκή Ένωση χρησιμοποιεί το δίκτυο ασφαλών διευρωπαϊκών υπηρεσιών τηλεματικής μεταξύ διοικήσεων (STESTA) ως ιδιωτικό δίκτυο βάσει IP. Ως εκ τούτου, το δίκτυο αυτό είναι επίσης κατάλληλο για τη μόνιμη σύνδεση των μητρώων.

3.2.3. Εφαρμογή της IPsec

Η χρήση του πρωτοκόλλου IPSec για να σχηματιστεί η υποδομή VPN από ιστότοπο σε ιστότοπο θα προβλέπει τον έλεγχο ταυτότητας από ιστότοπο σε ιστότοπο, την ακεραιότητα των δεδομένων και την κρυπτογράφηση των δεδομένων. Οι διατάξεις IPSec στο πλαίσιο VPN διασφαλίζουν τον ορθό έλεγχο ταυτότητας μεταξύ δύο άκρων σε σύνδεση VPN. Τα συμβαλλόμενα μέρη θα εντοπίζουν και θα ελέγχουν την ταυτότητα του εξ αποστάσεως πελάτη μέσω της σύνδεσης IPSec με χρήση ψηφιακών πιστοποιητικών που παρέχονται από αρχή πιστοποίησης η οποία έχει αναγνωριστεί από το άλλο άκρο.

Το IPsec διασφαλίζει επίσης την ακεραιότητα των δεδομένων όλων των επικοινωνιών που διέρχονται μέσω της διοχέτευσης VPN. Τα πακέτα δεδομένων κατακερματίζονται και υπογράφονται με τη χρήση των πληροφοριών ελέγχου ταυτότητας που παρέχονται από το VPN. Η εμπιστευτικότητα των δεδομένων εξασφαλίζεται με τον ίδιο τρόπο, με την παροχή δυνατότητας κρυπτογράφησης IPSec.

3.2.4. Πρωτόκολλο ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων

Η μόνιμη σύνδεση των μητρώων βασίζεται σε πολλά στρώματα κρυπτογράφησης για την ασφαλή ανταλλαγή δεδομένων μεταξύ των συμβαλλόμενων μερών. Και τα δύο συστήματα και τα διαφορετικά περιβάλλοντά τους είναι διασυνδεδεμένα σε επίπεδο δικτύου μέσω διοχετεύσεων VPN. Στο επίπεδο της εφαρμογής, τα αρχεία διαβιβάζονται με τη χρήση πρωτοκόλλου ασφαλούς ανταλλαγής για τη διαβίβαση μηνυμάτων σε επίπεδο συνεδρίας.

3.2.5. Κρυπτογράφηση και υπογραφή XML

Στα αρχεία XML η υπογραφή και η κρυπτογράφηση εμφανίζονται σε δύο επίπεδα. Κάθε αίτημα συναλλαγής, απόκριση συναλλαγής και μήνυμα αντιπαραβολής υπογράφονται ψηφιακά και ξεχωριστά.

Σε δεύτερο στάδιο, κάθε επιμέρους στοιχείο του στοιχείου «μήνυμα» είναι κρυπτογραφημένο χωριστά.

Επιπλέον, ως τρίτο στάδιο και για να διασφαλιστεί η ακεραιότητα και η μη άρνηση αναγνώρισης ολόκληρου του μηνύματος, το βασικό μήνυμα που περιέχει όλα τα υπόλοιπα στοιχεία του αρχείου (root element) είναι ψηφιακά υπογεγραμμένο. Αυτό έχει ως αποτέλεσμα υψηλό επίπεδο προστασίας για τα ενσωματωμένα δεδομένα XML. Η τεχνική εφαρμογή τηρεί τα πρότυπα της Κοινοπραξίας του Παγκόσμιου Ιστού.

Για να αποκρυπτογραφηθεί και να επαληθευτεί το μήνυμα, ακολουθείται η διαδικασία με αντίστροφη σειρά.

3.2.6. Κρυπτογραφικά κλειδιά

Για την κρυπτογράφηση και την υπογραφή θα χρησιμοποιούνται συστήματα κρυπτογράφησης με δημόσιο κλειδί.

Στην ειδική περίπτωση της IPSec, χρησιμοποιείται ψηφιακό πιστοποιητικό που εκδίδεται από αρχή πιστοποίησης (στο εξής: ΑΠ) την οποία εμπιστεύονται και τα δύο συμβαλλόμενα μέρη. Η εν λόγω ΑΠ επαληθεύει την ταυτότητα και εκδίδει πιστοποιητικά τα οποία χρησιμοποιούνται για τη θετική ταυτοποίηση μιας οργάνωσης και τη δημιουργία ασφαλών διαύλων επικοινωνίας δεδομένων μεταξύ των συμβαλλόμενων μερών.

Τα κρυπτογραφικά κλειδιά χρησιμοποιούνται για την υπογραφή και την κρυπτογράφηση των διαύλων επικοινωνίας και των αρχείων δεδομένων. Τα δημόσια πιστοποιητικά ανταλλάσσονται ψηφιακά από τα συμβαλλόμενα μέρη με τη χρήση ασφαλών διαύλων και επαληθεύονται εκτός ζώνης. Η διαδικασία αυτή αποτελεί αναπόσπαστο μέρος της διαδικασίας διαχείρισης της ασφάλειας των πληροφοριών στις ΚΕΔ.

3.3. Κατάλογος λειτουργιών στο πλαίσιο της σύνδεσης

Η σύνδεση προσδιορίζει το σύστημα μεταφοράς για μια σειρά λειτουργιών που υλοποιούν τις διαδικασίες εμπορίας δικαιωμάτων εκπομπών οι οποίες απορρέουν από τη συμφωνία. Η σύνδεση περιλαμβάνει επίσης τις προδιαγραφές για τη διαδικασία αντιπαραβολής και για τα μηνύματα δοκιμής που θα καταστήσουν δυνατή την εφαρμογή παρακολούθησης «χτύπων καρδιάς».

3.3.1. Συναλλαγές σχετικές με δραστηριότητες εμπορίας δικαιωμάτων εκπομπών

Από την πλευρά των δραστηριοτήτων, η σύνδεση εξετάζει τέσσερα (4) είδη αιτημάτων συναλλαγής:

- Εξωτερική μεταφορά:
  - Μετά την έναρξη ισχύος της σύνδεσης των ΣΕΔΕ, τα δικαιώματα της ΕΕ και της Ελβετίας είναι εναλλάξιμα και, επομένως, πλήρως μεταβιβάσιμα, μεταξύ των συμβαλλόμενων μερών.
  - Στη μεταφορά που αποστέλλεται μέσω της σύνδεσης εμπλέκονται ένας λογαριασμός μεταφοράς του ενός ΣΕΔΕ και ένας λογαριασμός απόκτησης του άλλου ΣΕΔΕ.

- Η μεταφορά μπορεί να περιλαμβάνει οποιοδήποτε ποσό από τα τέσσερα (4) είδη δικαιωμάτων:
    - Γενικά δικαιώματα της Ελβετίας (CHU)
    - Δικαιώματα του κλάδου αερομεταφορών της Ελβετίας (CHUA)
    - Γενικά δικαιώματα της ΕΕ (EUA)
    - Δικαιώματα του κλάδου αερομεταφορών της ΕΕ (EUAA)

- Διεθνής κατανομή:

Οι φορείς εκμετάλλευσης αεροσκαφών τους οποίους διαχειρίζεται το ένα ΣΕΔΕ και οι οποίοι έχουν υποχρεώσεις στο άλλο ΣΕΔΕ και έχουν δικαίωμα να λαμβάνουν δωρεάν δικαιώματα από το δεύτερο αυτό ΣΕΔΕ, θα λαμβάνουν δωρεάν δικαιώματα του κλάδου των αερομεταφορών από το δεύτερο ΣΕΔΕ, μέσω της συναλλαγής διεθνούς κατανομής.

- Αντιστροφή διεθνούς κατανομής:

Η συναλλαγή αυτή θα πραγματοποιηθεί στην περίπτωση που πρέπει να αντιστραφεί το σύνολο των δωρεάν δικαιωμάτων τα οποία έχουν κατανεμηθεί σε φορέα εκμετάλλευσης αεροσκαφών από το άλλο ΣΕΔΕ.

- Επιστροφή πλεοναζόντων δικαιωμάτων:

Παρόμοια με την αντιστροφή, με τη διαφορά ότι η κατανομή δεν χρειάζεται να αντιστραφεί πλήρως, και μόνο τα πλεονάζοντα κατανεμηθέντα δικαιώματα πρέπει να επιστραφούν στο ΣΕΔΕ που τα κατένειμε.

3.3.2. Πρωτόκολλο αντιπαραβολής

Οι αντιπαραβολές θα πραγματοποιούνται μόνο αφού έχουν κλείσει τα παράθυρα για την πρόσληψη, την επικύρωση και την επεξεργασία των μηνυμάτων.

Οι αντιπαραβολές αποτελούν αναπόσπαστο μέρος των μέτρων ασφάλειας και συνέπειας της σύνδεσης. Τα δύο συμβαλλόμενα μέρη θα συμφωνήσουν για τον ακριβή χρόνο της αντιπαραβολής πριν από την κατάρτιση οποιουδήποτε χρονοδιαγράμματος. Μπορεί να πραγματοποιείται ημερήσια τακτική αντιπαραβολή εφόσον συμφωνηθεί από τα δύο συμβαλλόμενα μέρη. Ωστόσο, τουλάχιστον μια προγραμματισμένη αντιπαραβολή θα πραγματοποιείται μετά την πρόσληψη.

Παρά ταύτα, κάθε συμβαλλόμενο μέρος μπορεί να προβαίνει σε χειρωνακτικές αντιπαραβολές ανά πάσα στιγμή.

Ο χειρισμός των αλλαγών στο χρονοδιάγραμμα και στη συχνότητα της προγραμματισμένης αντιπαραβολής θα διεξάγεται με τήρηση των επιχειρησιακών διαδικασιών που ορίζονται στη διαδικασία ικανοποίησης αιτημάτων των ΚΕΔ.

3.3.3. Δοκιμαστικό μήνυμα

Προβλέπεται η αποστολή δοκιμαστικού μηνύματος για τη δοκιμή της διατερματικής επικοινωνίας. Το μήνυμα θα περιέχει δεδομένα που θα το χαρακτηρίζουν ως δοκιμαστικό και θα απαντηθεί μόλις ληφθεί από το άλλο άκρο.

3.4. Απαιτήσεις καταγραφής δεδομένων

Για να υποστηριχθεί η ανάγκη των δύο συμβαλλόμενων μερών να διατηρούν ακριβείς και συνεπείς πληροφορίες, και για να παρέχονται εργαλεία προς χρήση στη διαδικασία αντιπαραβολής για την επίλυση των ανακολουθιών, τα δύο συμβαλλόμενα μέρη τηρούν τέσσερις (4) τύπους συστημάτων καταγραφής δεδομένων:

- Ημερολόγια συναλλαγών·
- Ημερολόγια αντιπαραβολής·
- Αρχείο μηνυμάτων·
- Ημερολόγια εσωτερικού ελέγχου.

Όλα τα δεδομένα των εν λόγω αρχείων τηρούνται τουλάχιστον κατά τη διάρκεια τριών (3) μηνών για την ανίχνευση λαθών και η περαιτέρω διατήρησή τους θα εξαρτηθεί από το εφαρμοστέο δίκαιο σε κάθε άκρο για τον σκοπό του εσωτερικού ελέγχου. Αρχεία διάρκειας άνω των τριών (3) μηνών μπορούν να αρχειοθετούνται σε ασφαλή τοποθεσία σε ανεξάρτητο σύστημα ΤΠ, εφόσον είναι δυνατή η ανάκτηση ή η πρόσβαση σε αυτό εντός εύλογου χρονικού διαστήματος.

Ημερολόγια συναλλαγών

Αμφότερα τα υποσυστήματα EUTL και SSTL αποτελούν εφαρμογές ημερολογίων συναλλαγών. Είναι συνδεδεμένα με τα δύο συστήματα ΣΕΔΕ.

Ειδικότερα, τα ημερολόγια συναλλαγών θα τηρούν αρχείο για κάθε προτεινόμενη συναλλαγή που αποστέλλεται στο άλλο ΣΕΔΕ. Κάθε εγγραφή περιλαμβάνει όλα τα πεδία του περιεχομένου της συναλλαγής και το επακόλουθο αποτέλεσμα της συναλλαγής (την απάντηση του ΣΕΔΕ αποδέκτη). Τα ημερολόγια συναλλαγών θα τηρούν επίσης αρχείο για τις εισερχόμενες συναλλαγές, καθώς και την απάντηση που στάλθηκε στο ΣΕΔΕ προέλευσης.

Ημερολόγια αντιπαραβολής

Το ημερολόγιο αντιπαραβολής περιλαμβάνει αρχείο για κάθε μήνυμα αντιπαραβολής που ανταλλάσσεται μεταξύ των δύο συμβαλλόμενων μερών, συμπεριλαμβανομένων της ταυτότητας της αντιπαραβολής, της χρονοσφραγίδας και του αποτελέσματος της αντιπαραβολής: Κατάσταση αντιπαραβολής «Επιτυχία» ή «Ασυμφωνίες». Στη μόνιμη σύνδεση των μητρώων, τα μηνύματα αντιπαραβολής αποτελούν αναπόσπαστο μέρος των ανταλλασσόμενων μηνυμάτων και, επομένως, αποθηκεύονται όπως περιγράφεται στην ενότητα «Αρχείο μηνυμάτων».

Τα δύο συμβαλλόμενα μέρη καταγράφουν κάθε αίτημα και τη σχετική απόκριση στο ημερολόγιο αντιπαραβολής. Παρά το γεγονός ότι οι πληροφορίες του ημερολογίου αντιπαραβολής δεν κοινοποιούνται άμεσα στο πλαίσιο της εκάστοτε αντιπαραβολής, η πρόσβαση σε αυτές τις πληροφορίες μπορεί να είναι αναγκαία για την επίλυση των ανακολουθιών.

Αρχείο μηνυμάτων

Αμφότερα τα συμβαλλόμενα μέρη οφείλουν να αρχειοθετούν αντίγραφο των ανταλλασσόμενων δεδομένων (αρχεία XML), τα οποία έστειλαν και έλαβαν, και να σημειώνουν κατά πόσον αυτά τα μηνύματα ή μηνύματα XML είχαν τον σωστό μορφότυπο.

Κύριος σκοπός του αρχείου είναι ο έλεγχος, η απόδειξη της αποστολής και παραλαβής του προς και από το άλλο συμβαλλόμενο μέρος. Υπό την έννοια αυτή, μαζί με τα αρχεία, πρέπει να αρχειοθετούνται και τα σχετικά πιστοποιητικά.

Τα αρχεία αυτοί θα παρέχουν επίσης πρόσθετες πληροφορίες για την αποκατάσταση λαθών.

Ημερολόγιο εσωτερικού ελέγχου

Τα ημερολόγια αυτά καθορίζονται και χρησιμοποιούνται από κάθε συμβαλλόμενο μέρος από την πλευρά του.

3.5. Επιχειρησιακές απαιτήσεις

Η ανταλλαγή δεδομένων μεταξύ των δύο συστημάτων δεν είναι πλήρως αυτόνομη στη μόνιμη σύνδεση των μητρώων και αυτό απαιτεί από τους φορείς εκμετάλλευσης και τις διαδικασίες να καταστήσουν τη σύνδεση λειτουργική. Για τον σκοπό αυτό, στη διαδικασία αυτή περιγράφονται λεπτομερώς διάφοροι ρόλοι και εργαλεία.

4. ΔΙΑΤΑΞΕΙΣ ΠΕΡΙ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ

4.1. Σχεδιασμός της επικοινωνιακής διαθεσιμότητας

Η αρχιτεκτονική για τη μόνιμη σύνδεση των μητρώων είναι ουσιαστικά μια υποδομή ΤΠΕ και ένα λογισμικό που καθιστά δυνατή την επικοινωνία μεταξύ του ΣΕΔΕ της Ελβετίας και του ΣΕΔΕ της ΕΕ. Η διασφάλιση υψηλών επιπέδων διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας της εν λόγω ροής δεδομένων γίνεται, στη συνέχεια, μια ουσιαστική πτυχή που πρέπει να εξεταστεί κατά τον σχεδιασμό της μόνιμης σύνδεσης των μητρώων. Δεδομένου ότι πρόκειται για έργο στον οποίο οι υποδομές ΤΠΕ, το εξατομικευμένο λογισμικό και οι διαδικασίες διαδραματίζουν ουσιαστικό ρόλο, πρέπει να ληφθούν υπόψη και τα τρία στοιχεία προκειμένου να σχεδιαστεί ένα ανθεκτικό σύστημα.

Ανθεκτικότητα των υποδομών ΤΠΕ

Στο κεφάλαιο περί γενικών διατάξεων του παρόντος εγγράφου περιγράφονται λεπτομερώς τα δομοστοιχεία της αρχιτεκτονικής. Όσον αφορά τις υποδομές ΤΠΕ, η μόνιμη σύνδεση των μητρώων διαμορφώνει ένα ανθεκτικό δίκτυο VPN που δημιουργεί ασφαλείς διαύλους επικοινωνίας μέσω των οποίων μπορούν να πραγματοποιούνται ασφαλείς ανταλλαγές μηνυμάτων. Άλλα στοιχεία της υποδομής ρυθμίζονται σε υψηλή διαθεσιμότητα και/ή βασίζονται σε εφεδρικούς μηχανισμούς.

Ανθεκτικότητα του εξατομικευμένου λογισμικού

Οι εξατομικευμένες ενότητες λογισμικού που έχουν αναπτυχθεί ενισχύουν την ανθεκτικότητα μέσω της επανάληψης της επικοινωνίας για δεδομένη χρονική περίοδο με το άλλο άκρο, εάν αυτό, για οποιονδήποτε λόγο, δεν είναι διαθέσιμο.

Ανθεκτικότητα των υπηρεσιών

Στη μόνιμη σύνδεση των μητρώων, οι ανταλλαγές δεδομένων μεταξύ των συμβαλλόμενων μερών πραγματοποιούνται σε προκαθορισμένα χρονικά διαστήματα. Ορισμένα από τα βήματα που ακολουθούνται για τις προκαθορισμένες ανταλλαγές δεδομένων απαιτούν χειροκίνητη παρέμβαση των διαχειριστών συστημάτων και/ή των διαχειριστών μητρώου. Λαμβανομένης υπόψη της πτυχής αυτής και προκειμένου να αυξηθεί η διαθεσιμότητα και η επιτυχία των ανταλλαγών:

- Οι επιχειρησιακές διαδικασίες προβλέπουν χρονικά διαστήματα για την εκτέλεση κάθε βήματος.
- Οι ενότητες λογισμικού για τη μόνιμη σύνδεση των μητρώων εφαρμόζουν ασύγχρονη επικοινωνία.
- Η διαδικασία αυτόματης αντιπαραβολής θα εντοπίζει αν υπήρχαν ζητήματα σχετικά με την πρόσληψη αρχείων δεδομένων σε οποιοδήποτε άκρο.
- Οι διαδικασίες παρακολούθησης (υποδομή ΤΠΕ και εξατομικευμένες ενότητες λογισμικού) εξετάζονται και ενεργοποιούν διαδικασίες διαχείρισης περιστατικών (όπως ορίζονται στο έγγραφο των κοινών επιχειρησιακών διαδικασιών). Οι εν λόγω διαδικασίες που αποσκοπούν στη μείωση του χρόνου αποκατάστασης της κανονικής λειτουργίας έπειτα από περιστατικά είναι ουσιαστικής σημασίας για τη διασφάλιση υψηλών δεικτών διαθεσιμότητας.

4.2. Αρχικοποίηση, επικοινωνία, επανενεργοποίηση και σχέδιο δοκιμών

Όλα τα διαφορετικά στοιχεία που περιλαμβάνονται στην αρχιτεκτονική της μόνιμης σύνδεσης των μητρώων υποβάλλονται σε σειρά επιμέρους και συλλογικών δοκιμών προκειμένου να επιβεβαιωθεί η ετοιμότητα της πλατφόρμας σε επίπεδο υποδομής ΤΠΕ και συστήματος πληροφοριών. Οι εν λόγω επιχειρησιακές δοκιμές αποτελούν υποχρεωτική προϋπόθεση κάθε φορά που η πλατφόρμα αλλάζει την κατάσταση της μόνιμης σύνδεσης των μητρώων από «αναστολή» σε «λειτουργία».

Η ενεργοποίηση του καθεστώτος λειτουργίας της σύνδεσης απαιτεί στη συνέχεια την επιτυχή εκτέλεση προκαθορισμένου σχεδίου δοκιμών. Αυτό επιβεβαιώνει ότι κάθε μητρώο έχει πρώτα πραγματοποιήσει σειρά εσωτερικών δοκιμών, και στη συνέχεια, έχει επικυρώσει τη διατερματική συνδετικότητα πριν από την έναρξη υποβολής των συναλλαγών παραγωγής μεταξύ των δύο συμβαλλόμενων μερών.

Στο σχέδιο δοκιμών θα πρέπει να αναφέρεται η συνολική στρατηγική δοκιμών και λεπτομέρειες σχετικά με την υποδομή δοκιμών. Συγκεκριμένα, για κάθε στοιχείο κάθε ενότητας δοκιμών, θα πρέπει να περιλαμβάνονται:

- Τα κριτήρια και τα εργαλεία της δοκιμής·
- Οι ρόλοι που έχουν ανατεθεί σχετικά με την εκτέλεση της δοκιμής·
- Τα αναμενόμενα αποτελέσματα (θετικά και αρνητικά)·
- Το χρονοδιάγραμμα της δοκιμής·
- Η καταγραφή των απαιτήσεων σχετικά με τα αποτελέσματα των δοκιμών·
- Έγγραφα τεκμηρίωσης για την αποκατάσταση λαθών·
- Διατάξεις κλιμάκωσης.

Ως διαδικασία, οι δοκιμές ενεργοποίησης της κατάστασης λειτουργίας θα μπορούσαν να χωριστούν σε τέσσερα (4) εννοιολογικά τμήματα ή στάδια:

4.2.1. Εσωτερικές δοκιμές υποδομής ΤΠΕ

Οι δοκιμές αυτές πρέπει να διεξάγονται και/ή να ελέγχονται μεμονωμένα από αμφότερους τους διαχειριστές μητρώου σε κάθε άκρο.

Κάθε στοιχείο της υποδομής ΤΠΕ σε κάθε άκρο υποβάλλεται σε δοκιμή μεμονωμένα. Αυτό περιλαμβάνει κάθε επιμέρους στοιχείο της υποδομής. Οι δοκιμές αυτές μπορούν να εκτελούνται αυτόματα ή χειροκίνητα, αλλά επαληθεύουν ότι κάθε στοιχείο της υποδομής είναι λειτουργικό.

4.2.2. Δοκιμές επικοινωνίας

Οι δοκιμές αυτές ξεκινούν μεμονωμένα σε κάθε συμβαλλόμενο μέρος και ολοκληρώνονται σε συνεργασία με το άλλο άκρο.

Μόλις τεθούν σε λειτουργία τα επιμέρους στοιχεία, πρέπει να ελέγχονται οι δίαυλοι επικοινωνίας μεταξύ των δύο μητρώων. Για τον σκοπό αυτό, κάθε συμβαλλόμενο μέρος επαληθεύει ότι η πρόσβαση στο διαδίκτυο λειτουργεί, ότι έχουν δημιουργηθεί οι διοχετεύσεις VPN και ότι υπάρχει συνδεσιμότητα IP μεταξύ εγκαταστάσεων. Στη συνέχεια, θα πρέπει να επιβεβαιωθεί η δυνατότητα πρόσβασης σε τοπικά και εξ αποστάσεως στοιχεία υποδομών και η συνδεσιμότητα IP·στο άλλο άκρο.

4.2.3. Δοκιμές πλήρους συστήματος (διατερματικά)

Οι δοκιμές αυτές πρέπει να εκτελεστούν σε κάθε άκρο και τα αποτελέσματά τους κοινοποιούνται στο άλλο συμβαλλόμενο μέρος.

Αφού οι δίαυλοι επικοινωνίας και κάθε επιμέρους κατασκευαστικό στοιχείο των δύο μητρώων υποβληθούν σε δοκιμή, κάθε άκρο καταρτίζει σειρά προσομοιούμενων συναλλαγών και αντιπαραβολής που είναι αντιπροσωπευτικές όλων των λειτουργιών που πρόκειται να υλοποιηθούν στο πλαίσιο της σύνδεσης.

4.2.4. Δοκιμές ασφαλείας

Οι δοκιμές αυτές πρέπει να διενεργούνται και/ή να ενεργοποιούνται από τους διαχειριστές των μητρώων σε κάθε άκρο, όπως περιγράφεται στις ενότητες «Κατευθυντήριες γραμμές για τους ελέγχους ασφαλείας» και «Διατάξεις αξιολόγησης κινδύνου».

Μόνο αφού κάθε μια από τις τέσσερις φάσεις/ενότητες περατωθεί με προβλέψιμα αποτελέσματα, μπορεί να θεωρηθεί ότι η μόνιμη σύνδεση των μητρώων βρίσκεται σε κατάσταση λειτουργίας.

Πόροι για τις δοκιμές

Κάθε συμβαλλόμενο μέρος προβλέπει ειδικούς πόρους για τις δοκιμές (ειδικό λογισμικό και υλισμικό υποδομής ΤΠΕ) και αναπτύσσει λειτουργίες δοκιμής στα αντίστοιχα συστήματά του για την υποστήριξη της χειρωνακτικής και συνεχούς επικύρωσης της πλατφόρμας. Χειροκίνητες ατομικές ή συνεργατικές διαδικασίες δοκιμής μπορούν να διενεργούνται ανά πάσα στιγμή από τους διαχειριστές των μητρώων. Η ενεργοποίηση της κατάστασης λειτουργίας αποτελεί καθαυτή μια χειροκίνητη διαδικασία.

Επίσης προβλέπεται ότι η πλατφόρμα θα διενεργεί αυτόματους ελέγχους σε τακτά χρονικά διαστήματα. Οι εν λόγω έλεγχοι αποσκοπούν στην αύξηση της διαθεσιμότητας της πλατφόρμας με την έγκαιρη ανίχνευση πιθανών προβλημάτων υποδομών ή λογισμικού. Αυτό το σχέδιο παρακολούθησης της πλατφόρμας αποτελείται από δύο στοιχεία:

- Παρακολούθηση υποδομών ΤΠΕ: και στα δύο άκρα, η υποδομή θα παρακολουθείται από τους παρόχους υπηρεσιών υποδομής ΤΠΕ. Οι αυτόματες δοκιμές θα καλύπτουν τα διάφορα στοιχεία της υποδομής και τη διαθεσιμότητα των διαύλων επικοινωνίας.
- Παρακολούθηση της εφαρμογής: οι ενότητες του λογισμικού της μόνιμης σύνδεσης των μητρώων θα εφαρμόζουν παρακολούθηση της επικοινωνίας του συστήματος σε επίπεδο εφαρμογής (είτε χειροκίνητα είτε/και σε τακτά χρονικά διαστήματα), η οποία θα ελέγχει τη διατερματική διαθεσιμότητα της σύνδεσης, μέσω της προσομοίωσης ορισμένων από τις συναλλαγές διαμέσου της σύνδεσης.

4.3. Περιβάλλοντα αποδοχής / δοκιμών

Η αρχιτεκτονική του ενωσιακού μητρώου και του ελβετικού μητρώου αποτελείται από τα ακόλουθα τρία περιβάλλοντα:

- Παραγωγή (PROD): Το περιβάλλον αυτό έχει στην κατοχή του τα πραγματικά δεδομένα και επεξεργάζεται πραγματικές συναλλαγές.
- Αποδοχή (ACC): Το περιβάλλον αυτό περιέχει μη πραγματικά ή ανωνυμοποιημένα αντιπροσωπευτικά δεδομένα. Είναι το περιβάλλον στο οποίο οι διαχειριστές συστημάτων από τα δύο συμβαλλόμενα μέρη επικυρώνουν τις νέες αναρτήσεις.
- Δοκιμή (TEST): Το περιβάλλον αυτό περιέχει μη πραγματικά ή ανωνυμοποιημένα αντιπροσωπευτικά δεδομένα. Το περιβάλλον αυτό περιορίζεται στους διαχειριστές των μητρώων και προορίζεται να χρησιμοποιείται για τη διενέργεια δοκιμών ολοκλήρωσης από τα δύο συμβαλλόμενα μέρη.

Με εξαίρεση το VPN, τα τρία περιβάλλοντα είναι πλήρως ανεξάρτητα το ένα από το άλλο, δηλαδή το υλισμικό, το λογισμικό, οι βάσεις δεδομένων, τα εικονικά περιβάλλοντα, οι διευθύνσεις IP, οι θύρες διαμορφώνονται και λειτουργούν ανεξάρτητα το ένα από το άλλο.

Όσον αφορά τη διάταξη VPN, η επικοινωνία μεταξύ των τριών περιβαλλόντων πρέπει να είναι πλήρως ανεξάρτητη, γεγονός που εξασφαλίζεται με τη χρήση του STESTA.

5. ΔΙΑΤΑΞΕΙΣ ΓΙΑ ΤΗΝ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΤΗΝ ΑΚΕΡΑΙΟΤΗΤΑ

Οι μηχανισμοί και οι διαδικασίες ασφαλείας προβλέπουν εξέταση από δύο πρόσωπα («αρχή των τεσσάρων ματιών») για πράξεις που εκτελούνται στη σύνδεση μεταξύ του ενωσιακού μητρώου και του ελβετικού μητρώου. Η εξέταση από δύο πρόσωπα εφαρμόζεται όποτε αυτό είναι απαραίτητο, αλλά ενδέχεται να μην ισχύει για όλα τα βήματα που εκτελούν οι διαχειριστές των μητρώων.

Οι απαιτήσεις ασφαλείας εξετάζονται και αντιμετωπίζονται στο σχέδιο διαχείρισης της ασφάλειας, το οποίο περιλαμβάνει επίσης διαδικασίες σχετικά με τη διαχείριση περιστατικών που θέτουν σε κίνδυνο την ασφάλεια κατόπιν ενδεχόμενης παραβίασης της ασφάλειας. Το επιχειρησιακό μέρος των εν λόγω διαδικασιών περιγράφεται στις ΚΕΔ.

5.1. Υποδομή για τους ελέγχους της ασφάλειας

Κάθε συμβαλλόμενο μέρος δεσμεύεται να δημιουργήσει υποδομή για τον έλεγχο της ασφάλειας (χρησιμοποιώντας το από κοινού καθορισμένο λογισμικό και το υλισμικό που χρησιμοποιούνται για τον εντοπισμό των τρωτών σημείων στα στάδια της ανάπτυξης και της λειτουργίας):

- Ξεχωριστά από το περιβάλλον παραγωγής·
- Όταν η ασφάλεια αναλύεται από ομάδα ανεξάρτητη από την ανάπτυξη και τη λειτουργία του συστήματος.

Κάθε συμβαλλόμενο μέρος αναλαμβάνει την εκτέλεση στατικής και δυναμικής ανάλυσης.

Στην περίπτωση δυναμικής ανάλυσης (όπως οι δοκιμές διείσδυσης), τα δύο συμβαλλόμενα μέρη δεσμεύονται να περιορίζουν κατά κανόνα τις αξιολογήσεις στα περιβάλλοντα δοκιμής και αποδοχής (όπως ορίζονται στο τμήμα «Περιβάλλοντα αποδοχής / δοκιμών»). Εξαιρέσεις από την πολιτική αυτή υπόκεινται στην έγκριση και των δύο συμβαλλόμενων μερών.

Πριν από την εγκατάστασή της στο περιβάλλον παραγωγής, κάθε ενότητα λογισμικού της σύνδεσης (όπως ορίζεται στην ενότητα «Αρχιτεκτονική της σύνδεσης επικοινωνίας») υποβάλλεται σε έλεγχο ασφάλειας.

Οι υποδομές δοκιμής πρέπει να διαχωρίζονται, τόσο σε επίπεδο δικτύου όσο και σε επίπεδο υποδομής, από το επίπεδο παραγωγής, ενώ πρέπει να είναι δυνατή η διενέργεια των δοκιμών ασφαλείας που απαιτούνται για τον έλεγχο της συμμόρφωσης με τις απαιτήσεις ασφαλείας.

5.2. Αναστολή της σύνδεσης και διατάξεις για την επανενεργοποίηση

Σε περίπτωση που υπάρχει υπόνοια ότι έχει διακυβευτεί η ασφάλεια του ελβετικού μητρώου, του SSTL, του ενωσιακού μητρώου ή του EUTL, αμφότερα τα συμβαλλόμενα μέρη αλληλοενημερώνονται αμέσως και αναστέλλουν τη σύνδεση μεταξύ του SSTL και του EUTL.

Οι διαδικασίες για την ανταλλαγή πληροφοριών, την απόφαση αναστολής και την απόφαση επανενεργοποίησης αποτελούν μέρος της διαδικασίας ικανοποίησης αιτημάτων των ΚΕΔ.

Αναστολές

Αναστολή της σύνδεσης του μητρώου σύμφωνα με το παράρτημα ΙΙ της συμφωνίας μπορεί να συμβεί για τους εξής λόγους:

- Διοικητικούς λόγους (συντήρηση κ.λπ.), δηλαδή προγραμματισμένη αναστολή·
- Λόγους ασφαλείας (ή αναλύσεις σχετικά με βλάβες της υποδομής ΤΠ), δηλαδή μη προγραμματισμένη αναστολή.

Σε περίπτωση έκτακτης ανάγκης, οποιοδήποτε από τα συμβαλλόμενα μέρη ενημερώνει το άλλο μέρος και αναστέλλει μονομερώς τη σύνδεση του μητρώου.

Εάν ληφθεί απόφαση για αναστολή της σύνδεσης του μητρώου, κάθε συμβαλλόμενο μέρος θα διασφαλίζει ότι η σύνδεση διακόπτεται σε επίπεδο δικτύου (με το κλείδωμα μερών ή του συνόλου των εισερχόμενων και εξερχόμενων συνδέσεων).

Η απόφαση είτε για προγραμματισμένη είτε για μη προγραμματισμένη αναστολή της σύνδεσης του μητρώου θα ληφθεί σύμφωνα με τη διαδικασία διαχείρισης αλλαγών ή τη διαδικασία διαχείρισης περιστατικών ασφάλειας των ΚΕΔ.

Επανενεργοποίηση επικοινωνίας

Η απόφαση για επανενεργοποίηση θα ληφθεί σύμφωνα με την αναλυτική περιγραφή των ΚΕΔ και, σε κάθε περίπτωση, όχι πριν από την επιτυχή ολοκλήρωση των διαδικασιών ελέγχου της ασφάλειας, όπως περιγράφονται στις ενότητες «Κατευθυντήριες γραμμές για τις δοκιμές ασφάλειας» και «Σχεδιασμός αρχικοποίησης, επανενεργοποίησης επικοινωνίας και δοκιμών».

5.3. Διατάξεις για την παραβίαση της ασφάλειας

Η παραβίαση της ασφάλειας θεωρείται περιστατικό που επηρεάζει την εμπιστευτικότητα και την ακεραιότητα τυχόν ευαίσθητων πληροφοριών και/ή τη διαθεσιμότητα του συστήματος χειρισμού τους.

Οι ευαίσθητες πληροφορίες προσδιορίζονται στον κατάλογο ευαίσθητων πληροφοριών και ο χειρισμός τους μπορεί να γίνεται εντός του συστήματος ή σε οποιοδήποτε συνδεδεμένο τμήμα.

Οι πληροφορίες που σχετίζονται άμεσα με την παραβίαση της ασφάλειας θα θεωρούνται ευαίσθητες, με την ένδειξη «SPECIAL HANDLING: *ETS Critical*» και ο χειρισμός τους θα γίνεται σύμφωνα με τις οδηγίες χειρισμού, εκτός εάν ορίζεται διαφορετικά.

Κάθε παραβίαση της ασφάλειας θα αντιμετωπίζεται σύμφωνα με το κεφάλαιο των ΚΕΔ για τη διαχείριση περιστατικών ασφάλειας.

5.4. Κατευθυντήριες γραμμές για τους ελέγχους της ασφάλειας

5.4.1. Λογισμικό

Οι δοκιμές της ασφάλειας, συμπεριλαμβανομένων των δοκιμών διείσδυσης, κατά περίπτωση, πραγματοποιούνται τουλάχιστον σε όλες τις νέες μείζονες εκδόσεις του λογισμικού σύμφωνα με τις απαιτήσεις ασφάλειας που ορίζονται στα ΤΠΣ με σκοπό την αξιολόγηση της ασφάλειας της σύνδεσης και των σχετικών κινδύνων.

Εάν κατά τους τελευταίους 12 μήνες δεν έχει υπάρξει καμία μείζων έκδοση, διενεργείται δοκιμή της ασφάλειας στο τρέχον σύστημα, λαμβανομένης υπόψη της εξέλιξης της κυβερνοαπειλής που σημειώθηκε τους τελευταίους 12 μήνες.

Η δοκιμή ασφάλειας της σύνδεσης των μητρώων πραγματοποιείται στο περιβάλλον αποδοχής και, εφόσον απαιτείται, στο περιβάλλον παραγωγής, με συντονισμό και αμοιβαία συμφωνία των δύο συμβαλλόμενων μερών.

Κατά τις δοκιμές της εφαρμογής στο διαδίκτυο θα τηρούνται τα διεθνή ανοικτά πρότυπα, όπως αυτά που έχουν αναπτυχθεί στο πλαίσιο του Open Web Application Security Project (OWASP).

5.4.2. Υποδομές

Οι υποδομές που στηρίζουν το σύστημα παραγωγής εξετάζονται τακτικά για ανίχνευση τρωτών σημείων (τουλάχιστον μία φορά το μήνα) και τα εντοπιζόμενα τρωτά σημεία αποκαθίστανται βάσει της ίδιας αρχής που ορίζεται στην προηγούμενη ενότητα, με χρήση επικαιροποιημένης βάσης δεδομένων τρωτότητας.

5.5. Διατάξεις αξιολόγησης κινδύνου

Εάν εφαρμόζεται δοκιμή διείσδυσης, πρέπει να περιλαμβάνεται στη δοκιμή ασφάλειας.

Κάθε συμβαλλόμενο μέρος μπορεί να αναθέσει σύμβαση για τη διενέργεια δοκιμών ασφάλειας σε εξειδικευμένη εταιρεία, υπό την προϋπόθεση ότι η εν λόγω εταιρεία:

- Διαθέτει τις δεξιότητες και την πείρα για να διενεργεί τις εν λόγω δοκιμές ασφάλειας·
- Δεν υποβάλλει αναφορά απευθείας στον σχεδιαστή του λογισμικού και/ή στον ανάδοχό του και δεν εμπλέκεται στην ανάπτυξη του λογισμικού της σύνδεσης, ούτε είναι υπεργολάβος του σχεδιαστή του λογισμικού·
- Έχει υπογράψει συμφωνία μη κοινολόγησης, ώστε τα αποτελέσματα να παραμείνουν εμπιστευτικά και να τα χειριστεί στο επίπεδο «SPECIAL HANDLING: ETS Critical» σύμφωνα με τις οδηγίες χειρισμού.