Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστήμων

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτυών*

Μεταπτυχιακή Διατριβή

Εκτίμηση αντίκτυπου σχετικά με τα προσωπικά δεδομένα που επεξεργάζονται τα έξυπνα αεροδρόμια Μελέτη περίπτωσης.

Κώστας Τζιάζας

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστήμων

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτυών*

Μεταπτυχιακή Διατριβή

Εκτίμηση αντίκτυπου σχετικά με τα προσωπικά δεδομένα που επεξεργάζονται τα έξυπνα αεροδρόμια Μελέτη περίπτωσης.

Κώστας Τζιάζας

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών Στην Ασφάλεια Υπολογιστών και Δικτυών από τη Σχολή Θετικών και Εφαρμοσμένων Επιστήμων του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2022

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η παρούσα διατριβή πραγματεύεται την υλοποίηση μιας Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ) στο περιβάλλον ενός «έξυπνου αεροδρομίου», χρησιμοποιώντας σαν υποστηρικτικό εργαλείο μια μεθοδολογία διαχείρισης κινδύνου ως προς την ασφάλεια της επεξεργασίας. Σε πρωταρχικό στάδιο δίνουμε τον ορισμό του τι είναι ένα «έξυπνο» αεροδρόμιο σύμφωνα με την βιβλιογραφία και τα ειδικά χαρακτηριστικά που φέρουν τα «έξυπνα» αεροδρόμια. Ακολούθως αναλύουμε τα διαφορά θέματα ασφάλειας αλλά και προστασίας προσωπικών δεδομένων που μπορεί να αντιμετωπίζουν τα σύγχρονα αεροδρόμια. Μετέπειτα, γίνεται μια ειδική επισκόπηση των αεροδρομιακών συστημάτων που επεξεργάζονται προσωπικά δεδομένα, δίνοντας έμφαση στον κύκλο ζωής των δεδομένων αλλά και την δομή τους καθώς και μια ανάλυση των απαιτήσεων του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (ΓΚΠΔ).

Στο πρακτικό μέρος της διατριβής, πραγματοποιείται μία συστηματική προσέγγιση των κινδύνων για τα προσωπικά δεδομένα και για την αντιμετώπισή τους υλοποιείται μία εκτίμηση αντικτύπου ως προς την προστασία δεδομένων (ΕΑΠΔ), αξιοποιώντας τη μεθοδολογία, αλλά και το σχετικό λογισμικό ανοικτού κώδικα , της ανεξάρτητης Αρχής Προστασίας Δεδομένων της Γαλλίας (CNIL). Επιπρόσθετα γίνεται χρήση της μεθοδολογίας OCTAVE -Allegro για τον εντοπισμό και την αξιολόγηση των κινδύνων για την ασφάλεια των πληροφοριών. Με την ολοκλήρωση της ΕΑΠΔ, η οποία δύναται να αποτελέσει οδηγό για κάθε αντίστοιχη περίπτωση, εξάγονται σημαντικά συμπεράσματα που θα μπορούσαν να καθοδηγήσουν τον οποιονδήποτε αεροδρομιακό φορέα που πραγματοποιεί μία τέτοια επεξεργασία.

Summary

This thesis deals with the application of a Personal Data Impact Assessment (PDIA) in a "smart airport" environment, using as a supporting tool, a risk management methodology for the secure processing of information. At a primary stage, we define what a "smart" airport is according to the literature and the special characteristics that "smart" airports have, then we analyze the different security issues that modern airports face. After that, a precise overview of airport systems that process this type of personal data is given, emphasizing to the structure and life cycle of the data, followed by an analysis of the requirements of the General Regulation for the Protection of Personal Data (GDPR).

In the practical part of the thesis, a systematic approach is followed to identify the threats regarding personal data and a data protection impact assessment (DPIA) is conducted to address those risks utilizing the methodology, but also the relevant open-source software, of the independent Protection Authority Data of France (CNIL). In addition, the OCTAVE-Allegro methodology is used to identify and evaluate information security risks. With the completion of the DPIA, which can be used as a guide for each respective case, important conclusions are drawn that could guide any airport operator that carries out such processing.

Ευχαριστίες

Στο παρόν στάδιο θα ήθελα να ευχαριστήσω των καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη για την καθοδήγηση αλλά και τις πολύτιμες συμβουλές του.

Ένα μεγάλο ευχαριστώ στην οικογένεια μου, και ειδικότερα τους γονείς μου, την σύζυγο μου και στα παιδιά μου. Σας ευχαριστώ όλους από καρδιάς.

Περιεχόμενα

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

Κεφάλαιο 1
Εισαγωγή

Τα έξυπνα αεροδρόμια συσσωρεύουν, επεξεργάζονται και αποθηκεύουν προσωπικά αλλά και ευαίσθητα προσωπικά δεδομένα επιβατών μέσω διαφόρων αεροπορικών συστημάτων αλλά και έξυπνων εφαρμογών και συσκευών. Η επεξεργασία αυτών των δεδομένων έχει σκοπό να διασφαλίσει την ομαλή και απρόσκοπτη λειτουργία των αεροδρομίων αλλά έχει και την υποχρέωση να διασφαλίσει τα προσωπικά δικαιώματα των επιβατών.

Όπως είναι φυσιολογικό σε ένα ταχέως εξελισσόμενο και απαιτητικό περιβάλλον, όπως τα αεροδρόμια, που αποτελούν κρίσιμες υποδομές, σύμφωνα και με την οδηγία της Ευρωπαϊκής Ένωσης (ΕΕ) 2016/1148 περί Ασφάλειας Συστημάτων Δικτύου και Πληροφοριών (NIS Directive), τα προσωπικά και ειδικότερα τα ευαίσθητα προσωπικά δεδομένα των επιβατών θα πρέπει να διαφυλάσσονται από πιθανούς κινδύνους κυβερνοασφάλειας αλλά και από τυχαία ή/και μη σκόπιμα γεγονότα που θίγουν το δικαίωμα στην προστασία προσωπικών δεδομένων όπως αναφέρεται στο Γενικό Κανονισμό Προσωπικών Δεδομένων(ΕΕ)2016/679 (ΓΚΠΔ).

Η χρήση των πληροφοριακών συστημάτων, δικτυών αλλά και τεχνολογιών Internet of Things (IoT) θεωρείται στις μέρες μας αναγκαία από τα έξυπνα αεροδρόμια ώστε να εξυπηρετήσουν το επιβατικό κοινό, η συλλογή όμως μεγάλου όγκου προσωπικών δεδομένων για διάφορους σκοπούς επεξεργασίας, ελλοχεύει διάφορους κινδύνους από εξωτερικούς ή και εσωτερικούς παράγοντες. Η ανάγκη χαρτογράφησης αλλά και η σωστή εφαρμογή τεχνικών και οργανωτικών μέτρων για την διασφάλιση της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων των επιβατών είναι υψίστης σημασίας, αφού οι επιπτώσεις αν δεν εφαρμοστούν τα καταλληλά μέτρα μπορεί να επηρεάσουν άμεσα τα δικαιώματα και τις ελευθερίες των επιβατών.

1.1 Σκοπός Έρευνας

Σκοπός της διατριβής είναι η πραγματοποίηση μιας γενικής επισκόπησης των αεροδρομιακών συστημάτων αλλά και των IoT συσκευών που χρησιμοποιούνται σε ένα αεροδρομιακό περιβάλλον, καθώς επίσης και να αναλυθούν τα θέματα ασφάλειας και προστασίας δεδομένων που δύνανται να αντιμετωπίζουν, εστιάζοντας στα συστήματα που επεξεργάζονται τα ευαίσθητα προσωπικά δεδομένα των ατόμων με αναπηρία και των ατόμων με μειωμένη κινητικότητα (ΑμεΑ). Ο απώτερος στόχος είναι η υλοποίηση μιας ολοκληρωμένης εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων (ΕΑΠΔ) αυτών των ατόμων. Η εν λόγω επεξεργασία δεδομένων είναι υψηλής κρισιμότητας και κινδύνων για τα θεμελιώδη δικαιώματα, λαμβάνοντας υπόψη ότι είναι μία επεξεργασία μεγάλης κλίμακας η οποία αφορά και ευαίσθητα δεδομένα υγείας. Πράγματι, τα άτομα με αναπηρία και τα άτομα με μειωμένη κινητικότητα έχουν το δικαίωμα χρήσης αερομεταφορών και αερολιμένων με βάση τον Ευρωπαϊκό Κανονισμό (ΕΚ) αριθ. 1107/2006, τα ενδιαφερόμενα μέρη που συμβάλουν για την εξυπηρέτηση τους ποικίλουν και η ροή αυτών των δεδομένων καταλήγει στους φορείς αεροδρομίων και τυγχάνουν επεξεργασίας.

Η διατριβή θα εστιάσει στα θέματα ασφάλειας αλλά και προστασίας προσωπικών δεδομένων που ενδέχεται να αντιμετωπίζουν αυτά τα συστήματα από εσωτερικούς και εξωτερικούς παράγοντες παραδείγματος χάριν λάθη από αμέλεια ή από κυβερνοεπιθέσεις λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που χρειάζονται για την προστασία και ασφάλεια των συστημάτων και των δεδομένων που τυγχάνουν επεξεργασίας και αποθήκευσης αλλά και τις τεχνολογίες που χρησιμοποιούνται για την ροή αυτών των δεδομένων από και προς τους φορείς των αερολιμένων.

1.2 Μεθοδολογία Έρευνας

Για να μπορέσουμε να πραγματοποιήσουμε μια ολοκληρωμένη ΕΑΠΔ, θα πρέπει σε πρώτο στάδιο να δώσουμε ένα ξεκάθαρο ορισμό για το τι θεωρούμε έξυπνο αεροδρόμιο, ακολούθως θα υπάρξει μια γενική χαρτογράφηση συστημάτων και τεχνολογιών που

χρησιμοποιούνται από τα έξυπνα αεροδρόμιά αλλά και τις απειλές που μπορεί να τα επηρεάσουν. Μετέπειτα, θα εστιάσουμε σε συγκεκριμένες τεχνολογίες που επεξεργάζονται προσωπικά δεδομένα, δίνοντας έμφαση στην ροή πληροφοριών και την αρχιτεκτονική τους. Στο τελικό στάδιο θα αναλύσουμε εάν οι πράξεις επεξεργασίας που διενεργούνται από τους φορείς επιβάλλουν την υλοποίηση μιας ΕΑΠΔ με βάση των ΓΚΠΔ. Δεν υπάρχει συγκεκριμένη μεθοδολογία για την διεκπεραίωση της ΕΑΠΔ αλλά διάφορα εργαλεία που παρέχει η Αρχή Προστασίας Δεδομένων της Γαλλίας (CNIL) σε συνδυασμό με μια μεθοδολογία εκτίμησης κινδύνου που θα έχει υποστηρικτικό ρόλο στην υλοποίηση της ΕΑΠΔ, όπως η OCATVE -Allegro θα μπορούσαν να χρησιμοποιηθούν.

1.3 Βασικά Ερευνητικά Ερωτήματα

Τα έξυπνα αεροδρόμια, όπως και άλλες επιχειρήσεις, χρησιμοποιούν καινοτόμες τεχνολογίες με σκοπό την καλύτερη και ταχύτερη εξυπηρέτηση των πελατών τους με στόχο την αύξηση των εσόδων τους, αυτό που δεν πρέπει να ξεχνούμε είναι ότι ακόμα και σήμερα τα αεροδρόμια και γενικότερα ο τομέας της αεροναυτιλίας βασίζετε σε τεχνολογίες που είχαν αναπτυχθεί πριν αρκετές δεκαετίες. Λαμβάνοντας τα πιο πάνω υπόψη θέτουμε τα πιο κάτω ερωτήματα :

1. Τι ειδικά χαρακτηριστικά φέρουν τα «έξυπνα» αεροδρόμια;
2. Ποιες είναι οι κυβερνοαπειλές που αντιμετωπίζουν τα σημερινά σύγχρονα «έξυπνα» αεροδρόμια, λαμβάνοντας υπόψιν ότι πεπαλαιωμένα και σύγχρονα συστήματα χρησιμοποιούνται σε συνδυασμό για την επεξεργασία προσωπικών δεδομένων ;
3. Μπορεί μία ολοκληρωμένη ΕΑΠΔ να βοηθήσει στην επιτυχή αντιμετώπιση όλων των κινδύνων προστασίας δεδομένων; Πώς μπορεί να αλληλεπιδράσει με μία διαχείριση κινδύνων ασφαλείας;
4. Μπορεί να αναπτυχθεί μία ΕΑΠΔ που να αποτελεί βάση αναφοράς για κάθε αντίστοιχη επεξεργασία από οποιονδήποτε αεροδρομιακό φορέα;

1.4 Αναγκαιότητα και Σπουδαιότητα Έρευνας

Το δικαίωμα ελεύθερης μετακίνησης είναι αναφαίρετο δικαίωμα όλων των πολιτών της Ευρωπαϊκής Ένωσης καθώς όμως και η διασφάλιση της ιδιωτικότητας και προστασίας των προσωπικών τους δεδομένων.

Σύμφωνα με των ΓΚΠΔ ο υπεύθυνος επεξεργασίας δεδομένων , στην περίπτωσή μας το εκάστοτε αεροδρόμιο (το αντίστοιχο νομικό πρόσωπο που είναι αρμόδιο για τη διαχείρισή του), μπορεί να επεξεργάζεται τα προσωπικά δεδομένα με βάση την νομική του υποχρέωση ή όταν είναι αναγκαία για την εκπλήρωση καθηκόντων ως προς το δημόσιο συμφέρον. Τα προσωπικά δεδομένα πρέπει όμως να επεξεργάζονται σύμφωνα με τις αρχές που περιγράφονται στον Κανονισμό.

Η χαρτογράφηση των συστημάτων των αεροδρομίων αλλά και των πιθανών θεμάτων ασφάλειάς που μπορεί να αντιμετωπίζουν είναι πρώτιστης σημασίας για την διεκπεραίωση μιας σωστής ΕΑΠΔ προτείνοντας σαν αποτέλεσμα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία αλλά και την σωστή επεξεργασία αυτών των δεδομένων.

Επίσης, δεδομένου ότι πολλά αεροδρόμια έχουν αντίστοιχες επεξεργασίες, με αντίστοιχους κινδύνους ως προς την προστασία δεδομένων, η εκπόνηση μίας ΕΑΠΔ για μία τέτοια επεξεργασία δεδομένων μπορεί να αποτελέσει «βάση αναφοράς» για όλα τα αεροδρόμια.

1.5 Δομή Διατριβής

Η Παρούσα διατριβή αποτελείται από έξι κεφάλαια. Στο πρώτο κεφάλαιο έχουμε την «Εισαγωγή» που μας ενημερώνει τι πραγματεύεται η παρούσα διατριβή. Στο δεύτερο κεφάλαιο «Έξυπνο Αεροδρόμιο» δίνουμε τον ορισμό ενός έξυπνου αεροδρομίου παρουσιάζοντας την υποδομή του και πως οι τεχνολογίες IoT είναι πλέον αναπόσπαστο μέρος αυτής της υποδομής. Στο δεύτερο κεφάλαιο «Ασφάλεια Πληροφοριακών

Συστημάτων» αναλύονται οι παράγοντες απειλών, οι ευπάθειες ασφάλειας αλλά και τα μέτρα που προτείνονται για την διασφάλιση των αεροδρομιακών συστημάτων.

Στο τέταρτο κεφάλαιο «Συστήματα Αεροδρομίων» γίνεται μια λεπτομερής αναφορά στον τρόπο δομής μηνυμάτων ΙΑΤΑ που εμπεριέχουν προσωπικά δεδομένά και ειδικές κατηγορίες προσωπικών δεδομένων. Ακολούθως γίνεται μια ανασκόπηση των συστημάτων τα οποία επεξεργάζονται.

Στο πέμπτο κεφάλαιο έχουμε μια ανασκόπηση του Γενικού Κανονισμού Προσωπικών Δεδομένων (ΓΚΠΔ) και την εξέλιξη του από οδηγία σε κανονισμό. Στο έκτο κεφάλαιο γίνεται μια εκτίμηση κινδύνου προσωπικών δεδομένων με σκοπό να υποστηρίξει την ολοκλήρωση μια Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ). Στο τελευταίο κεφάλαιο έχουμε τα τελικά συμπεράσματα και το αποτέλεσμα.

Κεφάλαιο 2
Έξυπνο Αεροδρόμιο

2.1 Πως ορίζεται ένα έξυπνο αεροδρόμιο

Έξυπνα αεροδρόμια ορίζονται σύμφωνα με το άρθρο “Implementing Cyber-Security Measures in Airports” [1] σαν τα αεροδρόμια που χρησιμοποιούν σύγχρονες τεχνολογίες με σκοπό τη μεγιστοποίηση της επιχειρησιακής τους αποτελεσματικότητας και της συνεργασίας μεταξύ των διαφόρων φορέων που απαρτίζουν την αεροδρομιακή κοινότητα. Ο ENISA [2] τα ορίζει ως τα αεροδρόμια που χρησιμοποιούν δεδομένα που όχι μόνο στοχεύουν στη βελτίωση της εμπειρίας των επιβατών μέσω της χρήσης των συσκευών IoT, αλλά και στην αύξηση των επιπέδων ασφάλειας της κοινότητας του αεροδρομίου, που αποτελείται από αεροπορικές εταιρείες, φορείς εκμετάλλευσης αεροδρομίων, παρόχους υπηρεσιών και κρατικούς φορείς. Επιπρόσθετα, συμφώνα με τους N.Koroniotis [3], ο στόχος των συσκευών IoT είναι να βελτιώσουν την ευρωστία και την αποτελεσματικότητα των παρεχόμενων υπηρεσιών.

Ο ENISA χρησιμοποιεί τον όρο Smart Components για να περιγράψει και να ορίσει τις συσκευές IoT. Σύμφωνα με την έκθεση [2] , "Τα Smart components μπορούν να οριστούν ως οποιοδήποτε δικτυωμένο σύστημα που έχει την ικανότητα επεξεργασίας δεδομένων που κυμαίνεται από τη συγκέντρωση απλών δεδομένων έως την εξαγωγή πληροφοριών για την υποστήριξη ανθρώπινων αποφάσεων και την ενεργοποίηση μιας αυτοματοποιημένης απόκρισης", καταλαβαίνουμε ότι αυτό είναι μια πολύ ευρεία έννοια που περιλαμβάνει σχεδόν όλα τα στοιχεία της υποδομής του αεροδρομίου.

Επιπλέον, οι E. Ukwandu et al. [4] υποστηρίζουν και επεκτείνουν τον όρο των συσκευών IoT σε αισθητήρες και ενεργοποιητές. Περαιτέρω, όπως περιγράφεται στο άρθρο [4], οι συσκευές IoT είναι υπεύθυνες για τη συγχώνευση Τεχνολογίας Πληροφοριών και Επικοινωνιών με βιομηχανικές συσκευές με αποτέλεσμα να εγείρονται θέματα ασφάλειας. Αυτό αυξάνει την ανάγκη άμεσης αντιμετώπισης των ζητημάτων σχετικά με τον τρόπο με τον οποίο αυτές οι συσκευές μπορούν να επηρεαστούν από ζητήματα

ασφάλειας στον κυβερνοχώρο και πώς μπορούν να περιοριστούν και να μετριαστούν τα περιστατικά και οι κίνδυνοι, αντίστοιχα.

Σύμφωνα με το άρθρο Cyber Security for Airports [5] , η βιομηχανία avionics είναι σχετικά προηγμένη στη χρήση προτύπων ασφάλειας στον κυβερνοχώρο έναντι των ομολόγων της στον τομέα των μεταφορών, αλλά αυτό δεν ισχύει για όλες τις εμπλεκόμενες οντότητες, τα αεροδρόμια είναι ένα από αυτά. Μάλιστα, οι Gopalakrishnan et al. [5, p. 367] αναφέρουν ξεκάθαρα ότι "Χάρη στο ίδιο το σύστημα, τα αεροδρόμια είναι ιδιαίτερα ευάλωτα σε εσωτερικές και εξωτερικές απειλές".

2.2 Συσκευές Διαδικτύου των Πραγμάτων (IoT)

Η χρήση συσκευών Διαδικτύου των Πραγμάτων (IoT) ή όπως ο ENISA [2] τις αναφέρει ως "Smart Components που διαθέτουν δυνατότητες επεξεργασίας δεδομένων", έχουν στόχο τη βελτίωση των λειτουργιών οποιασδήποτε εταιρείας και τη βελτίωση της εμπειρίας των πελατών της. Η ανάγκη διερεύνησης των ρίσκων από τη χρήση τέτοιων τεχνολογιών για την προστασία της υποδομής μας είναι επιτακτική τόσο για να διαβεβαιώσουμε όλα τα ενδιαφερόμενα μέλη για την ασφάλεια των υπηρεσιών που προσφέρουμε αλλά και την συμμόρφωση του οργανισμού με τις εκάστοτε νομοθεσίες,

Για να προσδιορίσουμε την έκθεση στον κίνδυνο που αντιμετωπίζει οποιοσδήποτε οργανισμός από Συσκευές IoT και smart components , πρώτον, πρέπει να τα εντοπίσουμε και, δεύτερον, να μπορούμε να χαρτογραφήσουμε όλες τις διασυνδέσεις μεταξύ αυτών και των παραδοσιακών υποδομών. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (ENISA) [6] παρουσιάζει τον παρακάτω πίνακα ταξινομώντας τις IoT συσκευές αλλά και πως αλληλοεπιδρούν με την παραδοσιακή υποδομή ενός οργανισμού :

Ταξινόμηση Αγαθών	Αγαθά	Περιγραφή
Συσκευές IoT (IoT Devices)	Υλικό (Hardware)	Τα διάφορα φυσικά στοιχεία από τα οποία μπορούν να κατασκευαστούν οι συσκευές IoT, συμπεριλαμβανομένων μικροεπεξεργαστών και η μητρική πλακέτα
	Λογισμικό (Software)	Το λογισμικό περιλαμβάνει το λειτουργικό σύστημα της συσκευής IoT, το υλικολογισμικό της, τα προγράμματα και τις εφαρμογές που έχουν εγκατασταθεί και τρέχουν.
	Αισθητήρες (Sensors)	Είναι τα υποσυστήματα που ανιχνεύουν και μετρούν γεγονότα στο περιβάλλον τους και στέλνουν τις πληροφορίες σε άλλα ηλεκτρονικά είδη προς επεξεργασία. Υπάρχουν αισθητήρες για τη μέτρηση θερμοκρασίας, κίνησης κ.λπ.
	Ενεργοποιητές (Actuators)	Πρόκειται για μονάδες εξόδου συσκευών IoT, οι οποίες εκτελούν αποφάσεις με βάση τις προηγουμένως επεξεργασμένες πληροφορίες.
Άλλες Συσκευές που βρίσκονται στο περιβάλλον τον IoT συσκευών	Συσκευές για διασύνδεσης με IoT Devices	Πρόκειται για συσκευές των οποίων ο σκοπός είναι να χρησιμεύουν ως διεπαφή μεταξύ άλλων συσκευών IoT ενός δεδομένου οικοσυστήματος IoT. Επιπλέον, οι συσκευές χρησιμοποιούνται από τους χρήστες για διασύνδεση και αλληλεπίδραση με συσκευές IoT.
	Συσκευές για τη διαχείριση IoT Devices	Πρόκειται για συσκευές ειδικά σχεδιασμένες για τη διαχείριση άλλων συσκευών IoT, δικτύων κ.λπ.

	Ενσωματωμένα συστήματα	Βασίζονται σε μια μονάδα επεξεργασίας που τους επιτρέπει να επεξεργάζονται δεδομένα μόνα τους. Περιλαμβάνουν ενσωματωμένους αισθητήρες και ενεργοποιητές, δυνατότητες δικτύου για απευθείας σύνδεση στο cloud, αποτύπωμα μνήμης και δυνατότητα εκτέλεσης του λογισμικού.
Δικτυακές Επικοινωνίες (Communications)	Δίκτυα (Networks)	Επιτρέπουν στους διαφορετικούς κόμβους ενός οικοσυστήματος IoT να ανταλλάσσουν δεδομένα και πληροφορίες μέσω ενός data link . Υπάρχουν διάφορα είδη δικτύων ανάλογα με τη χωρική τους κάλυψη, η οποία περιλαμβάνει μεταξύ άλλων (W)LAN, (W)PAN, PAN και (W)WAN.
	Πρωτόκολλα (Protocols)	Είναι ένα σύνολο κανόνων που καθορίζουν τον τρόπο με τον οποίο πρέπει να εκτελείται η επικοινωνία μεταξύ δύο ή περισσότερων συσκευών IoT μέσω ενός συγκεκριμένου καναλιού. Υπάρχουν πολλά πρωτόκολλα επικοινωνίας, τα οποία μπορεί να είναι είτε ασύρματα είτε ενσύρματα. Παραδείγματα πρωτοκόλλων επικοινωνίας IoT είναι τα ZigBee, MQTT, CoAP, BLE κ.λπ.
	Δρομολογητές (Routers)	Είναι τα στοιχεία δικτύωσης που διαβιβάζουν πακέτα δεδομένων μεταξύ των διαφορετικών δικτύων του οικοσυστήματος IoT.
	Πύλες (Gateways)	Αυτοί είναι οι κόμβοι δικτύου που χρησιμοποιούνται για διασύνδεση με άλλο δίκτυο από το περιβάλλον IoT που χρησιμοποιεί διαφορετικά

Υποδομή (Infrastructure)		πρωτόκολλα. Οι πύλες ενδέχεται να παρέχουν μεταφραστές πρωτοκόλλων, απομονωτές σφαλμάτων κ.λπ., για την παροχή διαλειτουργικότητας του συστήματος.
	Παροχή ηλεκτρικού ρεύματος (Power supply)	Παρέχει ηλεκτρική ενέργεια σε μια συσκευή IoT και στα εσωτερικά εξαρτήματά της. Η πηγή τροφοδοσίας μπορεί να είναι εξωτερική και ενσύρματη ή μια μπαταρία ενσωματωμένη στην ίδια τη συσκευή.
	Περιουσιακά στοιχεία ασφαλείας (Security assets)	Αυτή η ομάδα περιλαμβάνει τα στοιχεία που επικεντρώνονται ρητά στην ασφάλεια των συσκευών, των δικτύων και των πληροφοριών IoT. Πιο εμφανή, αυτά περιλαμβάνουν τείχη προστασίας, τείχη προστασίας εφαρμογών Ιστού (WAF), CASB για την προστασία του νέφους, IDS, IPS και συστήματα ελέγχου ταυτότητας/εξουσιοδότησης.
Platform & Backend	Web-based Services	Αυτές οι υπηρεσίες εντός του World Wide Web παρέχουν μια web based διεπαφή προς στους χρήστες ή εφαρμογές συνδεδεμένες στο διαδικτύου . Αυτό σημαίνει ότι οι τεχνολογίες Ιστού μπορούν να χρησιμοποιηθούν στο IoT οικοσύστημα για επικοινωνίες ανθρώπου με μηχανή (H2M) και επικοινωνίες M2M.
	Υποδομές και υπηρεσίες cloud (Cloud infrastructure and services)	Στο IoT, το backend του cloud μπορεί να χρησιμοποιηθεί για τη συγκέντρωση και επεξεργασία δεδομένων από διασκορπισμένες συσκευές και παρέχει επίσης υπολογιστικές δυνατότητες,

		δυνατότητες αποθήκευση, εφαρμογές, υπηρεσίες κ.λπ.
Λήψη αποφάσεων (Decision Making)	Data Mining	Αυτό αναφέρεται σε αλγόριθμους και υπηρεσίες για την επεξεργασία συλλεγόμενων δεδομένων και τη μετατροπή τους σε μια καθορισμένη δομή για περαιτέρω χρήση, χρησιμοποιώντας τεχνολογίες big data για την ανακάλυψη προτύπων σε εκτεταμένα σύνολα δεδομένων
	Επεξεργασία δεδομένων και Computing	Οι υπηρεσίες διευκολύνουν την επεξεργασία των συγκεντρωμένων δεδομένων για τη λήψη χρήσιμων πληροφοριών, οι οποίες μπορούν να χρησιμοποιηθούν για την εφαρμογή κανόνων και λογικής, τη λήψη αποφάσεων και την αυτοματοποίηση των διαδικασιών.
Εφαρμογή & Υπηρεσίες (Applications & Services)	Data analytics and visualization	Αφού συλλεχθούν και υποβληθούν σε επεξεργασία τα δεδομένα, οι πληροφορίες που προκύπτουν μπορούν να αναλυθούν και να οπτικοποιηθούν για τον εντοπισμό νέων προτύπων, τη βελτίωση της λειτουργικής αποτελεσματικότητας κ.λπ.
	Διαχείριση συσκευών και δικτύου (Device and network management)	Η διαχείριση των συσκευών και των δικτύων του οικοσυστήματος IoT περιλαμβάνει τις ενημερώσεις λογισμικού του λειτουργικού συστήματος, του υλικολογισμικού και των εφαρμογών. Περιλαμβάνει επίσης την παρακολούθηση των συσκευών και των δικτύων, τη συλλογή και την αποθήκευση αρχείων καταγραφής που μπορούν αργότερα να

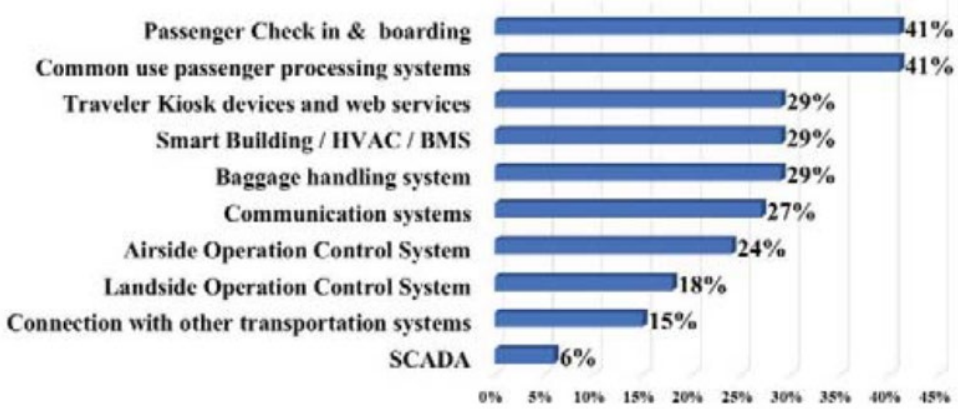
		χρησιμοποιηθούν για διαγνωστικά.
	Χρήση συσκευών (Device usage)	Η προσαρμογή των συσκευών και των δικτύων του οικοσυστήματος IoT για την κατανόηση μιας κατάστασης, των προτύπων χρήσης, της απόδοσης κ.λπ.
Πληροφορίες (Information)	Σε Αποθήκευση (At rest)	Οι πληροφορίες αποθηκεύονται σε μια βάση δεδομένων, στο backend του cloud ή στις ίδιες τις συσκευές
	Κατά την Μεταφορά (In transit)	Οι πληροφορίες αποστέλλονται ή ανταλλάσσονται μέσω του δικτύου μεταξύ δύο ή περισσότερων στοιχείων IoT
	Κατά την Χρήση (In use)	Πληροφορίες που χρησιμοποιούνται από μια εφαρμογή, υπηρεσία ή στοιχείο IoT.

Πίνακας 1 Ταξινόμηση IoT συσκευών Πηγή : [6]

Μια σειρά από Smart components περιγράφεται από την G. Lykou et al. [1] και τον ENISA [2], ενώ οι K. Gopalakrishnan et al. [5] κάνουν ειδική αναφορά για τα συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA). Τα λεγόμενα Smart components αποτελούν μέρος όλων των κρίσιμων συστημάτων των αεροδρομίων και είναι διασυνδεδεμένα με όλα τα επίπεδα της υποδομής πληροφορικής. Για να δώσουμε μια πιο ξεκάθαρη εικόνα μερικά από αυτά τα συστήματα είναι τα εξής:

- Συστήματα επεξεργασίας επιβατών κοινής χρήσης (Common Use Passengers Processing System (CUPPS))
- Βάση Επιχειρησιακών Δεδομένων Αεροδρομίου (Airport Operational Database (AODB))
- Σύστημα Αντιστοίχισης Αποσκευών – (Baggage Reconciliation System)
- Συστήματα απεικόνισης πληροφοριών πτήσης(Flight Information Display Systems (FIDS))
- SCADA

Το γράφημα πιο κάτω απεικονίζει ποιες έξυπνες εφαρμογές χρησιμοποιούνται στα αεροδρόμια.



Εικόνα 1 Εφαρμογές IoT Πηγή [1]

2.3 Αεροδρομιακή Κοινότητα

Η αεροδρομιακή κοινότητα αποτελείται από μια πληθώρα κυβερνητικών και μη υπηρεσιών που σκοπό έχουν την εξυπηρέτηση και την ασφάλεια του επιβατικού κοινού. Σύμφωνα με τον David Schaar και Lance Sherry [8], και στο πλαίσιο της παρούσας μελέτης τα αεροδρόμια πρέπει να προσφέρουν σε όλους του εμπλεκομένους φορείς τις κατάλληλες υποδομές, όπως θα αναφερθούν και πιο κάτω, για να μπορούν να διεκπεραιώσουν τις εργασίες τους. Στον πίνακα 2 πιο κάτω παρουσιάζονται σε συντομία μερικοί από τους εμπλεκομένους φορείς.

Αντιλαμβανόμαστε ότι πολλά από τα πιο κάτω ενδιαφερόμενα μέλη έχουν τις δικές τους διαδικασίες και πολιτικές αλλά έχουν και την υποχρέωση να εφαρμόζουν τοπικές αλλά και ευρωπαϊκές νομοθεσίες - όπως για παράδειγμα ισχύει για εμπλεκομένους όπως η πολιτική αεροπορία η αστυνομία και το τελωνείο.

Αναμενόμενο είναι λοιπόν εκτός, από τον αριθμό επιβατών, να έχουμε και ένα μεγάλο αριθμό εργαζόμενων όπου τα προσωπικά τους δεδομένα τυγχάνουν επεξεργασίας και από την διαχειρίστρια εταιρεία των αεροδρομίων αλλά και από τις τοπικές αρχές.

ΕΝΔΙΑΦΕΡΟΜΕΝΟΣ ΜΕΛΟΣ	ΤΟΜΕΑΣ
Επιβατικό κοινό	-
Πολιτική Αεροπορία	Κυβερνητικός Τομέας
Αστυνομία	Κυβερνητικός Τομέας
Τελωνείο	Κυβερνητικός Τομέας
Διαχειριστές Αεροδρόμιων	Ιδιωτικός Τομέας
Αεροπορικές Εταιρίες	Ιδιωτικός Τομέας
Διαχειριστές Αερογραμμών	Ιδιωτικός Τομέας
Μέσα Μαζικής Μεταφοράς	Ιδιωτικός Τομέας
Διάφορες Ιδιωτικές Εταιρείες	Ιδιωτικός Τομέας

Πίνακας 2 Μέλη Αεροδρομιακής Κοινότητας

2.4 Υποδομή Πληροφορικής στα Αεροδρόμια

Σύμφωνα με το Airport Cooperative Research Program (ACRP) [9], τα αεροδρομιακά συστήματα και η υποδομή πληροφορικής γενικότερα στον αεροδρομιακό τομέα είναι αρκετά περίπλοκη. Η αρχιτεκτονική μπορεί να ομαδοποιηθεί σε 4 κατηγορίες. Οι συσκευές IoT συνδέονται με τα ακόλουθα επίπεδα της υποδομής πληροφορικής, όπως αναφέρεται στην αναφορά του ACRP [9]:

- Φυσικό Στρώμα (Physical Layer): Σε αυτό το επίπεδο περιγράφονται οι καλωδιώσεις οπτικών ινών και χαλκού.
- Στρώμα Δικτύου (Networking Layer): Σε αυτό το στρώμα συμπεριλαμβάνονται switches, routers, gateways, and wireless access points
- Στρώμα Εφαρμογών (Application Layer): Το στρώμα των εφαρμογών συμπεριλαμβάνει όλες τις εφαρμογές που υποστηρίζουν τις επιχειρησιακές δραστηριότητες των αεροδρόμιων.
- Στρώμα Διασύνδεσης (Integration Layer): Αυτό το στρώμα επιτρέπει την επικοινωνία μεταξύ των εφαρμογών και την κοινοποίηση των πληροφοριών.

Η εικόνα 2 από το ACRP [9] δίνει ένα λεπτομερή πίνακα που αντιστοιχεί ομάδες συστημάτων αλλά και συστήματα στο κάθε επίπεδο. Αντιλαμβανόμαστε λοιπόν, σύμφωνα με τον ορισμό που δώσαμε πιο πάνω για τα έξυπνα αεροδρόμια, ότι οι συσκευές IoT χρησιμοποιούνται στην πλειονότητα των αεροδρομιακών εφαρμογών.

System Layer	System Grouping	System Name
Physical layer	Cable and fiber infrastructure	
Networking layer	LAN, WAN, wireless communications	Licensed wireless
		Local area network
		Wireless area network WAN
		Wireless LAN
Application layer	Airside systems	Airfield lighting
		AWOS
		Fuel monitoring system
		Noise monitoring
		Resource management system
		SMGCS
		Surface movement radar
	Landside systems	Audio paging system
		AVI
		PARC
		Roadway dynamic signage
	Passenger processing systems	Baggage sortation/RFID
		CUPPS
		CUSS
		LDCS
		MUFIDS
	Business/finance systems	Asset management system
		Email
		Financial management system
		Human resource management system
		Property management system
		Telephony
		Website
	Safety/security systems	ACS
		Badging system
		CCTV
		CAD
		Fire alarm
		Fire department systems
		Police systems
		Ring-down circuit
	Facility/maintenance systems	CMMS
		Building management system
Systems integration layer		Airport operational database (AODB)
		Geographic information display system
		Message broker
		Systems manager

Εικόνα 2 Airports IT Infrastructure Πηγή: [7]

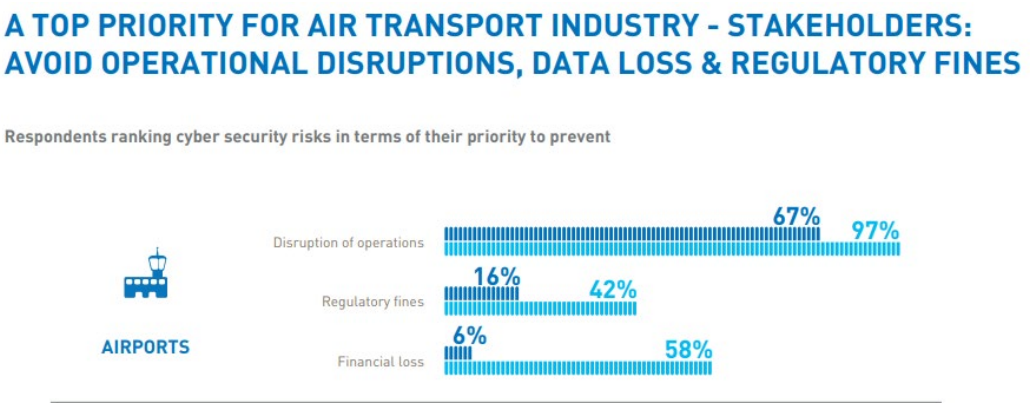
Κεφάλαιο 3
Ασφάλεια Πληροφοριακών συστημάτων

3.1 Κυβερνοαπειλές στα έξυπνα αεροδρόμια

Έχοντας πλέον ορίσει το τι είναι ένα έξυπνο αεροδρόμιο αλλά επίσης και την υποδομή που στηρίζεται για να μπορεί να διενεργεί τις επιχειρησιακές του δραστηριότητες συμπεριλαμβανομένης και την προσφορά υπηρεσιών στους διάφορους φορείς θα προχωρήσουμε στην ανάλυση κινδύνων και απειλών που αντιμετωπίζουν.

Ένας λεπτομερής πίνακας δίνεται από τον ENISA [2] που εμπεριέχει μια γκάμα από κυβερνοαπειλές που μπορεί να στοχεύσουν και να επηρεάσουν τα αντίστοιχα έξυπνα αεροδρομιακά συστήματα. Στον πίνακα 3 βλέπουμε τις κακόβουλες και στοχευμένες επιθέσεις προς τον αεροδρομιακό τομέα , διαπιστώνοντας ότι στο αεροδρομιακό περιβάλλον ισχύουν οι περισσότεροι τύποι επιθέσεων οι οποίοι εμφανίζονται και σε άλλους οργανισμούς.

Σύμφωνα με την αναφορά AIR TRANSPORT CYBERSECURITY 2 INSIGHTS 2018 [10], μια μελέτη που ανατέθηκε στην State Information Technology Agency (SITA), ο αεροδρομιακός τομέας έχει σαν κύρια απειλή την διακοπή υπηρεσιών από επικείμενες επιθέσεις όπως φαίνεται και στην εικόνα 3.



Εικόνα 3 Πηγή: 2018 AIR TRASNPORT CYBERSECURITY INSIGHTS 2018

Οι Κακόβουλες ενέργειες μπορεί να χαρακτηριστούν σαν διάφορες μέθοδοι που μπορούν να χρησιμοποιηθούν από άτομα με κακόβουλη πρόθεση για να στοχεύσουν αεροδρομιακά συστήματα με σκοπό να διακόψουν την ομαλή λειτουργία των αεροδρομίων. Κάθε μία από αυτές τις επιθέσεις μπορεί να αποτελέσει παραβίαση του τρίπτυχου CIA, δηλαδή της παραβίασης του απορρήτου (Confidentiality), της ακεραιότητας (Integrity), της διαθεσιμότητας (Availability) των πληροφοριακών συστημάτων, των πληροφοριών που αποθηκεύουν και γενικότερα ολόκληρης της υποδομής.

Κατηγορία	Τύπος Επίθεσης
Κακόβουλες επιθέσεις (Malicious Attacks)	Άρνηση υπηρεσίας - (DoS)Denial of Service (DoS)
	Εκμετάλλευση τρωτών σημείων λογισμικού (Exploitation of software Vulnerabilities)
	Κατάχρηση εξουσίας / (Misuse of authority / authorisation)
	Επιθέσεις δικτύου/υποκλοπών (Network/interception attacks)
	επίθεση κοινωνικής μηχανικής (Social attacks)
	Παραβίαση συσκευών αεροδρομίου (Tampering with Airport Devices)
	Παραβίαση φυσικών ελέγχων πρόσβασης / διαχειριστικών ελέγχων (Breach of physical access controls / administrative controls)
	Κακόβουλο λογισμικό σε στοιχεία πληροφορικής (Malicious software on IT assets)
	επιθέσεις σε περιουσιακά στοιχεία του αεροδρομίου (Physical attacks on airport assets)

Πίνακας 3 Τύποι Κακόβουλων επιθέσεων

Μια επίθεση άρνησης υπηρεσίας (DDos) είναι μια κακόβουλη προσπάθεια να διακοπεί η κίνηση του δικτύου προς ένα server, προς μια υπηρεσία ή ένα άλλο δίκτυο συντρίβοντας τον στόχο ή την υποδομή του με μια διαδικτυακή κίνηση (Internet Traffic) που ονομάζεται «πλημμύρα» (flood) .

Η εκμετάλλευση ευπαθειών λογισμικού είναι ένας ακόμα πιθανός τρόπος να υλοποιηθεί μια κυβερνοεπίθεση στη υποδομή των αεροδρομίων. Θέματα ασφάλειας που μπορεί να έχουν επιλυθεί με διάφορες αναβαθμίσεις ασφάλειας (Security Patches), λόγω των επιχειρησιακών δραστηριοτήτων ενός αεροδρομίου σε φυσικό εύρος αλλά και σε χρόνο (επί εικοσιτετράωρού βάσεως) μπορεί να μην υλοποιούνται στα συστήματα παραγωγής.

Οι επιθέσεις κοινωνικής δικτύωσης έχουν σκοπό να εκμεταλλευτούν το έμψυχο δυναμικό των αεροδρομίων ώστε να κλέψουν στοιχεία από το προσωπικό όπως το όνομα χρήστη και τον κωδικό τους. Οι επιθέσεις κοινωνικής δικτύωσης μπορεί να οδηγήσουν και σε άλλες μορφές επιθέσεων όπως για παράδειγμα privilege escalation attacks αλλά και την εγκατάσταση κακόβουλου λογισμικού (malware).

Είναι πολύ σημαντικό να μην ξεχνάμε ότι σε ένα τεράστιο αεροδρομιακό περιβάλλον είναι πολύ δύσκολο να περιορίσουμε την φυσική πρόσβαση σε όλα τα συστήματα πληροφορικής. Για παράδειγμα, υπολογιστές που χρησιμοποιούνται για την διαδικασία του check-in αλλά και κατά διάρκεια της επιβίβασης των επιβατών και διάφορες θύρες (port) δικτύου είναι εκτεθειμένες στο ευρύ κοινό με αποτέλεσμα να μην υπάρχει ιδιαίτερος βαθμός δυσκολίας να πραγματοποιηθούν επιθέσεις όπως βανδαλισμοί, παραβίαση αυτών των συσκευών ακόμα και επιθέσεων υποκλοπών με ενσύρματα αλλά και ασύρματα μέσα.

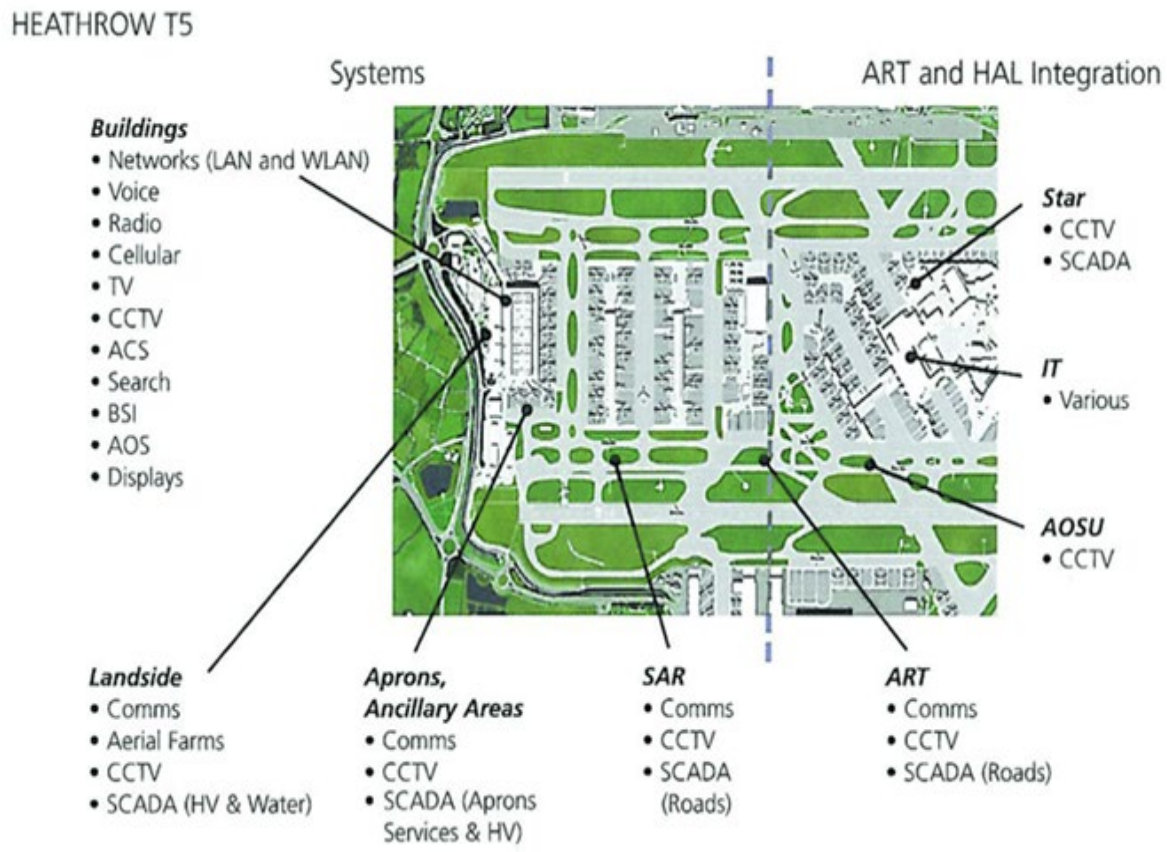
Επιπρόσθετα οι τύποι επιθέσεων αντιστοιχούνται στα αεροδρομιακά συστήματα τα οποία μπορούν να επηρεαστούν. Μερικά από τα αεροδρομιακά συστήματα είναι τα πιο κάτω:

- Κοινή πλατφόρμα επεξεργασίας επιβατών (Common-Use Passenger Processing Systems (CUPPS))
- Σύστημα πληροφοριών πτήσεων (Flight Information Display System (FIDS))

- SCADA
- Συσκευές Kiosk για ηλεκτρονικά εισιτήρια (Kiosk Devices (E-ticketing))
- Συστήματα ελέγχου φωτισμού αεροδρομίου και παρακολούθησης διαδρόμου (Airfield Lighting Control Systems and Runway Monitoring)

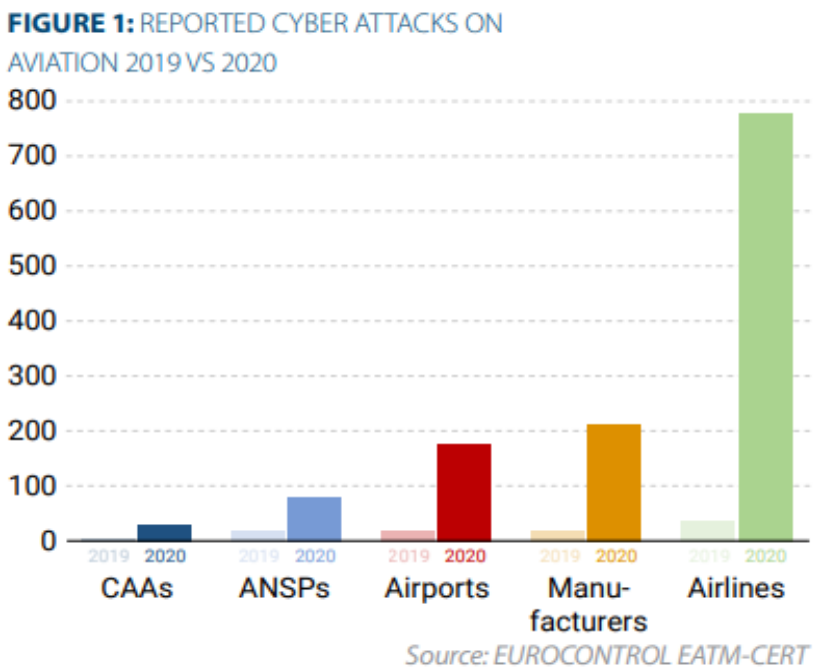
Η χρήση των IoT συσκευών είναι διάχυτη σε ολόκληρο το αεροδρομιακό περιβάλλον. Σύμφωνα με την έκθεση του ENISA [2] αλλά και το άρθρο " Cyber Security For Airports" [5], όπου δίνεται η εικόνα 4 που απεικονίζει τις τεράστιες περιοχές που διαθέτει μια υποδομή αεροδρομίου όπου διάφοροι υπάλληλοι της διαχειρίστριας εταιρείας αλλά και φορείς υπηρεσιών, πρέπει να έχουν πρόσβαση στις απομακρυσμένες τοποθεσίες που φιλοξενούν κρίσιμα συστήματα πληροφορικής. Η διάσπαρτη τοποθεσία αυτών των έξυπνων συσκευών αυξάνει τον κίνδυνο περιστατικών ασφάλειας στον κυβερνοχώρο που προέρχονται από εσωτερικές απειλές, καθώς αυτές οι τοποθεσίες είναι συχνά ανεπιτήρητες .

Επιπλέον, οι συσκευές IoT μπορούν να χαρακτηριστούν ως εφαλτήρια σημεία για πολλές κυβερνοεπιθέσεις, επομένως ένας συνδυασμός μη εποπτευόμενων τοποθεσιών που φιλοξενούν πιθανά σημεία εκτόξευσης κυβερνοεπιθέσεων μπορεί να θέσει σε κίνδυνο μια ολόκληρη κρίσιμη υποδομή. Κατά τη διάρκεια της έρευνάς τους, οι Ukwandu et al. [4], προβλέπουν ότι οι απειλές στον κυβερνοχώρο στον κλάδο της πολιτικής αεροπορίας θα αυξηθούν για διάφορους λόγους. Η συνεχής ανάπτυξη του κλάδου και η εξάρτηση από συσκευές IoT είναι δύο από τους κύριους λόγους.



Εικόνα 4 Τοποθεσίες IoT συσκευών [5]

Η αναφορά του EUROCONTROL EATM-CERT (European Air Traffic Management Computer Emergency Response Team) Services " Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?" [11] αναφέρει ότι Οι Κυβερνοεπιθέσεις που επισημάνθηκαν ή εντοπίστηκαν από την EATM- CERT του EUROCONTRO αυξήθηκαν ποσοστιαία κατά 530% μεταξύ 2019 και 2020, με εντυπωσιακές επιπτώσεις σε όλα τα τμήματα της αγοράς, όπως δείχνει η εικόνα 5.



Εικόνα 5 Κυβερνοεπιθέσεις στην Βιομηχανία Aviation 2019 VS 2020 [10]

Η STEPHERSON HARWOOD σε μια δημοσίευση της [12] αναλύει την πιο πάνω αναφορά και σχηματίζει τον ενδεικτικό πίνακα που παρουσιάζεται στο Παράρτημα Β της παρούσας διατριβής με τις πιο πρόσφατες και σοβαρές κυβερνοεπιθέσεις και καταλήγει στο συμπέρασμα ότι " Όπως φαίνεται από αυτά τα παραδείγματα, πολλά από τα μεγαλύτερα περιστατικά στον κυβερνοχώρο τα τελευταία 7 χρόνια σχετίζονται με την κλοπή εξαιρετικά ευαίσθητων προσωπικών δεδομένων που σχετίζονται με επιβάτες, συμπεριλαμβανομένων στοιχείων πιστωτικής κάρτας, στοιχείων διαβατηρίου και δεδομένων αρχείου ονομάτων επιβατών ("PNR"). Επί του παρόντος αυτού του είδους η επίθεση, μαζί με την κλοπή πολύτιμης πνευματικής ιδιοκτησίας από κατασκευαστές, είναι ίσως οι πιο πιεστικές απειλές που αντιμετωπίζει η βιομηχανία. Ωστόσο, καθώς διερευνούμε λεπτομερέστερα παρακάτω, η αυξανόμενη εξάρτηση της αεροπορικής βιομηχανίας από πολύπλοκα και αλληλένδετα συστήματα τεχνολογίας πληροφοριών σημαίνει ότι υπάρχουν πλέον περισσότερες ευκαιρίες για κυβερνοεπιθέσεις με στόχο αεροσκάφη και αεροδρόμια απευθείας από ό,τι ποτέ πριν"

Οι τύποι των επιθέσεων αναφέρονται επιγραμματικά πιο κάτω :

- Ransomware attack

- Third-party software system failure.
- DDos Attack
- Phishing Attacks
- Malicious Code Attack
- Sophisticated Cyber Attacks

3.2 Ευπάθειες Ασφαλείας

Οι Ευπάθειες ασφαλείας είναι αδυναμίες ή άλλες συνθήκες σε έναν οργανισμό που ένας παράγοντας απειλής, όπως ένας χάκερ, ένα εχθρικό κράτος, ένας δυσαρεστημένος υπάλληλος ή άλλοι εισβολείς, μπορεί να τις εκμεταλλευτεί για να επηρεάσει αρνητικά την ασφάλεια δεδομένων.

Το ψηφιακό αποτύπωμα κάθε οργανισμού καθημερινά μεγαλώνει με την χρήση νέων και καινοτόμων τεχνολογιών. Αυτό έχει σαν φυσικό επακόλουθο να δημιουργούνται καινούργιες ευπάθειες που αυτό με την σειρά του αυξάνει τις πιθανότητες για επιτυχημένες επιθέσεις που θα μπορούσαν να οδηγήσουν σε παραβίαση συστημάτων ή δεδομένων και να επηρεάσουν αρνητικά τους επιβάτες και το προσωπικό της κοινότητας του αεροδρομίου, επιπλέον θέτουν σε κίνδυνο τη συμμόρφωση με τις νομικές υποχρεώσεις ενός οργανισμού, εκτός από τις υλικοτεχνικές ζημιές που μπορεί να προκληθούν. Επομένως, κάθε εταιρεία πρέπει να λαμβάνει υπόψη το περιβάλλον στο οποίο θα δραστηριοποιείται. Οι συσκευές IoT αποτελούν μέρος αυτού του περιβάλλοντος.

Όπως κάθε άλλο σύστημα πληροφορικής , οι συσκευές IoT αντιμετωπίζουν προκλήσεις ασφάλειας και προστασίας πληροφοριών σύμφωνα με διάφορους αξιόπιστους οργανισμούς όπως οι ENISA, ISACA και OWASP αναγνωρίζονται οι πιο κάτω αδυναμίες:

- Αδύναμοι ή επαναχρησιμοποιούμενοι κωδικοί πρόσβασης (Weak password protection)
- Αδύναμοι μηχανισμοί αναβαθμίσεων ασφάλειας (Lack of regular patches and updates and weak update mechanism)
- Μη ασφαλείς διεπαφές (Insecure interfaces)

- Ανεπαρκής Προστασία Δεδομένων (Insufficient data protection)
- Κακοδιαχείριση συσκευών IoT (Poor IoT Device management)
- Ανεπάρκεια Δεξιοτήτων στον τομέα IoT (The IoT skills gap)
- Ανασφαλής μεταφορά και αποθήκευση δεδομένων (Insecure Data Transfer and Storage)
- Τροποποίηση Συσκευών (Device Modification)
- Διαχωρισμός Δικτυών (Network Segregation)

Είναι κατανοητό ότι καθένα από τα προαναφερθέντα «τρωτά σημεία» δεν έχει τον ίδιο αντίκτυπο και δεν μπορεί να αξιοποιηθεί με την ίδια ευκολία, ωστόσο όπως είναι πολύ γνωστό στον κόσμο της κυβερνοασφάλειας, η εκμετάλλευση ενός συνδυασμού αυτών των τρωτών σημείων μπορεί να οδηγήσει σε σημαντικά περιστατικά, που μπορούν να επηρεάσουν τις λειτουργίες οποιασδήποτε εταιρείας που χρησιμοποιεί τεχνολογίες IoT προκαλώντας ζημιά στη φήμη της .

Ο Πίνακας 4 παρακάτω περιγράφει συνοπτικά πώς οποιαδήποτε από τις πιο πάνω αδυναμίες μπορεί να αξιοποιηθεί για να επηρεάσει τις Συσκευές IoT και κατά συνέπεια τμήματα της υποδομής ενός αεροδρομίου .

Ευπάθεια	Περιγραφή	Επηρεαζόμενα στοιχεία
Αδύναμοι ή επαναχρησιμοποιημένοι κωδικοί πρόσβασης	Οι ενσωματωμένοι, προεπιλεγμένοι κωδικοί πρόσβασης είναι επιρρεπείς σε κάθε είδους γνωστές επιθέσεις, όπως επιθέσεις δυνάμεως επεξεργαστή	• IoT Devices
Μη ενημερωμένα λογισμικά (Non-Updated Software)	Τα μη ενημερωμένα, συστήματα είναι ευάλωτα και δίνουν την ευκαιρία στους επιτιθέμενους να εκμεταλλευτούν γνωστά τρωτά σημεία ασφαλείας μιας πλατφόρμας που χρησιμοποιούν τα	• IoT Devices • Other IoT Ecosystem Devices • Platform Backend • Infrastructure

	στοιχεία του IoT ή χειραγωγούν κακώς γραμμένο κώδικα ενός λογισμικού.	• Application and Services
Κακοδιαχείριση συσκευών IoT	Γενικά, η Διαχείριση Συσκευών απαιτεί μεγάλη διοικητική προσπάθεια. Οι συσκευές IoT θα πρέπει να ελέγχονται πριν εισέλθουν στο οικοσύστημα μιας εταιρείας	• IoT Devices • Infrastructure • Application Services
Ανασφαλής μεταφορά και αποθήκευση δεδομένων	Η έλλειψη κρυπτογράφησης και διαχείρισης πρόσβασης χρηστών μπορεί να οδηγήσει σε διαρροή εταιρικών ή προσωπικών δεδομένων που συλλέγονται.	• IoT devices • Other IoT Ecosystem devices • Platform & Backend Information
Μη ασφαλείς υπηρεσίες δικτύου	"Οι μη απαραίτητες ή μη ασφαλείς υπηρεσίες δικτύου που εκτελούνται στην ίδια τη συσκευή, ειδικά εκείνες που εκτίθενται στο Διαδίκτυο, θέτουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα/αυθεντικότητα ή τη διαθεσιμότητα των πληροφοριών ή επιτρέπουν τον μη εξουσιοδοτημένο απομακρυσμένο έλεγχο." Όπως ορίζεται από το OWASP (OWASP IoT2: Mitigating Insecure Network Services from https://niccs.cisa.gov/training/search/security-innovation/owasp-iot2-mitigating-insecure-network-services)	• IoT Devices • Other IoT Ecosystem Devices • Platform Backend • Infrastructure Application and Services
Διαχωρισμός Δικτυών	Η έλλειψη διαχωρισμού δικτύου με τη μη χρήση firewall ή τουλάχιστον Access Lists, μπορεί να θέσει σε κίνδυνο ολόκληρη την υποδομή της εταιρείας.	• Infrastructure

Πίνακας 4 Αδυναμίες Συσκευών IoT

Όλοι οι παραπάνω κίνδυνοι μπορούν να εντοπιστούν σε όλα τα οικοσυστήματα πληροφορικής. Ο ENISA ορίζει ένα οικοσύστημα συσκευών IoT σαν «ένα κυβερνο-φυσικό οικοσύστημα διασυνδεδεμένων αισθητήρων και ενεργοποιητών, που επιτρέπουν τη λήψη έξυπνων αποφάσεων» αντιλαμβανόμαστε ότι επεκτείνουν σε μεγάλο βαθμό το παραδοσιακό μας δίκτυο (IT Backbone) σε ένα τεράστιο, πολύπλοκο και χαοτικό δίκτυο διασυνδεδεμένων πηγών πληροφοριών, που συνδέεται άμεσα ή

έμμεσα με την υποδομή μας και που μπορεί να αποθηκεύει και να επεξεργάζεται δεδομένα

3.3 Πήγες Απειλών

Έχουν εντοπιστεί διάφορες ομάδες απειλών σύμφωνα και με την αναφορά του ENISA «ENISA THREAT LANDSCAPE 2021» [13], που μπορεί να έχουν την επιθυμία να διαταράξουν οποιαδήποτε εταιρική λειτουργία και αναφερόμαστε αναλυτικά σε αυτές παρακάτω.

Κυβερνοεγκληματίες: Είναι άτομα ή ομάδες ατόμων που εκμεταλλεύονται το διαδίκτυο και τις τεχνολογίες που σχετίζονται με το διαδίκτυο για να διαπράξουν εγκλήματα. Οι κυβερνοεγκληματίες έχουν οικονομικά κίνητρα και ποικίλλουν σε επίπεδο δεξιοτήτων και πόρων. Οι οργανωμένες εγκληματικές ομάδες μπορεί να είναι προσοντούχες και καλά εφοδιασμένες , γεγονός που τις καθιστά έναν από τους κορυφαίους παράγοντες απειλής. Καθώς το κυβερνοέγκλημα ως υπηρεσία γίνεται ολοένα και πιο διαθέσιμο και φθηνό μέσω του dark web, η αύξηση των επιθέσεων εναντίον οποιουδήποτε οργανισμού είναι πολύ πιθανή, καθώς αυτοί οι παράγοντες ανοίγουν αυτήν την επιλογή σε ένα ευρύτερο κοινό.

Hacktivists: Άτομα ή ομάδες που παρακινούνται από έναν πολιτικό, κοινωνικό ή θρησκευτικό σκοπό, για παράδειγμα, την ελευθερία του λόγου, τα ανθρώπινα δικαιώματα ή την ελευθερία της ενημέρωσης. Οι ομάδες hacktivist είναι συχνά αποκεντρωμένες και αποτελούνται από ανόμοια άτομα που μοιράζονται παρόμοιες απόψεις. Οι επιθέσεις έχουν συχνά στόχο την διακοπή των υπηρεσιών, όπως οι DDos attacks. Οι hacktivists είναι σε θέση να υποβάλλουν τα θύματά τους σε μεγαλύτερες και πιο μακροχρόνιες επιθέσεις που περιλαμβάνουν διαγραφή ή διαρροή ευαίσθητων πληροφοριών. Όπως και οι εγκληματίες του κυβερνοχώρου, οι hacktivists μπορεί να διαφέρουν ως προς το επίπεδο δεξιοτήτων και τη διαθεσιμότητα πόρων. Οι ομάδες hacktivist μπορεί να περιέχουν χιλιάδες μέλη, πολλά από τα οποία είναι εξαιρετικά εξειδικευμένα και πολυμήχανα.

Insiders: Υπάλληλοι που κατά λάθος ή κακόβουλα μπορεί προκαλέσουν κάποιου είδους ζημά σε έναν οργανισμό. Οι ακούσιες ενέργειες ή παραλείψεις, όπως το κλικ σε ένα email ηλεκτρονικού ψαρέματος, η σύνδεση ενός μολυσμένου USB stick, η λήψη μη ασφαλούς περιεχομένου από το Διαδίκτυο ή η παράβλεψη μιας πολιτικής ασφάλειας πληροφοριών θα μπορούσαν να οδηγήσουν σε παρόμοια αποτελέσματα με αυτά που προκύπτουν από τους εγκληματίες στον κυβερνοχώρο ή τους hacktivists.

Οι παραπάνω παράγοντες απειλής μπορούν να αξιοποιηθούν για την πραγματοποίηση μιας σειράς από επιθέσεις εκμεταλλευόμενοι τα τρωτά σημεία που αναφέρονται πιο πάνω. Ο παρακάτω πίνακας 6 απεικονίζει λεπτομερώς τις επιθέσεις και το αποτέλεσμα κάθε επίθεσης. Οι πληροφορίες για τη συμπλήρωση του πίνακα ελήφθησαν από τον ENISA [6] (Baseline Security Recommendations for IoT).

Επίθεση	Αποτέλεσμα
Άρνηση υπηρεσίας - DDos Attack	• Βλάβη συστημάτων - Failure of Systems • Διακοπές Δικτύου Network Outages • Απώλεια Υποστηρικτικών Υπηρεσιών - Loss of Support Services
Επίθεση κακόβουλου Λογισμικού - Malware Attack	• Βλάβη συστημάτων - Failure of Systems • Διακοπές Δικτύου Network Outages • Απώλεια Υποστηρικτικών Υπηρεσιών - Loss of Support Services
Εκμετάλλευση από κακόβουλες συσκευές -Counterfeit by Malicious Devices	• Εκμετάλλευση Υλικού - Manipulation of Hardware • Εκμετάλλευση Λογισμικού- Manipulation of Software • Δημιουργία και Χρήση Generation πλαστόν πιστοποιητικών and use of roque Certificates
Επιθέσεις κατά του - απορρήτου Privacy Attacks	• Κατάχρηση Προσωπικών Δεδομένων (Abuse of personal data) • Κατάχρηση Εξουσιοδότησης (Abuse authorizations) • Έκθεση εμπιστευτικών πληροφοριών (Compromising confidential Information)
Man in the middle	• Υποκλοπή Πληροφοριών Interception of Information

Πίνακας 5 Αποτελέσματα Απειλών [6]

3.4 Διασφάλιση έξυπνων αεροδρομίων – Ελαχιστοποίηση κινδύνων

Στο άρθρο [3], βλέπουμε ότι τα έξυπνα αεροδρόμια πρέπει να λαμβάνουν υπόψη τον αντίκτυπο (Impact) των συσκευών IoT όταν σχεδιάζουν την ασφάλεια της υποδομής πληροφορικής, καθώς οι συσκευές IoT συνδέονται με κρίσιμα στοιχεία της υποδομής είτε παρέχοντας δεδομένα είτε υποστηρίζοντας λειτουργικές διαδικασίες. Επιπλέον, περιγράφει τον τρόπο με τον οποίο θα πρέπει να χαρτογραφούνται οι επιφάνειες επίθεσης και θα πρέπει να υπάρχουν επαρκείς τεχνικοί έλεγχοι για την προστασία της ομαλής λειτουργίας ενός έξυπνου αεροδρομίου.

Μια μεθοδολογία αξιολόγησης για τον εντοπισμό τρωτών σημείων περιγράφεται από τους K. Gopalakrishnan [5], και βασίζεται σε τεχνικές αξιολογήσεις ασφάλειας πραγματοποιώντας είτε αποτίμηση ευπαθειών (vulnerability assessments) είτε δοκιμές διείσδυσης (Penetration Tests). Παρόλο που οι δύο διαδικασίες είναι παρόμοιες από πολλές απόψεις, η πιο σημαντική διαφορά είναι ότι η δοκιμή διείσδυσης (Pen Test) προσπαθεί να εκμεταλλευτεί τις ευπάθειες που ανακαλύφθηκαν: αυτή η διαδικασία μπορεί να επηρεάσει τα συστήματα παραγωγής και δηλώνεται ξεκάθαρα ότι δεν συνιστάται στα συστήματα SCADA. Η μεθοδολογία αξιολόγησης περιλαμβάνει:

- Δοκιμή διείσδυσης (Penetration Test)
- Ανίχνευση ευπαθειών (Vulnerability Scanning) όπου συμπεριλαμβάνονται :
    - Η ανακάλυψη δικτύου, Αναγνώριση θύρας και πρωτοκόλλου (Network Discovery, Port and Protocol Identification)
    - Η Ανασκόπηση διαμόρφωσης των συστημάτων (System Configuration Review)
- Απαιτήσεις συμμόρφωσης (Compliance Requirements)

Οι βέλτιστες πρακτικές Ασφάλειας Πληροφοριών για έξυπνα αεροδρόμια ομαδοποιούνται σε τρεις κατηγορίες όπως περιγράφεται από τους G. Lykou et al [1] . Η Τεχνική κατηγορία περιλαμβάνει μια σειρά τεχνικών ελέγχων όπως:

- Χρήση εφαρμογών κατά κακόβουλου λογισμικού (Antimalware)

- Αναβάθμιση λογισμικού και υλικού (Software and Hardware Updates)
- Firewalls και Τμηματοποίηση Δικτύου (Firewalls and Network Segmentation)
- Ισχυρές Μέθοδοι Αυθεντικοποίησης (Strong User Authentication)
- Αλλαγή Προκαθορισμένων Διαπιστευτηρίων (Change Default Credentials)
- Κρυπτογράφηση Δεδομένων (Data Encryption)
- Έλεγχοι για την διαχείριση ιδιωτικών συσκευών (Bring your own device controls)
- Σχέδια αποκατάστασης από καταστροφές (Disaster Recovery Plans)
- Ασφάλεια εφαρμογών & Ασφαλής σχεδιασμός (Application security & Secure design)

Η οργανωτική κατηγορία περιλαμβάνει:

- Διορισμός ενός Υπεύθυνου Ασφάλειας Πληροφορικής (Appoint an IT Security Officer).
- Εφαρμογή πολιτικών για την εγκατάσταση προγραμμάτων (Enforce rules Governing Installation of Software)
- Συνεχής Επίβλεψη της Ασφάλειας Πληροφορικής (Continuous Monitoring of Information Security)
- Εγκαθίδρυση ενός προγράμματος διαχείρισης της ασφάλειας της Πληροφορικής και συμμόρφωση με τα διεθνή πρότυπα και κανονισμούς (ISMS, International standards, and compliance Audits)
- Συμμόρφωση με την Ασφάλεια πληροφορικής από εξωτερικούς συνεργάτες (Information Security Compliance from external providers)

Οι πολιτικές και τα πρότυπα περιλαμβάνουν:

- Διαχείριση πρόσβασης χρηστών (User Access Management)
- Εξειδικευμένη εκπαίδευση στην Ασφάλεια Πληροφοριών (Specialised Information Security training)
- Απαιτήσεις ασφάλειας προσωπικού για τρίτους παρόχους (Personnel security requirements for third party providers

- Εκπαίδευση Προσωπικού Αεροδρομίου στην αντιμετώπιση περιστατικών για συστήματα πληροφορικής (Train Airport Personnel in incident response for IT systems)
- Διασφάλιση συμφωνίας πρόσβασης σε άτομα πριν από την παραχώρηση πρόσβασης (Ensure access agreement to individuals prior to grant access)
- Δοκιμή και άσκηση ικανότητας απόκρισης περιστατικού σε συστήματα πληροφορικής (Test and exercise incident response capability for IT systems)
- Βασική εκπαίδευση ευαισθητοποίησης για την ασφάλεια σε όλους τους χρήστες πληροφοριακών συστημάτων (Basic Security awareness training to all information system users)
- Έλεγχος ατόμων πριν από την εξουσιοδότηση πρόσβασης στο σύστημα πληροφορικής των αεροδρομίων (Screen individuals prior to authorize access to airports IT system)

Κεφάλαιο 4
Συστήματα Αεροδρομίων

Υπάρχει μια μεγάλη ποικιλία από συστήματα πληροφορικής που σκοπός τους είναι να υποστηρίζουν τις επιχειρησιακές δραστηριότητες των αεροδρόμιων. Σε αυτό το κεφάλαιο θα επικεντρωθούμε στα συστήματα τα οποία διαχειρίζονται τα προσωπικά δεδομένα των επιβατών με σκοπό την καλύτερη εξυπηρέτηση τους σαν μέρος των εργασιών τους. Οι εφαρμογές αυτές μπορούν να βρεθούν στο στρώμα ενοποίησης (Integration Layer) αλλά και στο στρώμα εφαρμογών (Application Layer).

4.1 Μηνύματα IATA

Τα αεροδρομιακά συστήματα έχουν την ιδιότητα να λαμβάνουν μηνύματα διάφορων τύπων. Τα μηνύματα αυτά είναι μηνύματα τα οποία καθορίζονται από την Διεθνή Ένωση Αερομεταφορών (IATA). Οι αερομεταφορείς αλλά και τα αεροδρόμια γενικότερα που βρίσκονται σε κράτη μέλη της ευρωπαϊκής ένωσης έχουν την υποχρέωση για την διαβίβαση των σωστών πληροφοριών όσον αφορά αυτά τα άτομα και το είδος της αναπηρίας ή προβλήματος κινητικότητας που αντιμετωπίζουν για να τους παρασχεθούν τα κατάλληλα μέσα για να ταξιδέψουν με άνεση και ασφάλεια. Οι πληροφορίες αυτές που εμπεριέχουν ευαίσθητα προσωπικά δεδομένα τροφοδοτούνται σε μορφή μηνυμάτων Passenger Service Message (PSM), Passenger Assistance List(PAL), Change Assistance List (CAL) σε διαφορά πληροφοριακά συστήματα.

Το μήνυμα Passenger Service Message (PSM) καθορίζεται από το Recommended Practice 1715 της IATA και έχει σκοπό να ενημερώσει τους επόμενους σταθμούς και τα αεροδρόμια για τις ειδικές ανάγκες που μπορεί να έχει κάποιο άτομο που ταξιδεύει. Η ανάγκη του επιβάτη καταχωρείται σε ένα ηλεκτρονικό σύστημα κρατήσεων (Computer Reservation System (CRS)) χρησιμοποιώντας ένα κωδικό που λέγεται Special Services Request (SSR).

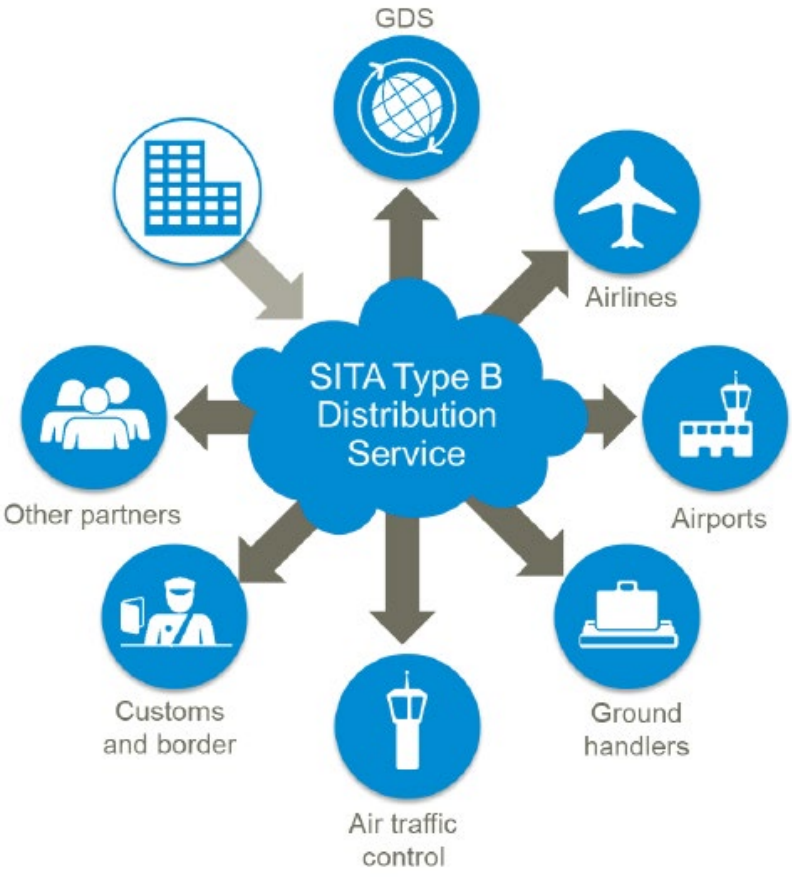
Όπως απεικονίζεται πιο κάτω, αυτά τα μηνύματα εμπεριέχουν δεδομένα όπως το όνομα και το επίθετο του ατόμου που ταξιδεύει, την πτήση του αλλά και το είδος αναπηρίας του.

```
1WILSON/GRACEANNEMRS 22B
BLND TRAVELLING WITH SERVICE ANIMAL. MONKEY NAMED SAMMY.
DEAF ABLE TO HEAR SPEAKER CLOSE TO EAR
MAAS
-ATH 3PAX/6SSR
BLND 000F 002Y
MAAS 000F 002Y
MEDA 000F 001Y
STCR 000F 001Y
F CLASS NIL
```

Εικόνα 6 Passenger Service Message Πηγή : http://wiki.aviabit.ru/doku.php?id=pub:psm_manual

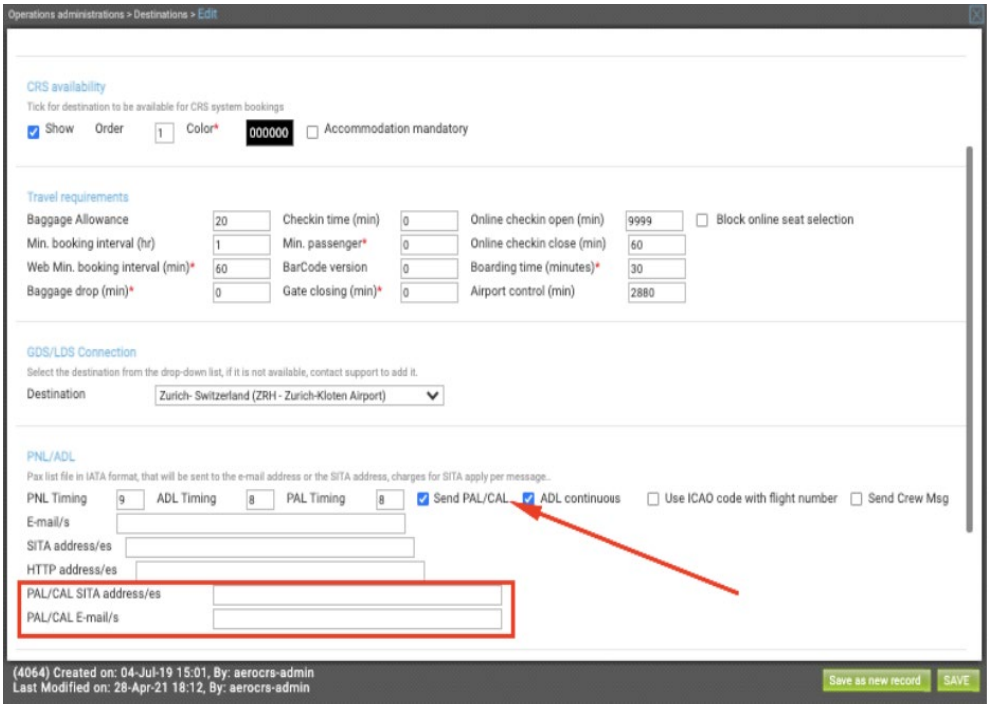
Τα μηνύματα Passenger Access List (PAL) σύμφωνα με το Recommended Practice 1708a της IATA είναι μια λίστα επιβατών PRM με το είδος της αναπηρίας ή προβλήματος κινητικότητας που μπορεί να αντιμετωπίζουν. Το μήνυμα παράγεται από το σύστημα κρατήσεων της αεροπορικής εταιρείας (CRS). Ένα PAL στέλνεται για κάθε αεροδρόμιο από το οποίο αναχωρεί μια πτήση αλλά και αφικνείται σε οποιοδήποτε αεροδρόμιο της Ευρώπης. Η λίστα αυτή επί της ουσίας εμπεριέχει τα ονόματα των επιβατών και το είδος του SSR που τους αντιστοιχεί. Το CAL είναι μια ενημερωμένη λίστα με τις αλλαγές που μπορεί να υπάρξουν. Τα PAL μηνύματα πάντα στέλνονται αν και μπορεί να υπάρχουν PRM επιβάτες, αν δεν υπάρξουν αλλαγές τότε τα CAL μηνύματα δεν στέλνονται.

Επιπρόσθετα είναι σημαντικό να προσθέσουμε ότι αποστέλνονται σε μια αποκλειστική διεύθυνση SITA του αεροδρόμιου ή μιας ηλεκτρονικής διεύθυνσης [14]. Η διευθυνσιοδότηση αυτών των μηνυμάτων γίνεται μέσω ενός συστήματος που ονομάζεται Type-B. Το Type B είναι ένα store-and-forward σύστημα επικοινωνιών που υποστηρίζει παγκόσμιες επιχειρησιακές εφαρμογές, υπηρεσίες βάσεων δεδομένων και διαπροσωπικές επικοινωνίες. Όπως συμβαίνει με όλες τις υπηρεσίες store-and-forward, η επικοινωνία Type B είναι one-way και η παράδοση πραγματοποιείται σύμφωνα με ένα σύστημα κωδικών προτεραιότητας τεσσάρων επιπέδων που κυμαίνονται από άμεσες έως αναβαλλόμενες.

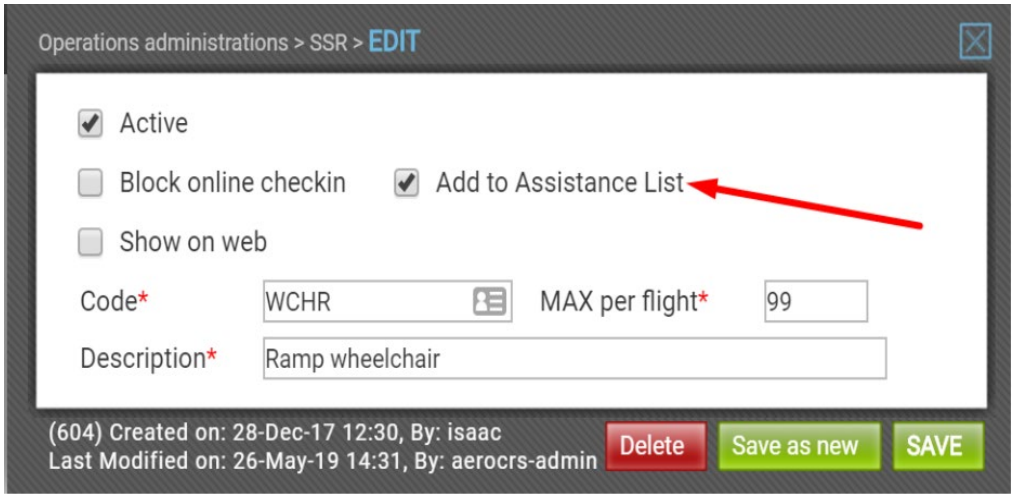


Εικόνα 7 SITA Type B Distribution Service, Source: https://www.sita.aero/globalassets/docs/use-cases/type-b-distribution-service-use-case.pdf

Ένα τυπικό παράδειγμα αποστολής αυτό των μηνυμάτων φαίνεται στις εικόνες 8,9 γραφικό περιβάλλον διεπαφής χρήστη της AeroCRS [15] οπού είναι ένα Σύστημα Εξυπηρέτησης Επιβατών (Passenger Service System - PSS) που βασίζεται σε τεχνολογία νέφους για τη διαχείριση και τη λειτουργία δρομολογίων για υπηρεσίες μεταφοράς, όπως αεροπορικές εταιρείες.

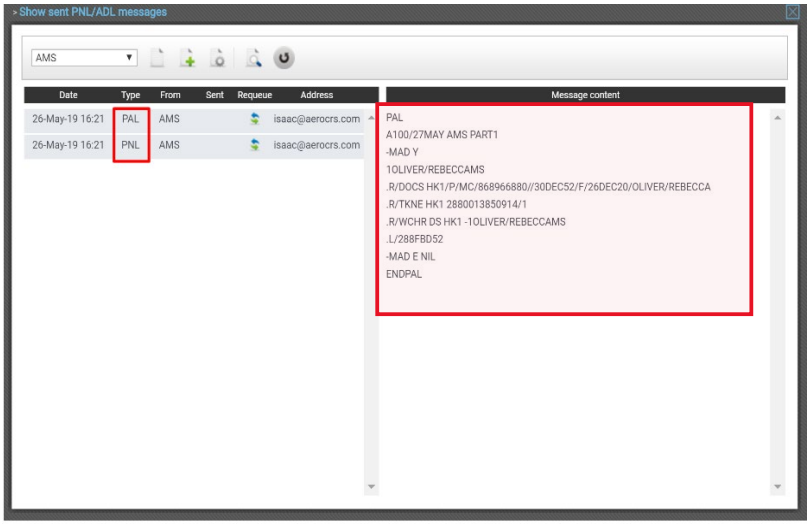


Εικόνα 8 PAL/CAL CRS Πηγή: https://support.aerocrs.com/hc/en-us/articles/360028504072-26-MAY-2019-PAL-CAL-messages



Εικόνα 9 Πρόσθεση Επιβάτη στην PAL Λίστα CRS Πηγή: https://support.aerocrs.com/hc/en-us/articles/360028504072-26-MAY-2019-PAL-CAL-messages

Στην εικόνα 10 παρουσιάζεται η δομή των μηνυμάτων PAL οπού αναγράφονται τα ονόματα των επιβατών και το είδος βοήθειας που χρειάζονται. Στο συγκεκριμένο μήνυμα βλέπουμε ότι οι επιβάτες κάνουν χρήση αναπηρικού αμαξιδιού.



Εικόνα 10 Δομή PAL Μηνύματος CRS Πηγή: https://support.aerocrs.com/hc/en-us/articles/360028504072-26-MAY-2019-PAL-CAL-messages

Ο πίνακας 6 είναι ενδεικτικός και αποτυπώνει το είδος του SSR που χρησιμοποιείται για τις ανάγκες που μπορεί να έχει κάποιος επιβάτης. Να σημειωθεί ότι τα SSR codes καθορίζονται στο AIRIMP που είναι το εγχειρίδιο ATA / IATA (Reservations Interline Message Procedures) που παράγεται και διανέμεται από την IATA με σκοπό την ανάπτυξη ενός προτύπου επικοινωνίας μεταξύ των συστημάτων κρατήσεων αεροπορικών εταιρειών (CRS) και των Departure Control System (DCS)

SSR CODE	Περιγραφή
BLND	Τυφλός επιβάτης (προσδιορίστε εάν συνοδεύεται ή όχι από σκύλο-οδηγό)
CHLD	Παιδί
DEAF	Κουφός
DEPA	Απέλαση, Συνοδευόμενος από συνοδό
DEPU	Απέλαση , Ασυνόδευτος
WCHR	Αναπηρικό αμαξίδιο - για ράμπα
WCHS	Αναπηρικό αμαξίδιο - πάνω και κάτω σκαλοπάτια
WCOB	Αναπηρικό αμαξίδιο - επί του σκάφους
WEAP	Όπλα, πυροβόλα όπλα ή πυρομαχικά που μεταφέρονται ως παραδοτέες
*UMNR	Ασυνόδευτος ανήλικος (καθορίστε την ηλικία)

Πίνακας 6 SSR CODES ΠΗΓΗ: https://servicehub.amadeus.com/c/portal/view-solution/768896/special-services-request-ssr-codes-and-airline-specific-codes

4.2 Βάση Επιχειρησιακών Δεδομένων Αεροδρομίου

Η Βάση Επιχειρησιακών Δεδομένων Αεροδρομίου (Airport Operations Database (AODB)) χαρακτηρίζεται σαν ο «πυρήνας» που επιτρέπει στο αεροδρόμιο να εκτελεί τις επιχειρησιακές του δραστηριότητες. Μέσω του AODB γίνεται η κατανομή πόρων του αεροδρομίου. Το σύστημα συλλέγει πληροφορίες από το σύστημα ελέγχου εναέριας κυκλοφορίας Traffic Control System (ATC), το σύστημα ανάθεσης κενών θέσεων Slot Assignment System (SAS) και γενικά, όλα τα συστήματα που σχετίζονται με τις λειτουργίες εντός του αεροδρομίου, με άμεση ενημέρωση για αλλαγές στις πτήσεις ώστε να γίνεται η καταλληλά ανάθεση των πόρων του αεροδρομίου.

Μπορεί να είναι μια ανοιχτή εφαρμογή που στέλνει επίσης πληροφορίες σε όλα τα άλλα εξωτερικά συστήματα όπως Flight Information Display Systems (FIDS), Baggage Reconciliation Systems (BRS), Web Servers και, φυσικά άλλες εφαρμογές που μπορούν να ενοποιηθούν μαζί του.

Υπάρχουν AODB εφαρμογές οι οποίες μπορεί να λαμβάνουν μηνύματα PAL/CAL, με αυτόν τον τρόπο ο διαχειριστής του αεροδρομίου μπορεί να έχει μια σφαιρική εικόνα για τους αναμενομένους PRM επιβάτες και πως να τους εξυπηρετήσει.

4.3 Διακομιστής Μηνυμάτων

Ο διακομιστής μηνυμάτων (Message Broker) είναι ένα ενδιάμεσο λογισμικό (middleware) που έχει την δυνατότητα να στέλνει και λαμβάνει μηνύματα από και προς διάφορα συστήματα και εφαρμογές ανεξαρτήτου πρωτοκόλλου που μπορεί να χρησιμοποιούν. Η Εικόνα 11, παρουσιάζει μια χαρτογράφηση των συστημάτων που μπορεί να επικοινωνήσει ένας Message Broker.

Εικόνα 11 Message Broker Πηγή : https://www.resa.aero/cms/FAIRWAY_Datasheet.pdf

Όπως φαίνεται και στην εικόνα 11 , ένας message broker μπορεί να στέλνει μηνύματα PAL/CAL, BSM αλλά και άλλους τύπους μυνημάτων σε διαφορά αεροδρομιακά συστήματα όπως :

1. Βάση Επιχειρησιακών Δεδομένων Αεροδρομίου (AODB)
2. Σύστημα Αντιστοίχισης Αποσκευών (BRS)
3. Αυτοματοποιημένα Συστήματα Ελέγχου Πρόσβασης (E-GATES)
4. Συστήματα επεξεργασίας επιβατών κοινής χρήσης(CUPPS)

4.4 Σύστημα Αντιστοίχισης Αποσκευών

Το σύστημα αντιστοίχισης αποσκευών (Baggage Reconciliation System) είναι ένα πλήρες σύστημα αντιστοίχισης και παρακολούθησης αποσκευών που έχει σχεδιαστεί για να παρακολουθεί συνεχώς τις αποσκευές από το Check-in μέχρι τη φόρτωσή τους στο αεροσκάφος. Θεωρείται ένα κρίσιμο σύστημα σε θέματα ασφάλειας και είναι επίσης απαραίτητο εργαλείο για την ποιότητα της εξυπηρέτησης των επιβατών.
Κύρια χαρακτηριστικά και πλεονεκτήματα του BRS είναι:

- Αντιστοίχιση αποσκευών με επιβαίνοντες
- Παρακολούθηση αποσκευών από το Check-in έως τη φόρτωση στο αεροσκάφος
- Μείωση αποσκευών που χάνονται ή στέλνονται σε λάθος προορισμό

- Γρήγορη εκφόρτωση αποσκευών εάν είναι απαραίτητο
- Όλες οι λειτουργίες καταγράφονται
- Φιλική προς το χρήστη λύση

Σε διασύνδεση με την AODB του αεροδρομίου και τα DCS των αεροπορικών εταιριών, το BRS πρεπει να παρέχει συνεχώς αξιόπιστες πληροφορίες για τη θέση των αποσκευών καθ' όλη τη διάρκεια του ταξιδιού του επιβάτη από τα Check-in μέχρι το σημείο φόρτωσης του αεροσκάφους.

Κατά την διάρκεια του Check-in τα συστήματα αυτά λαμβάνουν πληροφορίες όπως όνομα του επιβάτη, αριθμό και ημερομηνία πτήσης , την θέση του επιβάτη, τον αριθμό αποσκευών του επιβάτη, αριθμός ακολουθίας επιβατών (SQNR) της πτήσης όπως φαίνεται κα στην εικόνα 12.

Η πιο πάνω διαδικασία καθίσταται δυνατή μέσω των μηνυμάτων Baggage Source Message (BSM). Τα BSM είναι σχεδιασμένα σύμφωνα με το Recommended Practice 1745 της IATA. Ένα BSM αποστέλνεται από έναν αερομεταφορέα μέσω το συστήματος DCS του στον διαχειριστή του συστήματος BRS. Αυτό καθίσταται δυνατόν μέσω ενός message broker που έχει την δυνατότητα να λαμβάνει τα μηνύματα και να τα αποστέλλει στα κατάλληλα συστήματα, σε αυτήν την περίπτωση στο BRS.

Type 'B' Message – Sent to a sortation or reconciliation system in ZRH by SR

ZRHBSSR ZRHBRXH<Ξ	Address of sortation (BS) and reconciliation (BR)
.HDQKMSR 311800<Ξ	Signature of sender of message
BSM<Ξ	Standard Message Identifier
.V/1TZRH//6543210014/A/123ABC456Z<Ξ	Version; Transfer bag at ZRH; Ref. Nbr; Ack. Req. with encryption
.F/SR101/18APR/JFK/F<Ξ	Outbound carrier and flight; Date; Dest.; Class
.I/AZ318/18 APR/FCO/J<Ξ	Inbound carrier and flight; Date; Originating airport; Class
.N/0085123456003<Ξ	Bag tag number; Number of consecutive tags
.S/Y/3A/C<Ξ	Reconciliation data: Auth. to load; seat 3A; checked in
.P/SMITH/TOM<Ξ	Passenger name
.L/XY1C3P<Ξ	Automated PNR Address
.T/321A4C<Ξ	Printer ID
.E/RUSH<Ξ	Rush bag
.R/VIP<Ξ	Internal airline data
.X/XRAY<Ξ	Screening Description
ENDBSM<Ξ	End of Message Identifier

Εικόνα 12 Δομή Μηνύματος BSM Πηγή: https://wiac.info/docview

Μέσω της χρήσης φορητών scanners (IoT Device), οι χειριστές αποσκευών έχουν πρόσβαση στις πληροφορίες που παράγονται από την όλη διαδικασία σε πραγματικό χρόνο και μπορούν εύκολα να εντοπίσουν αποσκευές και να αναγνωρίσουν αποσκευές. Η όλη διαδικασία μπορεί να παρακολουθείται και από διάφορα τερματικά (Terminal Workstation) που έχουν πρόσβαση στην εφαρμογή.

4.5 Αυτοματοποιημένα Συστήματα Ελέγχου Πρόσβασης

Τα αυτοματοποιημένα συστήματα ελέγχου πρόσβασης έχουν σαν κύριο χαρακτηριστικό την αξιοποίηση δεδομένων που είναι διαθέσιμα στα έγγραφα επιβίβασης (Boarding Pass), με κύριο σκοπό να δώσουν πρόσβαση στο επιβατικό κοινό στις ελεγχόμενες περιοχές. Τα συστήματα αυτά επικοινωνούν με το AODB, και ακολουθώντας ένα σετ κανόνων που παραμετροποιείται από τον κάθε διαχειριστή του αεροδρομίου σε συνεργασία με τις εποπτικές αρχές της κάθε χώρας για να δοθεί νόμιμη και ασφαλή πρόσβαση στους χώρους αναχωρήσεων των επιβατών.

Οι πληροφορίες που εμπεριέχονται σε μια κάρτα επιβίβασης όπως φαίνεται και στην εικόνα 13 είναι το όνομα και το επίθετο του επιβάτη, η πτήση του, η ημερομηνία αναχώρησης του, το αεροδρόμιο αναχώρησης και άφιξης.

	New item number	Element Description	Field Size	Unique / repeated	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Notes
Mandatory Items	1	Format Code	1	U	M																				
	5	Number of Legs Encoded	1	U	1																				
	11	Passenger Name	20	U	D	E	S	M	A	R	A	I	S	/	L	U	C								
	253	Electronic Ticket Indicator	1	U	E																				
	7	Operating carrier PNR Code	7	R	A	B	C	1	2	3															
	26	From City Airport Code	3	R	Y	U	L																		
	38	To City Airport Code	3	R	F	R	A																		
	42	Operating carrier Designator	3	R	A	C																			
	43	Flight Number	5	R	0	8	3	4																	
	46	Date of Flight (Julian Date)	3	R	2	2	6																		August 14th
	71	Compartment Code	1	R	F																				
	104	Seat Number	4	R	0	0	1	A																	
	107	Check-in Sequence Number	5	R	0	0	2	5																	
	113	Passenger Status	1	R	1																				
	6	Field Size of variable size field (Conditional + Airline item 4)	2	R	0	0																			0 in Decimal = 00 in Hexadecimal

Εικόνα 13 Πληροφορίες Κάρτας Επιβίβασης Πηγή : https://tinkrmind.files.wordpress.com/2017/09/bcbp-implementation-guide-5th-edition-june-2016.pdf

Τα συστήματα αυτά μπορούν να φορτωθούν σε διάφορες συσκευές IoT όπως ηλεκτρονικές πύλες επιβίβασης και φορητά scanners. Οι συσκευές αυτές έχουν την δυνατότητα να χρησιμοποιούν διάφορα λειτουργικά συστήματα όπως Android και Windows. Στην εικόνα 14 φαίνεται η χρήση μιας κάρτας επιβίβασης με μια ηλεκτρονική Πύλη.

Τα συστήματα αυτά όμως με επιπρόσθετες παραμετροποιήσεις μπορούν προσφέρνουν και τις πιο κάτω υπηρεσίες :

- Διαχείριση της παρουσίας των επιβατών στη ζώνη επιβίβασης .
- Σαν εργαλείο μάρκετινγκ για την παρακολούθηση των επιβατών.
- Προσδίδουν πρόσβαση προτεραιότητας σε επιβάτες που έχουν αγοράσει τις ανάλογες υπηρεσίες.
- Μπορεί να ενοποιηθεί με το BRS και να πρόσδοση πληροφορίες για την φυσική παρουσία του επιβάτη στον χώρο τον αναχωρήσεων μαζί με την κατάσταση που βρίσκονται οι αποσκευές του.

Εικόνα 14 Ηλεκτρονική Πύλη Πηγή: https://www.gunneboentrancecontrol.com/en/products/boardsec/

4.6 Συστήματα επεξεργασίας επιβατών κοινής χρήσης

Τα συστήματα Common Use Passenger Processing Systems (CUPPS) σύμφωνα με την TAV Technologies [16] , "είναι ένα παγκοσμίως αποδεκτό πρότυπο που εισήχθη από τη Διεθνή Ένωση Αεροπορικών Μεταφορών (IATA) και περιγράφει το εύρος των υπηρεσιών, προδιαγραφών και προτύπων που έχουν θεσπιστεί για να επιτρέψουν σε πολλές αεροπορικές εταιρείες, παρόχους υπηρεσιών ή άλλους χρήστες να μοιράζονται φυσικούς ελέγχους - θέσεις στα Check-In ή στις πύλες επιβίβασης είτε ταυτόχρονα είτε διαδοχικά. Παραδοσιακά, κάθε αεροπορική εταιρεία θα είχε τα ειδικά γραφεία Check-in και τα τεχνικά της συστήματα, ενώ με το CUPPS, οι αεροπορικές εταιρείες και άλλοι ενδιαφερόμενοι φορείς του αεροδρομίου μοιράζονται εύκολα τον ίδιο εξοπλισμό.

Οι Πλατφόρμες CUPPS πρεπει να είναι πιστοποιημένες σύμφωνα με τα τελευταία τεχνικά χαρακτηρίστηκα που εκδίδει η IATA. Κάθε αεροπορική εταιρεία επί της ουσίας μπορεί να φορτώσει το δικό της Departure Control System (DCS) και να χρησιμοποιήσει τα κοινά περιφερειακά εργαλεία όπως υπολογιστές στα Check-in, εκτυπωτές 2D Boarding Pass αλλά και mobile devices για να εξυπηρετήσει το επιβατικό κοινό.

Είναι εύκολο να αντιληφθούμε ότι αυτή η κοινή πλατφόρμα μπορεί για σκοπούς υποστήριξης να συλλέγει διάφορα στοιχεία σε μορφή αρχείων (logs) . Τα αρχεία αυτά εμπεριέχουν τα προσωπικά στοιχεία επιβατών όπως για παράδειγμα όνομα, επίθετο, αριθμό πτήσης, την αερογραμμή αλλά και αριθμούς πιστωτικών καρτών.

Κεφάλαιο 5
Γενικός Κανονισμός για την προστασία Δεδομένων

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) εγκρίθηκε από την Ευρωπαϊκή Ένωση (ΕΕ) και τέθηκε σε ισχύ στις 25 Μαΐου 2018. Σύμφωνα με άρθρο στην ιστοσελίδα gdpr.eu [17] είναι "ο πιο σκληρός νόμος περί απορρήτου και ασφάλειας στον κόσμο". Επιβάλλει υποχρεώσεις σε οργανισμούς οπουδήποτε στον κόσμο, εφόσον συλλέγουν, αποθηκεύουν και επεξεργάζονται δεδομένα που σχετίζονται με άτομα στην ΕΕ. Ο ΓΚΠΔ θα επιφέρει σκληρές κυρώσεις σε όσους παραβιάζουν τα πρότυπα απορρήτου και ασφάλειας, οι κυρώσεις μπορεί να φτάνουν τα δεκάδες εκατομμύρια ευρώ.

Όπως είναι φυσικό τα αεροδρόμια δεν αποτελούν εξαίρεση και επηρεάζονται άμεσα από τον ΓΚΠΔ αφού εκ φύσεως, όπως είδαμε και στο πιο πάνω κεφάλαιο, συλλέγουν, αποθηκεύουν και επεξεργάζονται μεγάλους όγκους προσωπικών δεδομένων. Στις πιο κάτω ενότητες θα γίνει μια ιστορική ανασκόπηση της εξέλιξης του Κανονισμού και θα δοθεί έμφαση στις ειδικές κατηγορίες προσωπικών δεομένων και ποιες είναι οι ευθύνες που μπορεί να έχει ο εκάστοτε οργανισμός ως υπεύθυνος επεξεργασίας δεδομένων.

5.1 Μετάβαση από Οδηγία σε Κανονισμό.

Ο Γενικός Κανονισμός για την Προστασία προσωπικών Δεδομένων (ΓΚΠΔ) θεωρείται αναγκαίος σύμφωνα με την Ευρωπαϊκή Επιτροπή [18] και αποτελεί ένα " Αναγκαίο βήμα για την ενδυνάμωση των βασικών δικαιωμάτων των πολιτών " στην ψηφιακή εποχή, αλλά και για να διευκολύνει τις επιχειρήσεις με το να απλοποιεί τους κανονισμούς για εταιρείες που βρίσκονται στον τομέα της ενοποιημένης ψηφιακής αγοράς.

Δεδομένα προσωπικού χαρακτήρα σύμφωνα με τον ΓΚΠΔ είναι " κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο

ταυτότητας, όπως όνομα, αριθμό ταυτότητας, δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσδιορίζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου".

Ο ΓΚΠΔ ήρθε να αντικαταστήσει την ΟΔΗΓΙΑ 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Σύμφωνα με τον διεθνή οργανισμό IAPP (International Association of Privacy Professionals) [18] οι κρίσιμες αλλαγές στην νομοθεσία παρουσιάζονται με περιληπτικό τρόπο στα πιο κάτω 7 σημεία:

1. Εφαρμογή της νομοθεσίας : Ο ΓΚΠΔ είναι νομοθεσία και ισχύει απευθείας σε όλες τις χώρες της Ευρωπαϊκής Ένωσης σε αντίθεση με την οδηγία που μπορούσε να εφαρμοστεί σε εθνικό επίπεδο όπως όριζε η κάθε χώρα.
2. Η συγκατάθεση (Consent) για την επεξεργασία προσωπικών δεδομένων, εφόσον είναι το μόνο δικαιολογητικό για την επεξεργασία δεδομένων (δηλαδή η μόνη νομική βάση για την επεξεργασίας) πρέπει πλέον να ανταποκρίνεται σε υψηλά αντικειμενικά κριτήρια.
3. Τα άτομα έχουν πλέον μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων με τον Κανονισμό να απαιτεί να παρέχονται στα άτομα επαρκείς πληροφορίες για την χρήση και περαιτέρω επεξεργασία των προσωπικών τους δεδομένων , αλλά και με ενίσχυση των δικαιωμάτων τους.
4. Οι Εταιρείες, φορείς και οργανισμοί οι οποίοι είναι υπεύθυνοι για την επεξεργασία προσωπικών δεδομένων - οι λεγόμενοι ως υπεύθυνοι επεξεργασίας (Data Controllers) - έχουν πλέον αυξημένες υποχρεώσεις. Αντίστοιχα, αυξημένες υποχρεώσεις έχουν πλέον και όλοι όσοι τους ανατίθεται, από κάποιον υπεύθυνο επεξεργασίας, να επιτελέσουν την επεξεργασία – οι λεγόμενοι εκτελούντες την επεξεργασία (Data Processors). Κάποιες εκ των νέων υποχρεώσεων είναι ο ορισμός ενός υπεύθυνου ατόμου για την προστασία των προσωπικών δεδομένων (Data Protection Officer) αλλά και η διεξαγωγή εκτιμήσεων αντίκτυπου (Data Protection Impact Assessments) για διεργασίες οι οποίες μπορεί να κρίνονται υψηλού ρίσκου.

5. Η μεταφορά προσωπικών δεδομένων εκτός συνόρων της Ευρωπαϊκής Ένωσης πρέπει να διασφαλίζεται με τους απαραίτητους μηχανισμούς αλλά και ότι τα δικαιώματα των ατόμων διαφυλάσσονται στο πλαίσιο της νομοθεσίας
6. Τόσο ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων όσο και ο εκτελών την επεξεργασία είναι υπεύθυνοι να εφαρμόζουν επαρκή τεχνολογικά και οργανωτικά μέτρα για την διασφάλιση των δεδομένων.
7. Ο Κανονισμός δίνει το δικαίωμα αποζημίωσης στα άτομα που έχουν παραβιαστεί τα δικαιώματα τους με βάση την νομοθεσία.

5.2 Ειδικές Κατηγορίες Προσωπικών Δεδομένων

Ο κανονισμός ορίζει συγκεκριμένες κατηγορίες προσωπικών δεδομένων σαν «Ειδικές Κατηγορίες» που χρήζουν ιδιαίτερής προστασίας (κατηγορίες γνωστές και με τον όρο «ευαίσθητα δεδομένα»). Ο λόγος είναι ότι αυτού του είδους τα δεδομένα μπορούν να παρουσιάσουν σημαντικά ρίσκα ως προς τα δικαιώματα και τις ελευθερίες των ατόμων εάν και εφοσον υπάρχει κακοδιαχείριση αυτών των δεδομένων.

Οι ειδικές κατηγορίες είναι αυτές που αποκαλύπτουν :

1. Φυλετική και εθνική καταγωγή
2. Πολιτικές πεποιθήσεις
3. Θρησκευτικά και φιλοσοφικά πιστεύω
4. Συμμετοχή σε συνδικαλιστική οργάνωση
5. Επεξεργασία γενετικών δεδομένων
6. Βιομετρικά δεδομένα με σκοπό την αναγνώριση φυσικών ατόμων
7. Δεδομένα υγείας
8. Δεδομένα για την σεξουαλική ζωή η τον σεξουαλικό προσανατολισμό ενός φυσικού ατόμου.

Ο Κανονισμός συνεχίζει και δίνει περαιτέρω καθοδήγηση για το νόημα των δεδομένων υγείας και τα ορίζει σαν “Τα δεδομένα προσωπικού χαρακτήρα σχετικά με την υγεία θα πρέπει να περιλαμβάνουν όλα τα δεδομένα που αφορούν την κατάσταση της υγείας του υποκειμένου των δεδομένων και τα οποία αποκαλύπτουν πληροφορίες για την

παρελθούσα, τρέχουσα ή μελλοντική κατάσταση της σωματικής ή ψυχικής υγείας του υποκειμένου των δεδομένων".

Αυτά τα δεδομένα μπορεί να περιλαμβάνουν πληροφορίες σαν :

1. πληροφορίες σχετικά με το φυσικό πρόσωπο που συλλέγονται κατά την εγγραφή για υπηρεσίες υγείας και κατά την παροχή αυτών προς το εν λόγω φυσικό πρόσωπο
2. Ένα αριθμό, ένα σύμβολο ή ένα χαρακτηριστικό ταυτότητας που αποδίδεται σε φυσικό πρόσωπο με σκοπό την πλήρη ταυτοποίηση του φυσικού προσώπου για σκοπούς υγείας
3. Πληροφορίες που προκύπτουν από εξετάσεις ή αναλύσεις σε μέρος ή ουσία του σώματος, μεταξύ άλλων από γενετικά δεδομένα και βιολογικά δείγματα και κάθε πληροφορία, παραδείγματος χάριν, σχετικά με ασθένεια, αναπηρία, κίνδυνο ασθένειας, ιατρικό ιστορικό, κλινική θεραπεία ή τη φυσιολογική ή βιοϊατρική κατάσταση του υποκειμένου των δεδομένων, ανεξαρτήτως πηγής.

Καθίσταται πλέον εμφανές και σύμφωνα με τις κατευθυντήριες γραμμές της νομοθεσίας και την κωδικοποίηση που γίνεται στα δεδομένα υγείας από την IATA μέσω της χρήσης των κωδικών SSR που αναλύσαμε στο 4.1 αυτής της μελέτης, ότι υπάρχει επεξεργασία δεδομένων που εμπίπτει στις ειδικές κατηγορίες δεδομένων.

Το Γραφείο Επίτροπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κυπριακής Δημοκρατίας καθορίζει ότι ο υπεύθυνος επεξεργασίας πρέπει να διενεργεί μια ΕΑΠΔ [19] όταν εκτελείται σε μεγάλη κλίμακα επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων ή προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα. Αντίστοιχες υποχρεώσεις έχουν ορίσει και οι αρμόδιες εποπτικές αρχές σε όλα τα Κράτη Μέλη της ΕΕ.

5.3 Υπεύθυνος Επεξεργασίας και Εκτελών την Επεξεργασία – Νομιμότητα της επεξεργασίας

Οι έννοιες του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία θεσπίστηκαν από την Οδηγία 95/46/ΕΚ και παραμένουν ουσιαστικά παρόμοιες βάσει του κανονισμού. Στην πράξη, η εφαρμογή αυτών των εννοιών έχει γίνει ολοένα και πιο περίπλοκη λόγω της εξελισσόμενης φύσης των επιχειρήσεων και την τάση να στηρίζονται σε συστήματα πληροφορικής αλλά και της εξωτερικής ανάθεσης εργασιών σε τρίτους . Οι έννοιες αυτές χρησιμοποιούνται για τον καθορισμό της κατανομής των νομικών υποχρεώσεων που απορρέουν από τον κανονισμό και είναι αναγκαίες για την προστασία των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων.

Σύμφωνα με τον ΓΚΠΔ δίνονται οι πιο κάτω ορισμοί:

Υπεύθυνος Επεξεργασίας: Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

Εκτελών την Επεξεργασία: Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Οι φορείς διαχείρισης των αεροδρομίων θεωρούνται υπεύθυνοι για την επεξεργασία των προσωπικών δεδομένων των επιβατών, συμπεριλαμβανομένων των επιβατών ΑμεΑ, και είναι υπόχρεοι με βάση τον κανονισμό (ΕΚ) αριθ. 1107/2006 σχετικά με τα δικαιώματα των ατόμων με αναπηρία και των ατόμων με μειωμένη κινητικότητα όταν ταξιδεύουν αεροπορικώς να τους παρέχουν επαρκείς υπηρεσίες, άρα πρεπει να έχουν σε θέση τα καταλληλά τεχνολογικά και οργανωτικά μέτρα για την προστασία αυτών των δεδομένων τους. Επιπρόσθετα, δίνεται το δικαίωμα στα αεροδρόμια να μεταφέρουν

αυτήν την ευθύνη σε τρίτους μέσω συμβάσης άρα με βάση τον ΓΚΠΔ θα μπορούσε να υπάρχει και ένας, ή περισσότεροι, εκτελούντες την επεξεργασία.

Σύμφωνα με το άρθρο 6 (1) του ΓΚΠΔ για να θεωρείται έννομη μια διεργασία επεξεργασίας προσωπικών δεδομένων από τον Υπεύθυνο Επεξεργασίας πρέπει τουλάχιστον ισχύει μια από τις πιο κάτω προϋποθέσεις :

1. Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.
2. Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.
3. Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.
4. Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
5. Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
6. Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Νοούμενου ότι πληρείται μια από τις πιο πάνω προϋποθέσεις, αλλά το είδος επεξεργασίας θεωρείται υψηλού κίνδυνου τότε ο υπεύθυνος επεξεργασίας πρεπει να διεκπεραιώσει μια εκτίμηση αντίκτυπου προσωπικών δεδομένων όπως αναφέρεται στο σημείο 5.4 της παρούσας διατριβής.

5.4 Μεθοδολογία Εκτίμησης αντίκτυπου προστασίας προσωπικών δεδομένων (ΕΑΠΔ)

Σύμφωνα με το άρθρο 35 του ΓΚΠΔ, όταν το είδος επεξεργασίας των προσωπικών δεδομένων ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τότε ο υπεύθυνος επεξεργασίας οφείλει να διενεργήσει μια εκτίμηση αντίκτυπου προσωπικών δεδομένων πριν την έναρξη της επεξεργασίας αλλά και να ζητήσει την συμβουλή του υπεύθυνου προστασίας δεδομένων (ΥΠΔ). Πρεπει να τονίσουμε ότι μια ΕΑΠΔ επιβάλλεται να διενεργηθεί και σε υφιστάμενες, κατά την έναρξη ισχύος του ΓΚΠΔ, πράξεις επεξεργασίας που επιφέρουν υψηλούς κίνδυνους.

Η εκτίμηση αντίκτυπου προστασίας προσωπικών δεδομένων (ΕΑΠΔ) μπορεί να χρησιμοποιηθεί από εταιρείες για τον εντοπισμό και την αντιμετώπιση τυχόν ζητημάτων προστασίας δεδομένων που μπορεί να προκύψουν κατά την ανάπτυξη νέων προϊόντων και υπηρεσιών ή την ανάληψη νέων δραστηριοτήτων που περιλαμβάνουν την επεξεργασία προσωπικών δεδομένων. Σε ορισμένες περιπτώσεις, ο Κανονισμός τα απαιτεί, ιδίως όταν μια δραστηριότητα επεξεργασίας μπορεί να παρουσιάζει «υψηλό κίνδυνο» για τα δικαιώματα και τις ελευθερίες ενός υποκείμενου των δεδομένων.

Με απλά λόγια, μια ΕΑΠΔ (Dara Protection Impact Assessment -DPIA) είναι η διαδικασία με την οποία οι εταιρείες μπορούν συστηματικά να αξιολογούν και να προσδιορίζουν τις επιπτώσεις των προϊόντων και υπηρεσιών που παρέχουν ως προς στην προστασία της ιδιωτικής ζωής και των δεδομένων. Δίνει τη δυνατότητα στον υπεύθυνο επεξεργασίας να προσδιορίσει τις επιπτώσεις και να λάβει τα κατάλληλα μέτρα για την πρόληψη ή, τουλάχιστον, την ελαχιστοποίηση του κινδύνου αυτών των επιπτώσεων.

Μια ΕΑΠΔ πρεπει να διενεργείται ακόμα και σε υφιστάμενες πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και στις οποίες έχει επέλθει μεταβολή των κινδύνων, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας. Αντιλαμβανόμαστε ότι με βάση την νομοθεσία και την ανάλυση των

δεδομένων που παρουσιάσαμε πιο πάνω ότι ένα έξυπνο αεροδρόμιο επεξεργάζεται ακόμα και «ειδικές κατηγορίες δεδομένων» και, σε κάθε περίπτωση, δεδομένα μεγάλης κλίμακας, αρά επί της ουσίας επιβάλλεται η διενέργεια μιας ΕΑΠΔ.

Σύμφωνα με την ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων [20], αναφέρεται ότι δεν υπάρχει συγκεκριμένη μεθοδολογία για τη διενέργεια μιας ΕΑΠΔ, και ότι το ελάχιστο περιεχόμενο της όπως ορίζει Ο ΓΚΠΔ είναι :

- «περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας»·
- «εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας»·
- «εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων»·
- «τα προβλεπόμενα μέτρα:
    - «αντιμετώπισης των κινδύνων»·
    - «απόδειξης της συμμόρφωσης με τον παρόντα κανονισμό».

Ένα από τα υποδείγματα προς χρήση που προτείνονται και πληροί τα πιο πάνω κριτήριά είναι το υπόδειγμα που προσφέρεται από το Γραφείο Επιτρόπου Πληροφοριών (ICO) του του Ηνωμένου Βασιλείου που δημιουργήθηκε για να προασπίζει τα δικαιώματα πληροφόρησης προς το δημόσιο συμφέρον.

Το υπόδειγμα περιέχει εφτά βήματα για την διεκπεραίωση της ΕΑΠΔ από έναν υπεύθυνο επεξεργασίας και αναλύονται πιο κάτω :

1. **Προσδιορισμός της ανάγκης για την διεξαγωγή ΕΑΠΔ** : Ο υπεύθυνος επεξεργασίας πρεπει να προσδιορίσει αν υπάρχει ανάγκη για την διεξαγωγή μιας ΕΑΠΔ με έναν περιληπτικό τρόπο.
2. **Περιγραφή της Επεξεργασίας** : Σε αυτό το βήμα πρεπει να περιγράφει ο κύκλος ζωής των δεδομένων, οι σκοποί της επεξεργασίας αλλά και να δοθεί το κατάλληλο περιεχόμενο για το ποιους επηρεάζει αυτή η επεξεργασία και τα είδη των δεδομένων που επιδέχονται επεξεργασία.

3. **Διαδικασία διαβούλευσης :** Σε αυτό το στάδιο πρέπει να περιγράφεται το πως και πότε θα ζητηθεί η γνώμη των ατόμων για την διαδικασία της επεξεργασίας και αν δεν ζητηθεί να καταγραφεί ο λόγος που δεν ζητήθηκε. Επίσης καταγράφεται η γνώμη του υπευθύνου ασφάλειας δεδομένων (ΥΑΔ) του οργανισμού και άλλων ειδικών σε θέματα ιδιωτικότητας.
4. **Αξιολόγηση της αναγκαιότητας και της αναλογικότητας**: Εδώ περιγράφεται η νομική βάση κατά την οποία γίνεται επιτρεπτή η επεξεργασία δεδομένων αλλά και ποιον σκοπό θα επιτυγχάνει. Επιπρόσθετα περιγράφονται τα μέτρα τα οποία θα βοηθήσουν και θα διασφαλίσουν ότι επιτυγχάνεται μόνον ο σκοπός της επεξεργασίας για τον οποίο συλλέγονται τα δεδομένα αλλά και ότι η ποιότητα των δεδομένων αλλά και οι αρχές που ορίζονται στον ΓΚΠΔ τηρούνται.
5. **Προσδιορισμός και αξιολόγηση κινδύνων:** Εδώ καταγράφονται οι επικείμενοι κίνδυνοι που μπορεί να προκύψουν από την επεξεργασία αυτών των δεδομένων και αξιολογούνται ανάλογα με την σοβαρότητα και την πιθανότητα υλοποίησης τους .
6. **Προσδιορισμός μέτρων για τη μείωση του κινδύνου:** Σε αυτό το σημείο καταγράφονται τα μέτρα τα οποία ο οργανισμός θα πρεπει να λάβει για να μειώσει ή και ένα εξαλείψει τα ρίσκα. Επίσης γίνεται αναφορά αν τα μέτρα αυτά είναι αποδεκτά και επαρκή και αναλόγως εγκρίνονται και απορρίπτονται.
7. **Έγκριση και καταγραφή των αποτελεσμάτων :** Στο τελικό στάδιο της διαδικασίας καταγράφονται τα άτομα τα οποία έχουν πάρει μέρος στην διεκπεραίωση της ΕΑΠΔ και περιλαμβάνεται μια περίληψη των συμβουλών του ΥΠΔ, των μέτρων για την μείωση των κίνδυνων αλλά και από ποιον εγκριθήκαν τα υπολειπόμενα ρίσκα.

Το ακόλουθο γράφημα απεικονίζει τη γενική επαναλαμβανόμενη διαδικασία που πρέπει να ακολουθείται για τη διενέργεια ΕΑΠΔ:

Εικόνα 15 Διαδικασία DPIA Πηγή : https://www.lboro.ac.uk/data-privacy/resources/dpia/dpia-process/

Η Αρχή Προστασίας Δεδομένων της Γαλλίας (CNIL), προσφέρει την δική της μεθοδολογία αλλά και ένα εργαλείο λογισμικού που έχει σκοπό να καθοδηγήσει τους υπεύθυνους επεξεργασίας στην ορθή εκτέλεση μιας εκτίμησης αντικτύπου διευκολύνοντας τη χρήση της μεθόδου ΕΑΠΔ που αναπτύχθηκε από την CNIL. Η μεθοδολογία απαρτίζεται από 4 μέρη όπως περιγράφεται στο Privacy Impact Assessment Methodology (PIA) [21] όπως βλέπουμε και πιο κάτω:

1. Πρεπει να ορίσουμε και να περιγράψουμε το πλαίσιο της επεξεργασίας των υπό εξέταση προσωπικών δεδομένων.
2. Να αναλύσουμε τους ελέγχους που εγγυώνται τη συμμόρφωση με τις θεμελιώδεις αρχές, της αναλογικότητας και αναγκαιότητας της επεξεργασίας, αλλά και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.
3. Την αξιολόγηση των κινδύνων που σχετίζονται με την προστασία της ιδιωτικής ζωής για να διασφαλίσουμε ότι αντιμετωπίζονται επαρκώς.
4. Να επισημοποιηθεί και να καταγραφή η επικύρωση της ΕΑΠΔ και αν χρειαστεί να εκτελεστούν ξανά τα πιο πάνω βήματα.

Υπάρχουν και διεθνείς μεθοδολογίες ΕΑΠΔ, όπως η μεθοδολογία της Επιτροπής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Σιγκαπούρης (PDPC) που προσφέρει ένα αναλυτικότατο οδηγό (GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS) για την διεκπεραίωση μιας Εκτίμησης Αντίκτυπου (ΕΑ) αλλά και οργανισμοί όπως η Microsoft και η IAPP που προσεφέρουν τις δίκες τους μεθοδολογίες.

Στην παρούσα διατριβή, όπως θα παρουσιαστεί στη συνέχεια, θα αξιοποιηθεί η μεθοδολογία της CNIL. Η επιλογή της μεθοδολογίας τη CNIL βασίζεται στο γεγονός ότι είναι μια ευρωπαϊκή ανεξάρτητη εποπτική αρχή για την προστασία δεδομένων που προσφέρει τα κατάλληλα εργαλεία και την σωστή καθοδήγηση για την πραγμάτωση μιας επιτυχημένης ΕΑ που καλύπτει όλα όσα προνοεί ο ΓΚΠΔ.

5.5 Μεθοδολογία Διαχείρισης Κινδύνων Ασφάλειας

Από άποψη ασφάλειας της πληροφορικής και των πληροφοριακών συστημάτων , τα δεδομένα πρέπει να προστατεύονται από εξωτερικές και εσωτερικές επιθέσεις, αλλά και ανεπιθύμητα περιστατικά (όπως τεχνικές βλάβες). Αυτή η οπτική ισχύει εν μέρει και για την προστασία προσωπικών δεδομένων, ακόμη και αν η διατύπωση «προστασία των δεδομένων από επιθέσεις μπορεί να οδηγήσει λανθασμένα ότι υπονοεί «μόνο την ασφάλεια» τους, από πράξεις που μπορεί να διεκπεραιωθούν ακούσια ή εκ προθέσεως, δεν σταματά στον πατροπαράδοτο όρο της ασφάλειας.

Η προστασία προσωπικών δεδομένων εξετάζει την προστασία από επιθέσεις και ανεπιθύμητα συμβάντα, δηλαδή την ασφάλεια , αλλά αυτή η πτυχή καλύπτει μόνο μία από τις έξι αρχές προστασίας δεδομένων που περιγράφονται στο άρθρο 5 (1) του ΓΚΠΔ [22, pp. 35-36]. Με άλλα λόγια, η ασφάλεια πληροφορικής αποτελεί προϋπόθεση για την ασφαλή επεξεργασία των προσωπικών δεδομένων , αλλά δεν διασφαλίζει από μόνη της την πλήρη συμμόρφωση σύμφωνα με τον ΓΚΠΔ.

Όταν εξετάζουμε πέρα από την ασφάλεια και επικεντρωνόμαστε στην προστασία των δεδομένων, οι κύριοι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων προέρχονται από την επεξεργασία δεδομένων όπως έχει προγραμματιστεί,

δηλαδή ακόμη και με την απουσία ανεπιθύμητων γεγονότων και επιθέσεων. Η προστασία δεδομένων απαιτεί την ελαχιστοποίηση των αρνητικών επιπτώσεων της επεξεργασίας για τα επηρεαζόμενα άτομα.

Επομένως, μια ΕΑΠΔ πρέπει να αποδείξει, ότι όλες οι εργασίες επεξεργασίας είναι όντως απαραίτητες και αναλογικές σε σχέση με τους σκοπούς που διεκπεραιώνονται . Αυτό είναι προφανώς πολύ διαφορετικό από μια αξιολόγηση ασφάλειας. Για παράδειγμα, μια δραστηριότητα επεξεργασίας μπορεί να είναι εξαιρετικά ασφαλής έναντι περιστατικών και επιθέσεων, και ωστόσο να περιλαμβάνει απαράδεκτους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων (π.χ. να επιτρέπει την εξαγωγή συμπερασμάτων για τα άτομα τα οποία δεν θα έπρεπε να είναι δυνατόν να εξαχθούν).

Στον τομέα της ασφάλειας, τα μέτρα μετριασμού είναι ως επί το πλείστον τεχνικά και αποτρέπουν επιθέσεις ή μετριάζουν την επίδραση ανεπιθύμητων συμβάντων στα περιουσιακά στοιχεία του υπεύθυνου επεξεργασίας. Στον τομέα της προστασίας δεδομένων, αντίθετα, τα οργανωτικά μέτρα είναι εξίσου σημαντικά και τα μέτρα ελαχιστοποιούν τις αρνητικές επιπτώσεις στα επηρεαζόμενα άτομα. Παραδείγματα οργανωτικών μέτρων περιλαμβάνουν εκπαιδεύσεις προσωπικού για την προστασία και ορθή επεξεργασία των προσωπικών δεδομένων, συμφωνίες μη αποκάλυψης (non-disclosure-agreements) και ειδικές συμβάσεις για τυχόν επεξεργασία που ανατίθενται σε εξωτερικούς συνεργάτες (Data Processor) .

Στην ασφάλεια, ο κίνδυνος παραβίασης των δικαιωμάτων και των ελευθεριών λίγων μόνο ατόμων μπορεί να μην θεωρείται αρκετά σημαντικός. Στην προστασία δεδομένων, η προσοχή εστιάζεται στα άτομα (υποκείμενα δεδομένων), ανεξάρτητά από το αν επηρεάζονται μόνο λίγα σε αριθμό, ο κίνδυνος προσβολής δικαιωμάτων και ελευθεριών δεν μπορεί σε καμία περίπτωση να είναι αποδεκτός.

Ενώ στην ασφάλεια, τα μέτρα έχουν σχεδιαστεί για την άμυνα έναντι επιθέσεων και συμβάντων, στην προστασία δεδομένων έχουν σκοπό να ελαχιστοποιήσουν τις αρνητικές επιπτώσεις στα υποκείμενα δεδομένων ως προς θεμελιώδη δικαιώματα και ελευθερίες. Αυτό είναι εμφανές για παράδειγμα στον περιορισμό της περιόδου αποθήκευσης. Ομοίως, η ψευδωνυμοποίηση αποτρέπει την εύκολη αναγνώριση των

υποκειμένων των δεδομένων και έτσι μειώνει τον κίνδυνο που μπορεί να αντιμετωπίσουν τα υποκείμενα δεδομένων . Άλλα μέτρα στοχεύουν στη διαφάνεια της επεξεργασίας, έτσι ώστε το υποκείμενο των δεδομένων να μην υπόκεινται αβοήθητα στις αποφάσεις των υπευθύνων επεξεργασίας, αλλά να έχουν τη δυνατότητα να προστατεύουν τα δικαιώματά τους σε περίπτωση υπερβολικής ή αθέμιτης παραβίασης των δικαιωμάτων και των ελευθεριών τους και να γνωρίζουν επακριβώς ποια δεδομένα τους υφίστανται επεξεργασία, για ποιο σκοπό και από ποιον/ποιους. Τα υποκείμενα δεδομένων έχουν δικαιώματα τα οποία μπορούν να ασκήσουν σύμφωνα με τον ΓΚΠΔ. Αυτά τα παραδείγματα μέτρων προστασίας δεδομένων δείχνουν τον πολύ διαφορετικό χαρακτήρα σε σύγκριση με τα μέτρα ασφάλειας.

5.6 Επιλογή Μεθοδολογία Διαχείρισης Κινδύνων Ασφάλειας

Κατά την διάρκεια της διατριβής αξιολογήθηκαν δυο μεθοδολογίες διαχείρισης κινδύνου ως προς την ασφάλεια της επεξεργασίας: η OCATVE-Allegro αλλά και η μεθοδολογία που ανέπτυξε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) για την προστασία των προσωπικών δεδομένων.

Ο σκοπός της μεθοδολογίας του ENISA είναι να βοηθήσει τις μικρομεσαίες επιχειρήσεις να εναρμονιστούν με τον ΓΚΠΔ και θα μπορούσε να χρησιμοποιηθεί σε κάποιο βαθμό στην παρούσα διατριβή, η μεθοδολογία OCTAVE- Allegro όμως αναλύει σε μεγαλύτερο βαθμό και λεπτομέρεια τα θέματα ασφάλειας για μεγάλους οργανισμούς όπως είναι τα αεροδρόμια και για αυτό εφαρμόζεται στο Παράρτημα Α της παρούσας διατριβής.

Ο σκοπός χρήσης της μεθοδολογίας OCTAVE- Allegro που παρουσιάζεται αναλυτικά πιο κάτω είναι να υποστηρίξει την διεξαγωγή μιας ολοκληρωμένης ΕΑΠΔ. Η OCTAVE είναι μια μεθοδολογία για τον εντοπισμό και την αξιολόγηση των κινδύνων για την ασφάλεια και την προστασία των πληροφοριών που συμφώνα με τους Richard A. Caralli et al. [23] έχει σκοπό να βοηθήσει τους οργανισμούς:

- Να προσδιορίσουν τα περιουσιακά στοιχεία που είναι σημαντικά για την αποστολή τους.

- Να εντοπίσει τρωτά σημεία και απειλές για αυτά τα περιουσιακά στοιχεία.
- Να προσδιορίσει και να αξιολογήσει τις πιθανές συνέπειες για τον οργανισμό εάν πραγματοποιηθούν οι απειλές.

Το Software Engineering Institute (SEI) ανέπτυξε τη μέθοδο OCTAVE για να αντιμετωπίσει τις προκλήσεις συμμόρφωσης της ασφάλειας πληροφορικής που αντιμετώπιζε το Υπουργείο Άμυνας των ΗΠΑ (DoD) για την αντιμετώπιση των διατάξεων του Health Insurance Portability and Accountability Act (HIPAA) για το απόρρητο και την ασφάλεια της προσωπικής υγείας.

Υπάρχουν τρείς διακριτές μεθοδολογίες OCTAVE που είναι διαθέσιμες για δημόσια χρήση: η μέθοδος OCTAVE, OCTAVE-S και OCTAVE Allegro. Στην παρούσα διατριβή θα χρησιμοποιήσουμε την προσέγγιση OCTAVE Allegro.

Αυτή η προσέγγιση διαφέρει από προηγούμενες προσεγγίσεις της OCTAVE εστιάζοντας στον τρόπο που χρησιμοποιούνται, αποθηκεύονται, μεταφέρονται και επεξεργάζονται τα Information Assets αλλά και πώς εκτίθενται σε απειλές και ευπάθειες ως αποτέλεσμα του πιο πάνω «κύκλου ζωής» της πληροφορίας. Επίσης, η OCTAVE Allegro μπορεί να χρησιμοποιηθεί από άτομα που θέλουν να διεκπεραιώσουν μια αξιολόγηση κινδύνου χωρίς την εκτεταμένη συμμετοχή, από τον υπόλοιπο οργανισμό.

Η προσέγγιση OCTAVE Allegro όπως περιγράφεται στην αναφορά Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [23] αποτελείται από οκτώ βήματα που είναι οργανωμένα σε τέσσερις φάσεις:

- Στην πρώτη φάση «Establish Drivers», στοχεύει στην αιτιολόγηση και την ιεράρχηση των κριτηρίων μέτρησης του κινδύνου για έναν συγκεκριμένο οργανισμό.
- Στην δεύτερη φάση «Profile Assets», καθορίζονται τα κρίσιμα Information Assets και καταγράφονται οι απαιτήσεις ασφαλείας αλλά και γενικότερα ο «κύκλος ζωής» των δεδομένων όπως αναλύθηκε πιο πάνω.
- Στην τρίτη φάση «Identify Threats», καθορίζονται οι απειλές ανάλογα με τον «κύκλο ζωής» των δεδομένων.

- Στην τέταρτη «Identify and Mitigate Risk», και τελευταία φάση εντοπίζονται και αναλύονται τα ρίσκα που αντιμετωπίζουν τα Information Assets και καταρτίζονται σχέδια μετριασμού αυτών των ρίσκων.

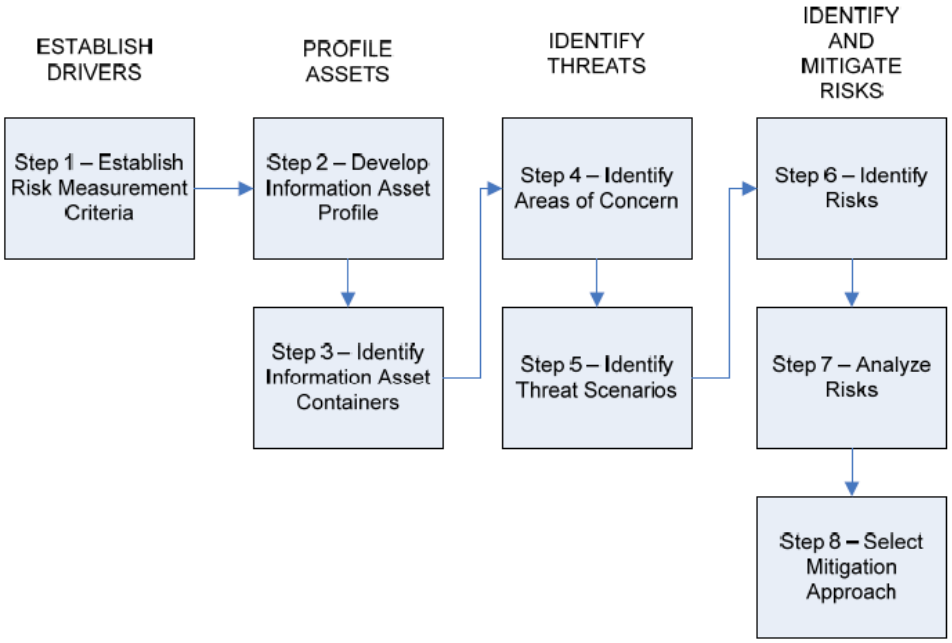


Figure 2: OCTAVE Allegro Roadmap

Εικόνα 16 Διαδικασία Octave Allegro [23]

Πιο κάτω γίνεται μια σύντομη ανάλυση των βημάτων που υπάρχουν στις 4 φάσεις που αναφέραμε πιο πάνω.

Βήμα 1. Η μεθοδολογία απαιτεί ένα ελάχιστο σύνολο περιοχών που καταγράφονται πιο κάτω, ακολούθως γίνεται μια πιο λεπτομερείς ανάλυση των επιπτώσεων στην κάθε περιοχή και αντιστοιχίζεται με ένα σετ κριτήριων (high,medium, low) όπως φαίνεται στο παράδειγμα του πίνακα 8 (Allegro Worksheet 1) για να αξιολογηθεί η σοβαρότητα των επιπτώσεων .

Σύνολο Περιοχών :

- Reputation and passenger confidence.
- Financial
- Productivity
- Safety and Health
- Fines and Legal Penalties

Allegro Worksheet 1	**RISK MEASUREMENT CRITERIA – REPUTATION AND PASSENGER CONFIDENCE**		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover from an adverse event	Reputation is damaged, and some effort and expense is required to recover from an adverse event	Reputation is irrevocably destroyed or damaged.

Πίνακας 7 Κριτήρια μέτρησης του κινδύνου

Στο ίδιο βήμα γίνεται μια βαθμονόμηση των περιοχών ανάλογα με την σοβαρότητα των επιπτώσεων. Η περιοχή με τις σημαντικότερες επιπτώσεις βαθμολογείται με τον αριθμό 5 και μετέπειτα όπως φαίνεται και στο παράδειγμα (Allegro Worksheet 7) του πίνακα 9 βαθμολογούνται οι υπόλοιπες περιοχές ανάλογα με την σοβαρότητα των επιπτώσεων.

Allegro Worksheet 7	**IMPACT AREA PRIORITIZATION WORKSHEET**
PRIORITY	**IMPACT AREAS**
1	**Reputation and Customer Confidence**
3	**Financial**
2	**Productivity**

5	**Safety and Health**
4	**Fines and Legal Penalties**

Πίνακας 8 Ιεράρχηση επιπτώσεων ως προς τη βαρύτητά τους

Βήμα 2: Στο δεύτερο βήμα καταρτίζεται ένα προφίλ του Information Asset. Στον πίνακα 10 καταγράφονται οι λόγοι (Εμπειρικά) που θεωρείται ένα Information Asset σημαντικό για τον οργανισμό. Η Διαφορά σε σχέση με άλλες μεθοδολογίες διαχείρισης κινδύνων είναι ότι τα assets αυτά φέρουν πληροφορία. Τυχόν υποστηρικτικές υποδομές, αν και αποτελούν περιουσιακά στοιχεία, δεν καταγράφονται εδώ (καλύπτονται σε μεταγενέστερο στάδιο)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
1. Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Μηνύματα IATA	Ο σκοπός επεξεργασίας τους είναι για να μπορεί Ο διαχειριστής των αεροδρομίων να είναι σε θέση να προσεφέρει στους επιβάτες τις κατάλληλές υπηρεσίες που χρειάζονται μέσα στον χώρο του αεροδρομίου ώστε να ταξιδέψουν με ασφάλεια. Η επεξεργασία των πιο πάνω μηνυμάτων που εμπίπτουν και στις ειδικές κατηγορίες δεδομένων πρεπει να γίνονται σε συμμόρφωση με τον ΓΚΠΔ	**Οι πληροφορίες αυτές που εμπεριέχουν ευαίσθητα προσωπικά δεδομένα τροφοδοτούνται σε μορφή μηνυμάτων Passenger Service Message (PSM), Passenger Assistance List(PAL), Change Assistance List (CAL) σε διαφορά πληροφοριακά συστήματα.**
(4) Owner(s)		

Who owns this information asset?		
Διαχειριστής/Φορέας - Αεροδρομίων		
(5) Security Requirements *What are the security requirements for this information asset?*		
✓ **Confidentiality**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, δεδομένου ότι μπορεί να περιέχουν πολύ ευαίσθητα προσωπικά δεδομένα.	**Στις Πληροφορίες πρεπει να έχει πρόσβαση το ενδεδειγμένο προσωπικό του αεροδρομίου και εξωτερικοί συνεργάτες που καθορίζονται μέσω σύμβασης**
✓ **Integrity**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει αυτές τις πληροφορίες. Η τήρηση ακριβών αρχείων των δεδομένων είναι σημαντική για την σωστή εξυπηρέτηση των επιβατών με κινητικά προβλήματα ή επιβατών με αναπηρία	**Μόνο εξουσιοδοτημένο προσωπικό του αεροδρομίου και των συνεργατών του, που καθορίζονται μέσω σύμβασης, αλλά και των αεροπορικών εταιρειών πρεπει να μπορούν τροποποιήσουν τις πληροφορίες**
✓ **Availability**	Οι πληροφορίες πρεπει να είναι διαθέσιμες στον φορέα για να μπορεί να διεκπεραιώνει τις εργασίες του.	**Η διαθεσιμότητα των συστημάτων είναι υψίστης σημασίας τόσο για την παροχή υπηρεσιών αλλά και για λογούς ασφάλειας**
	Οι πληροφορίες πρέπει να είναι διαθέσιμες για 24 ώρες, 7 ημέρες/εβδομάδα, 52 εβδομάδες/έτος	**Τα αεροδρόμια είναι ανοικτά και λειτουργούν επί 24ωρου βάσεως.**

✓ **Other**	Υπάρχουν ειδικές απαιτήσεις προστασίας και νομικής συμμόρφωσης	**Επειδή τα πιο πάνω μηνύματα εμπεριέχουν ευαίσθητα προσωπικά δεδομένα υπόκεινται στον ΓΚΠΔ.**

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
✓ Confidentiality	✓ Integrity	✓ Availability	✓ Other

Πίνακας 9 Προφίλ Information Asset

Βήμα 3: Στο τρίτο βήμα γίνεται μια χαρτογράφηση του «κύκλου ζωής» των Information Assets, επικεντρωνόμαστε στον τρόπο που χρησιμοποιούνται, αποθηκεύονται, μεταφέρονται και επεξεργάζονται αυτές οι πληροφορίες. Η χαρτογράφηση αυτή γίνεται σε τρία διαφορετικά επίπεδα:

- Σε φυσικό επίπεδο
- Σε τεχνικό επίπεδο
- Σε επίπεδο ανθρώπων που έχουν γνώση για αυτά τα αγαθά

Στον πίνακα 10 πιο κάτω παρουσιάζεται ένα παράδειγμα για την συμπλήρωση του Allegro Worksheet 9a.

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. SITA Designated address: Τα μηνύματα PAL./ CAL μπορεί αποστέλνονται σε μια αποκλειστική διεύθυνση SITA του αεροδρόμιου	Τμήμα Πληροφορικής Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων

2. **Email address Τα μηνύματα PAL./ CAL μπορεί αποστέλνονται σε μια ηλεκτρονική διεύθυνση (email)**	Τμήμα Πληροφορικής Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων
3. **Airport Operational Database (AODB): Υπάρχουν AODB εφαρμογές οι οποίες μπορεί να λαμβάνουν μηνύματα PAL/CAL, με αυτόν τον τρόπο ο διαχειριστής του αεροδρομίου μπορεί να έχει μια σφαιρική εικόνα για τους αναμενομένους PRM επιβάτες και πως να τους εξυπηρέτηση.**	Τμήμα Πληροφορικής Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων
4. **Baggage Reconciliation System (BRS): Κατά την διάρκεια του Check-in τα συστήματα αυτά λαμβάνουν πληροφορίες όπως όνομα του επιβάτη, αριθμό και ημερομηνία πτήσης, την θέση του επιβάτη των αριθμό αποσκευών του επιβάτη, αριθμός ακολουθίας επιβατών (SQNR).**	Τμήμα Πληροφορικής Αεροδρομίων
5. **Common Use Passenger Processing Systems (CUPPS): Είναι εύκολο να αντιληφθούμε ότι αυτή η κοινή πλατφόρμα μπορεί για σκοπούς υποστήριξης να συλλεγεί διαφορά στοιχεία σε μορφή αρχείων (logs). Τα αρχεία αυτά εμπεριέχουν τα προσωπικά στοιχεία επιβατών όπως για παράδειγμα όνομα, επίθετο, αριθμό πτήσης, την αερογραμμή αλλά και αριθμούς πιστωτικών καρτών.**	Τμήμα Πληροφορικής Αεροδρομίων
6. **Message Broker ένας message broker μπορεί να στέλνει μηνύματα PAL/CAL, BSM αλλά και άλλους τύπους μνημάτων σε διαφορά αεροδρομιακά συστήματα.**	Τμήμα Πληροφορικής Αεροδρομίων
7. **Network and Systems Infrastructure: Τα μηνύματα μεταφέρονται στα διαφορά συστήματα μέσο τη υποδομής του δικτύου και των συστημάτων του αεροδρομίου**	Τμήμα Πληροφορικής Αεροδρομίων
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. **Departure Control Systems (DCS)/ Passenger Processing Systems (PSS) / συστήματα κρατήσεων**	Αερογραμμές

αεροπορικών εταιρειών (CRS): Είναι τα πρωτογενή συστήματα που δημιουργούνται και διανέμονται η πληροφορίες.	
2. Internet: Τα μηνύματα IATA λαμβάνονται μέσω του διαδικτύου στις ενδεδειγμένες ηλεκτρονικές διευθύνσεις	Άγνωστος

Πίνακας 10 Εντοπισμός Θέσης Πληροφοριακού Αγαθού

Βήμα 4: Στο τέταρτο βήμα γίνεται ο προσδιορισμός των περιοχών ανησυχίας (Area of Concern) όπως περιγράφεται στο Allegro Worksheet 10 όπως φαίνεται στον πίνακα 13 από το σημείο 1 μέχρι 6.

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	**Threat**	Information Asset	Μηνύματα IATA	
		Area of Concern	Η διαθεσιμότητα των μηνυμάτων IATA είναι υψίστης σημασίας τόσο για την παροχή υπηρεσιών αλλά και για λογούς ασφάλειας. Μια επίθεση τύπου Denial of Service θα μπορούσε να σταματήσει την λήψη αυτών των μηνυμάτων.	
		(1) Actor *Who would exploit the area of concern or threat?*	Κυβερνοεγκληματίες, Hacktivists.	
		(2) Means *How would the actor do it? What would they do?*	Μια επίθεση άρνησης υπηρεσίας (DDos) είναι μια κακόβουλη προσπάθεια να διακοπεί η κίνηση του δικτύου προς ένα server, προς μια υπηρεσία ή ένα άλλο δίκτυο συντρίβοντας τον στόχο ή την υποδομή του με μια διαδικτυακή κίνηση (Internet Traffic) που ονομάζεται πλημμύρα (flood) .	
		(3) Motive *What is the actor's reason for doing it?*	Οι κυβερνοεγκληματίες έχουν οικονομικά κίνητρα και ποικίλλουν σε επίπεδο δεξιοτήτων και πόρων. Hacktivists: Άτομα ή ομάδες που παρακινούνται από έναν πολιτικό, κοινωνικό ή θρησκευτικό σκοπό	
		(4) Outcome	**Disclosure** **Destruction** **Modification** ✓ **Interruption**	

		What would be the resulting effect on the information asset?			
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Οι επιθέσεις DDoS είναι αποτελεσματικές χρησιμοποιώντας πολλαπλά παραβιασμένα συστήματα υπολογιστών ως πηγές επιθέσεων, που μπορεί να περιλαμβάνουν υπολογιστές και άλλους δικτυωμένους πόρους, όπως συσκευές IoT.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	**Low**

Πίνακας 11 Προσδιορισμός Περιοχών Ανησυχίας

Βήμα 5 Στο πέμπτο βήμα γίνεται ο προσδιορισμός των Σεναρίων Απειλών (Identify Threat Scenarios). Η μεθοδολογία παραθέτει μια σειρά από σενάρια απειλών με ενσωματωμένα ερωτηματολόγια για να μας βοηθήσει να αναγνωρίσουμε περισσότερες απειλές στο τεχνικό, φυσικό αλλά και στο επίπεδο των ανθρώπων που έχουν γνώση για αυτά τα αγαθά δίνοντας μας έτσι την δυνατότητα να ενημερώσουμε τον προσδιορισμό περιοχών ανησυχίας . Στον πίνακα 12 βλέπουμε 2 πιθανά σενάρια.

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
<u>Scenario 1:</u> Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**

Modified so that it is not usable for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes.	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
<u>Scenario 2:</u> Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**

Πίνακας 12 Risk Scenarios

Βήμα 6 : Στο βήμα «Αναγνώριση κινδύνων» καταγράφονται οι συνέπειες αν υλοποιηθεί μια από τις απειλές που καταγράψαμε. Η καταγραφή γίνεται στο πεδίο 7 του Allegro Worksheet 10

Βήμα 7: Στην ανάλυση κινδύνων (Analyze Risks) στο Allegro – Worksheet 10 πραγματοποιούμε μια ποιοτική αποτίμηση των συνεπειών (impact value) στις περιοχές επιπτώσεων που καταγράψαμε στο Βήμα 1, προσδίδοντας τις τιμές 1, 2 και 3 αντιστοίχως στο Low, Moderate και High. Ο υπολογισμός του συνολικού αποτελέσματος γίνεται με τον πολλαπλασιασμό της αξίας της περιοχής επιπτώσεων που δώσαμε στο φύλλο εργασίας 7 μαζί με την αξία των συνεπειών (Impact value).

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Διακοπή υπηρεσιών αεροδρομίου	Reputation & Customer	Low (1)	1
	Financial	Low (1)	3
	Productivity	Medium (2)	4
	Safety & Health	High (3)	15
	Fines & Legal Penalties	High (3)	12
	User Defined Impact Area	N/A	
		Relative Risk Score	**35**

Βήμα 8 : Ανάλογα με τα αποτελέσματα του βήματος 7 μπορούμε να κατηγοριοποιήσουμε τους κινδύνους σε 4 κατηγορίες (POOL) όπως φαίνεται και στην εικόνα πιο κάτω :

RELATIVE RISK MATRIX			
PROBABILITY	RISK SCORE		
	30 TO 45	16 TO 29	0 TO 15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

Εικόνα 17 Κατηγοριοποίηση κινδύνων

Ο οργανισμός ακολούθως θα πρεπει να αντιστοιχίσει την κάθε κατηγορία σπουδαιότητας κινδύνων με μια στρατηγική διαχείρισης του ρίσκου που μπορεί να είναι μια από τις ακόλουθες :

1. Αποδοχής (Accept)
2. Αναβολής (Defer)
3. Μετριασμού (Mitigate)
4. Μεταφοράς (Transfer)

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Εικόνα 18 Αντιστοίχιση κατηγοριών σπουδαιότητας κινδύνου με στρατηγική διαχείρισης του ρίσκου

Ανάλογα με το συνολικό αποτέλεσμα , τότε ακολουθούμε την κατάλληλη στρατηγική διαχείρισης του ρίσκου, στον πίνακα 15 παρουσιάζεται σαν παράδειγμα ο μετριασμός του κινδύνου από επιθέσεις τύπου DDoS.

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Network and Systems Infrastructure.	**Αγορά υπηρεσιών προστασίας δικτύου από έναν Internet Service Provider (ISP).** Οι επιθέσεις DDoS στα δίκτυα των εταιρειών και στην υποδομή IT αυξάνονται σε μέγεθος, συχνότητα και πολυπλοκότητα. Απλές λύσεις όπως, firewalls και Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS) δεν είναι πλέον επαρκείς για να σταματήσουν τέτοιου είδους επιθέσεις. Επίσης, οι απλές διαδικτυακές λύσεις ασφάλειας δεν μπορούν να σταματήσουν μια έξυπνη επίθεση DDoS αφού δεν μπορούν να χειριστούν επιθέσεις που υπερβαίνουν την ικανότητα σύνδεσής τους και οι χάκερ χρησιμοποιούν αυτές τις επιθέσεις για να υπονομεύσουν την άμυνα του δικτύου και στη συνέχεια να διεισδύσουν στο δίκτυο της εταιρείας.		

Πίνακας 13 Μετριασμός Ρίσκου

Κεφάλαιο 6
Μελέτη Περίπτωσης: Εκτίμηση αντίκτυπου προστασίας δεδομένων σε «έξυπνο» αεροδρόμιο

Σε αυτό το στάδιο της διατριβής θα προχωρήσουμε στην διεκπεραίωση μιας Εκτίμησης Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ) στο περιβάλλον ενός έξυπνου αεροδρομίου όπως έχει καθοριστεί στα πιο πάνω κεφάλαια. Η ΕΑΠΔ θα επικεντρωθεί στην επεξεργασία μηνυμάτων ΙΑΤΑ που εμπεριέχουν «ειδικές κατηγορίες προσωπικών δεδομένων»

Για την υλοποίηση της ΕΑΠΔ θα χρησιμοποιήσουμε δυο εργαλεία που αντικατοπτρίζουν το θεωρητικό υπόβαθρο που αναλύσαμε πιο πάνω και πληρούν όλες τις προϋποθέσεις που έχουν καθοριστεί από τον ΓΚΠΔ για την εκπλήρωση μιας ολοκληρωμένης ΕΑΠΔ.

Τα εργαλεία που πρόκειται να χρησιμοποιήσουμε είναι :

1. Η μεθοδολογία εκτίμησης κινδύνου ασφάλειας δεδομένων OCTAVE Allegro. Τα αποτελέσματά της θα «τροφοδοτήσουν» κατάλληλα το αντίστοιχο τμήμα της ΕΑΠΔ αναφορικά με την ασφάλεια της επεξεργασίας.
2. Το λογισμικό ανοιχτού κώδικα PIA (Διεκπεραίωση της ΕΑΠΔ) από την Αρχή Προστασίας Δεδομένων της Γαλλίας (Commission Nationale Informatique & Libertés)

6.1 Εφαρμογή Εκτίμησης Κινδύνου Προσωπικών Δεδομένων (ΕΚΠΔ)

Ο σκοπός της εκτίμησης κινδύνου που διεξάγεται στο παράρτημα Α της παρούσας διατριβής είναι για να ενισχύσει και να υποστηρίξει την διεκπεραίωση μιας εκτίμησης ΕΑΠΔ που υλοποιείται στο σημείο 6.2 της παρούσας διατριβής και σε καμία περίπτωση δεν πρεπει να εκλαμβάνεται σαν μια ολοκληρωτική λύση για την προστασία δεδομένων, αφού όπως αναλύσαμε στο σημείο 5.5 η ασφάλεια των δεδομένων και των πληροφοριακών συστημάτων γενικότερα, δεν φέρει την πλήρη συμμόρφωση με τον ΓΚΠΔ .

Τα αποτελέσματα της εκτίμησης κινδύνου καταδεικνύουν ότι μια σειρά από τεχνικά και οργανωτικά μέτρα πρεπει να εφαρμοστούν ώστε να μετριαστούν τα ρίσκα που μπορεί να επηρεάσουν τα δικαιώματα και τις ελευθερίες των επιβατών στο σύνολο τους αλλά και ειδικότερα των επιβατών ΑμεΑ.

Οι κίνδυνοι για την καταστροφή, τροποποίηση, διαρροή αλλά και την διακοπή χρήσης αυτών των δεδομένων κρίνεται σημαντική στον μέγιστο βαθμό όπως φαίνεται και στις εικόνες 19 και 20. Επίσης προτείνονται μέτρα μετριασμού των κινδύνων που θα πρεπει να παρθούν από του φορείς των αεροδρομίων.

RELATIVE RISK MATRIX			
PROBABILITY	RISK SCORE		
	30 TO 45	16 TO 29	0 TO 15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

Εικόνα 19 Αποτέλεσμα Κατηγοριοποίησης κινδύνων

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Εικόνα 20 Αποτέλεσμα αντιστοίχισης κατηγοριών σπουδαιότητας κινδύνου με στρατηγική διαχείρισης του ρίσκου

Τα αποτελέσματα, λαμβάνονται υπόψη στην εκτίμηση Αντίκτυπου Προσωπικών Δεδομένων (ΕΑΠΔ) με υποστηρικτικό σκοπό.

6.2 Εφαρμογή Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ)

Για την εφαρμογή μια ΕΑΠΔ θα χρησιμοποιήσουμε το λογισμικό ανοιχτού κώδικα PIA που παρέχεται από την Αρχή Προστασίας Δεδομένων της Γαλλίας (Commission Nationale Informatique & Libertés [24]). Το εργαλείο προσφέρει την δυνατότητα διεκπεραίωσης μιας ολοκληρωμένης ΕΑΠΔ σύμφωνα με την ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων και το ελάχιστο περιεχόμενο το οποίο καθορίζεται από τον ΓΚΠΔ.

Η επιλογή του εργαλείου έγινε με βάση στο ότι προσδίδει στον χρήστη την δυνατότητα να διεκπεραίωση την μεθοδολογία της ΕΑΠΔ της CNIL βήμα προς βήμα. Επίσης διαθέτει μια αξιόλογη γνωσιακή βάση για κάθε βήμα που χρειάζεται για την πραγμάτωση της ΕΑΠΔ έτσι ώστε να βοηθήσει τον χρήστη να συμπληρώσει σωστά τις πληροφορίες που χρειάζονται για τις πιο κάτω κατηγορίες :

- Το Γενικό Πλαίσιο
- Της Θεμελιώδης Αρχές
- Τους Κινδύνους
- Την Επικύρωση της ΕΑΠΔ.

Επιπρόσθετα, είναι ένα εργαλείο που παρέχεται δωρεάν από την CNIL με σκοπό να βοηθήσει τους οργανισμούς να βελτιώσουν την συμμόρφωση τους με τον ΓΚΠΔ.

6.3 Γενικό Πλαίσιο

Στο γενικό πλαίσιο θα αναλύσουμε ποια είναι η υπό εξέταση επεξεργασία , τις ευθύνες του υπεύθυνου επεξεργασίας, το αν υπάρχουν πρότυπα για τον τρόπο επεξεργασίας, τα δεδομένα και τον κύκλο ζωής των δεδομένων αλλά και τα στοιχεία που υποστηρίζουν αυτά τα δεδομένα. Αυτό γίνεται εφικτό μέσα από μια σειρά ερωτώ-απαντήσεων που παρατίθενται πιο κάτω.

Εικόνα 21 Στιγμιότυπο από την Διαδικασία Γενικού Πλαισίου

Γενικό Πλαίσιο – ΕΠΙΣΚΟΠΗΣΗ : Αυτό το τμήμα μας επιτρέπει να προσδιορίσουμε και να παρουσιάσουμε το αντικείμενο της μελέτης.

Ποια είναι η υπό εξέταση επεξεργασία;

Η υπό εξέταση επεξεργασία είναι η λήψη και περαιτέρω διαχείριση των μηνυμάτων ΙΑΤΑ που εμπεριέχουν προσωπικά δεδομένα και με βάση τον ΓΚΠΔ εμπεριέχουν δεδομένα που ανήκουν σε ειδικές κατηγορίες.

Τα μηνύματα Passenger Assistance List (PAL), Change Assistance List (CAL) και Passenger Service Message (PSM) πρεπει να παραλαμβάνονται και να επεξεργάζονται από τον εκτελούντα την επεξεργασία (Διαχειριστής Αεροδρόμιου) για να παρέχονται οι κατάλληλες υπηρεσίες στους επιβάτες με αναπηρία και τα άτομα με μειωμένη κινητικότητα.

Ο σκοπός επεξεργασίας τους είναι αναγκαίος ούτος ώστε ο διαχειριστής των αεροδρομίων να είναι σε θέση να προσφέρει στους επιβάτες τις κατάλληλές υπηρεσίες που χρειάζονται μέσα στον χώρο του αεροδρομίου ώστε να ταξιδέψουν με ασφάλεια.

Τα Baggage Source Message (BSM) είναι μηνύματα τα οποία καθιστούν δυνατή την αντιστοίχιση ενός επιβάτη με τις αποσκευές του. Λαμβάνονται από τον διαχειριστή των αεροδρόμιων για μπορέσει να εξυπηρετήσει το επιβατικό κοινό.

Η επεξεργασία των πιο πάνω μηνυμάτων που εμπίπτουν και στις ειδικές κατηγορίες δεδομένων πρεπει να γίνονται σε συμμόρφωση με τον ΓΚΠΔ

Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;

Αεροπορικές εταιρείες και αεροπορικοί πράκτορες μέσω του συστήματος κρατήσεων τους (CRS), συστήματα διαχείρισης επιβατών (PSS) η ένα σύστημα ελέγχου αναχωρήσεων (DCS) παράγουν τα μηνύματα PAL/CAL/PSM/BSM τα οποία παραδίδονται μέσω μιας ενδεδειγμένης διεύθυνσης SITA email στον διαχειριστή των αεροδρομίων.

Οι φορείς εκμετάλλευσης αεροδρομίων θεωρούνται υπεύθυνοι για την :

1. Παραλαβή και αποθήκευση των μηνυμάτων
2. Την προώθηση των μηνυμάτων στους κατάλληλους φορείς προς επεξεργασία (εκτελών την επεξεργασία)
3. Η ανάλυση των δεδομένων μπορεί να γίνεται από την ίδια την διαχειρίστρια εταιρεία ή και από τρίτο.

Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;

Τα πρότυπα που ισχύουν για την επεξεργασία των μηνυμάτων είναι :

1. Type B
2. Recommended Practice 1715 της IATA PSM
3. Recommended Practice 1708a της IATA PAL/CAL
4. Recommended Practice 1745 της IATA BSM

Γενικό Πλαίσιο – ΔΕΔΟΜΈΝΑ, ΔΙΑΔΙΚΑΣΊΕΣ ΚΑΙ ΥΠΟΣΤΗΡΙΚΤΙΚΆ ΣΤΟΙΧΕΊΑ : Αυτό το τμήμα μας επιτρέπει να ορίσουμε και να περιγράψουμε λεπτομερώς το αντικείμενο της επεξεργασίας**.**

Ποιά προσωπικά δεδομένα υφίστανται επεξεργασία;

Τα προσωπικά δεδομένα του επιβάτη που υφίστανται επεξεργασία είναι τα εξής:

1. Όνομα
2. Επίθετο
3. Είδος Αναπηρίας (SSR CODE)
4. Αριθμός πτήσης
5. Όνομα Αεροπορικής εταιρείας
6. Σχόλια που μπορεί να αφορούν τις ανάγκες του επιβάτη

Πρόσβαση στα δεδομένα έχουν οι υπάλληλοι των αεροδρομίων αλλά και ένα σύνολο εξουσιοδοτημένων ατόμων.

Τα δεδομένα αποθηκεύονται και επεξεργάζονται από διάφορες εφαρμογές όπως :

1. PAL/CAL /PSM– AODB (IoT Devices)
2. BSM- BRS (IoT Devices)
3. PAL/CAL/PSM/BSM- Message Broker
4. Any other integrated system.

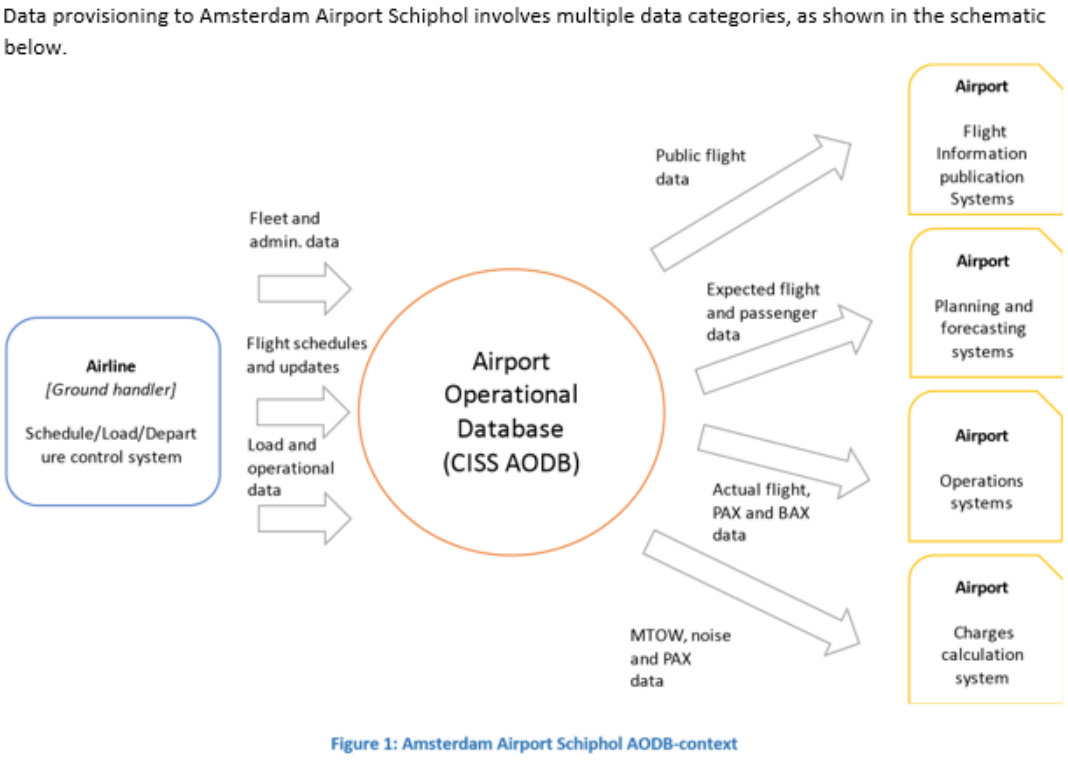
Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;

1. Το έγγραφο συνιστώμενης πρακτικής προτείνει την εισαγωγή μιας λίστας βοήθειας επιβατών (Passenger Assistance List (PAL)) και μιας αλλαγής λίστας βοήθειας (Change Assistance List(CAL)). Το PAL είναι μια λίστα με PRM που αφορούν ένα συγκεκριμένο σημείο πτήσης και επιβίβασης. Το μήνυμα παράγεται από το σύστημα κρατήσεων μιας αεροπορικής εταιρείας για την ειδική βοήθεια στη διαχείριση των επιβατών. Ένα PAL αποστέλλεται για κάθε αεροδρόμιο αναχώρησης στη διαδρομή μιας πτήσης, εάν η πτήση αναχωρεί από ή φθάνει σε αεροδρόμιο της ΕΕ. Μια λίστα PAL αποστέλλεται πάντα, ακόμη και όταν δεν υπάρχουν PRM στην πτήση . Σε τέτοιες περιπτώσεις, χρησιμοποιείται μια τιμή NIL. Οι λίστες PAL/CAL αποστέλλονται μέσω telext μηνυμάτων όπως καθορίζεται από κάθε αεροδρόμιο της ΕΕ.

   Η CAL είναι μια ενημερωμένη λίστα με τυχόν αλλαγές που έχουν συμβεί στο σύστημα κρατήσεων από την αποστολή του PAL μιας πτήσης ή μιας προηγούμενης CAL.

   Τόσο τα PAL όσο και τα CAL μπορούν να σταλούν μόνο σε μια διεύθυνση SITA η ένα email. Επομένως, τα αεροδρόμια της Ευρώπης πρέπει να δημιουργήσουν μια ενιαία διεύθυνση SITA ή email για να λαμβάνουν αυτά τα μηνύματα και να τα κοινοποιούν στις αεροπορικές τους εταιρείες.
2. Το PSM δημιουργείται από το σύστημα ελέγχου αναχώρησης (DCS) μιας αεροπορικής εταιρείας και μεταφέρεται στον επόμενο σταθμό (αεροδρόμιο) οπού μπορεί να περάσει ένας επιβάτης που χρειάζεται κάποιου είδους βοήθεια ανάλογα με το SSR Code.
3. Ένα BSM αποστέλνεται από το σύστημα ελέγχου αναχώρησης (DCS) η από τα Check-In στο BRS του αεροδρομίου. Ένα BSM στέλνεται για τον κάθε επιβάτη ή για γκρουπ επιβατών.

4. Ακολούθως τα μηνύματα μπορούν να εισαχθούν σε ένα οποιαδήποτε σύστημα ή εφαρμογή μέσω ενός Message Broker που να μπορεί να διεκπεραιώνει την επεξεργασία αυτών των δεδομένων για στατιστικούς λογούς αλλά και παρακολούθησης ποιότητας των εργασιών. Τα πιο πάνω μηνύματα είναι Type B και δεν υπάρχει ενδεδειγμένος χρόνος αποθήκευσης και διαγραφής αυτό εναπόκειται στην κρίση του υπεύθυνου επεξεργασίας . Στην εικόνα 22 Βλέπουμε ένα σχηματικό διάγραμμα της ροής πληροφοριών από το αεροδρόμιο Schiphol του Άμστερνταμ



Εικόνα 22 : Data specifications for operational data at Amsterdam Airport Schiphol Πηγή: https://www.schiphol.nl/en/download/b2b/1540980672/3GiELSi9kIMyUUYCK0yc66.pdf

Ποια είναι τα στοιχεία που υποστηρίζουν τα δεδομένα;

Τα συστήματα που υποστηρίζουν τα δεδομένα είναι τα ακόλουθα :

1. SITA Designated address
2. Email
3. Airport Operational Database (AODB)

4. Baggage Reconciliation System (BRS)
5. Common Use Passenger Processing Systems (CUPPS)
6. Departure Control Systems (DCS)
7. Passenger Processing Systems (PSS)
8. Message Broker
9. IoT Devices
10. Workstations
11. Internet
12. PRM Management Application

6.4 Θεμελιώδεις αρχές

Σύμφωνα με το εργαλείο αυτή η ενότητα μας επιτρέπει να δημιουργήσουμε το πλαίσιο συμμόρφωσης για τις αρχές απορρήτου.

Θεμελιώδεις αρχές – Αναλογικότητα και Αναγκαιότητα : Αυτό το τμήμα μας επιτρέπει να αποδείξουμε ότι εφαρμόζουμε τα απαραίτητα μέσα που θα επιτρέψουν στα ενδιαφερόμενα άτομα να ασκήσουν τα δικαιώματά τους.

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;
Σύμφωνα με τον Ευρωπαϊκό Κανονισμό (ΕΚ) αριθ. 1107/2006 τα άτομα με αναπηρία και τα άτομα με μειωμένη κινητικότητα θα πρέπει να γίνονται δεκτά στις αερομεταφορές, η δε αναπηρία ή η αδυναμία τους αυτή δεν θα πρέπει να αποτελεί λόγο άρνησης της μεταφοράς τους, εξαιρουμένων των δικαιολογημένων λόγων ασφαλείας που ορίζει ο νόμος

PAL/CAL/PSM: Η διαχειρίστρια εταιρεία των αεροδρόμιων πρεπει να επεξεργάζεται τα δεδομένα των επιβατών με αναπηρία ή με μειωμένη κινητικότητα για να τους παρέχει τις κατάλληλες υπηρεσίες. Η επεξεργασία αυτή μπορεί να ανατεθεί σε έναν data processor για την καλύτερη και πιο επαγγελματική παροχή υπηρεσιών.

BSM: Η διαχειρίστρια εταιρεία των αεροδρομίων παρέχει το σύστημα αντιστοίχισης αποσκευών (BRS) σε κάθε αεροπορική εταιρεία οπού με την σειρά της μπορεί να μεταφέρει αυτήν την ευθύνη σε κάποιο handling agent.

Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Η Νομική βάση εναπόκειται στα ακόλουθα :

Άρθρο 6 (γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας.

Τα PAL/CAL/PSM: Σύμφωνα με τον Ευρωπαϊκό Κανονισμό (ΕΚ) αριθ. 1107/2006 τα άτομα με αναπηρία και τα άτομα με μειωμένη κινητικότητα θα πρέπει, να γίνονται δεκτά στις αερομεταφορές, η δε αναπηρία ή η αδυναμία τους αυτή δεν θα πρέπει να αποτελεί λόγο άρνησης της μεταφοράς τους, εξαιρουμένων των δικαιολογημένων λόγων ασφαλείας που ορίζει ο νόμος .

Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»);

Τα προσωπικά δεδομένα που συλλέγονται ανάλογα και με τα Recommended Practices της IATA είναι τα απολύτως απαραίτητα για να διεκπεραιωθούν οι κατάλληλες εργασίες. Οποιοδήποτε και από τα δεδομένα αν εκλείψει, κάποια τουλάχιστον εκ των απαιτούμενων εργασιών δεν θα μπορεί να επιτελεστεί.
Η δομή και η πληροφορία που εμπεριέχεται στα μηνύματα πρεπει να είναι συγκεκριμένη ώστε η μεταφορά και η επεξεργασία της πληροφορίας αυτής να είναι επιτυχής.

Τα δεδομένα είναι ακριβή και ενημερωμένα;

Τα δεδομένα ενημερώνονται από τρίτα συστήματα αεροπορικών εταιρειών όπως Departure Control Systems (DCS), Passenger Service Systems PSS., Customer Service Systems (CRS).
Τα πρωτογενή δεδομένα στο αεροδρόμιο, φτάνουν από τις αεροπορικές εταιρείες. Η μόνη περίπτωση είναι αυτόνομων υποθέσεων επιβατών, που καταφτάνουν στο αεροδρόμιο χωρίς να έχουν δώσει κάποια προειδοποίηση μέσω των αεροπορικών εταιριών για την χρήση υπηρεσιών PRM.

Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Οι διαχειριστές των αεροδρομίων διατηρούν τα προσωπικά δεδομένα μόνο για όσο χρονικό διάστημα είναι εύλογα απαραίτητο για την εκπλήρωση των σκοπών για τους οποίους τα συλλέχτηκαν , συμπεριλαμβανομένων των σκοπών της ικανοποίησης τυχόν νομικών, κανονιστικών, φορολογικών, λογιστικών ή αναφορικών απαιτήσεων. Ενδέχεται να διατηρήσουν τα προσωπικά δεδομένα για μεγαλύτερο χρονικό διάστημα σε περίπτωση καταγγελίας ή εάν εύλογα πιστεύουν ότι υπάρχει πιθανότητα δικαστικής προσφυγής σε σχέση με τη σχέση τους μαζί με τους επιβάτες .

Για να καθοριστεί η κατάλληλη περίοδος διατήρησης για τα προσωπικά δεδομένα, λαμβάνεται υπόψη η ποσότητα, η φύση και η ευαισθησία των προσωπικών δεδομένων, ο πιθανός κίνδυνος βλάβης από μη εξουσιοδοτημένη χρήση ή αποκάλυψη των προσωπικών δεδομένων, τους σκοπούς για τους οποίους επεξεργάζονται τα προσωπικά δεδομένα και αν μπορεί να επιτύχουν τους σκοπούς τους με άλλα μέσα ώστε να μπορούν να διεκπεραιώσουν τις ισχύουσες νομικές, κανονιστικές, φορολογικές, λογιστικές ή άλλες απαιτήσεις.

Ψηφιακά αντίγραφα των προσωπικών δεδομένων θα αποθηκεύονται και σε ορισμένες περιπτώσεις, θα ανωνυμοποιούνται (ώστε να μην μπορούν πλέον να συσχετιστούν με τους επιβάτες) για ερευνητικούς ή στατιστικούς σκοπούς, οπότε ενδέχεται η χρήση αυτών των πληροφορίων επ' αόριστον χωρίς περαιτέρω ειδοποίηση.

ΚΙΝΔΥΝΟΣ: Το μέτρο προστασίας ανωνυμοποίησης προσωπικών δεδομένων, με στόχο την προστασία των προσωπικών πληροφοριών, πρεπει να ισχύει σε όλες τις περιπτώσεις και όχι σε ορισμένες όταν χρησιμοποιούνται για ερευνητικούς ή στατιστικούς σκοπούς.

Μέτρο αντιμετώπισης: Να υλοποιείται ένα αυστηρό εποπτικό πλαίσιο από τον φορέα του αεροδρομίου με σκοπό να διαβεβαιώνει ότι τηρούνται οι κατάλληλες διαδικασίες για την προστασία των προσωπικών δεδομένων, ιδίως δε σε περιπτώσεις ανωνυμοποίησης δεδομένων.

Θεμελιώδεις αρχές – Μέτρα για την Προστασία των Προσωπικών Δικαιωμάτων των Υποκειμένων των Δεδομένων:

Αυτό το τμήμα μας επιτρέπει να αποδείξουμε ότι εφαρμόζονται τα απαραίτητα μέσα που θα επιτρέψουν στα ενδιαφερόμενα άτομα να ασκήσουν τα δικαιώματά τους.

Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;

Τα υποκείμενα δεδομένων ενημερώνονται για την επεξεργασία των προσωπικών τους δεδομένων μέσω από μια σειρά ειδοποιήσεων απορρήτου (Privacy Notice) που αναρτιούνται και ανανεώνονται στην ιστοσελίδα του διαχειριστή του αεροδρομίου.

ΚΙΝΔΥΝΟΣ : Άτομα τα οποία ταξιδεύουν και δεν έχουν ευχέρεια με το Διαδίκτυο (π.χ. ηλικιωμένοι), δεν ενημερώνονται ευχερώς για την επεξεργασία**.**

Μέτρο αντιμετώπισης: Οι φορείς αεροδρομίων θα πρεπει να ενημερώνουν το επιβατικό κοινό, το οποίο δεν έχει τα ηλεκτρονικά μέσα για να συνδέεται στο διαδίκτυο σχετικά με τα δικαιώματα τους σύμφωνα με τον ΓΚΠΔ και τον τρόπο με τον οποίο θα μπορούσαν να ασκήσουν αυτά τα δικαιώματα.

Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;

Δεν ισχύει, αφού δεν είναι η συγκατάθεση η νομική βάση της επεξεργασίας.

Τα επόμενα τρία ερωτήματα μπορούν να απαντηθούν με τον ίδιο τρόπο :

- **Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους πρόσβασης και φορητότητας προσωπικών δεδομένων;**
- **Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους διόρθωσης και διαγραφής;**
- **Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους περιορισμού και εναντίωσης;**

Στην ειδοποίηση απορρήτου γίνονται γνωστά τα στοιχεία επικοινωνίας του υπεύθυνου προσωπικών δεδομένων του οργανισμού (ΥΠΔ) για να μπορέσουν να εξασκήσουν όλα τα νόμιμα δικαιώματα τους , τα στοιχεία αυτά μπορεί να είναι:

1. Όνομα και επίθετο ΥΠΔ
2. Ηλεκτρονική διεύθυνση επικοινωνίας
3. Τηλέφωνο
4. Φόρμα επικοινωνίας μέσο της ιστοσελίδας

Κίνδυνος: Άτομα τα οποία ταξιδεύουν και δεν έχουν ευχέρεια με το Διαδίκτυο (π.χ. ηλικιωμένοι), δεν ενημερώνονται ευχερώς για τα δικαιώματά τους και πώς μπορούν να τα ασκήσουν.
ΕΥΡΗΜΑ : Τα στοιχεία αυτά πρεπει να είναι διαθέσιμα και στα γραφεία πληροφοριών του αεροδρομίου η να αναρτώνται σε διάφορους χώρους του αεροδρομίου ως προς ενημέρωση του επιβατικού κοινού.

Οι υποχρεώσεις των εκτελούντων την επεξεργασία προσδιορίζονται σαφώς και διέπονται από σύμβαση;
Η διαχειριστές αεροδρόμιων έχουν δικαίωμα ανάθεσης της επεξεργασίας αυτών των δεδομένων εάν και εφοσον το επιθυμούν , σύμφωνα με όσα προβλέπει το άρθρο 28 του ΓΚΠΔ για τις υποχρεώσεις των εκτελούντων την επεξεργασία.

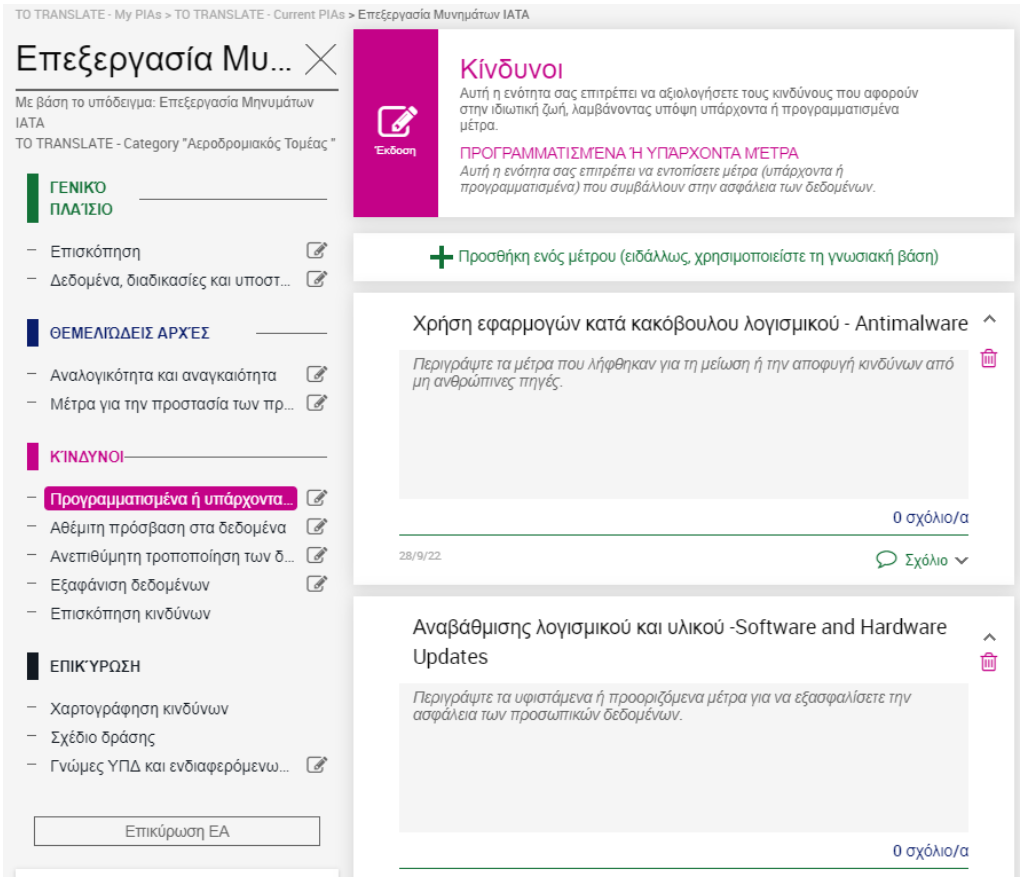
Σε περίπτωση μεταφοράς δεδομένων εκτός της Ευρωπαϊκής Ένωσης, τα προσωπικά δεδομένα προστατεύονται επαρκώς.
Τα δεδομένα δεν μεταφέρονται έκτος συνόρων του κράτους μέλους που υφίστανται επεξεργασία. Πρεπει να τονίσουμε και να διευκρινίσουμε ότι οι φορείς αεροδρομίων επεξεργάζονται και διαχειρίζονται τα δεδομένα σε τοπικό επίπεδο, είναι ευθύνη των αεροπορικών εταιριών η προώθηση των προσωπικών δεδομένων των επιβατών στους επομένους τους σταθμούς.

6.5 Κίνδυνοι ασφάλειας

Αυτή η ενότητα μας επιτρέπει να αξιολογήσουμε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα. Η κατηγορία αύτη αποτελείται από 5 υποκατηγορίες που χαρτογραφούνται τα προγραμματισμένα μετρά σε αντιστοίχιση με τους κίνδυνους ως προς την εμπιστευτικότητα , ακεραιότητα και διαθεσιμότητα των δεδομένων.

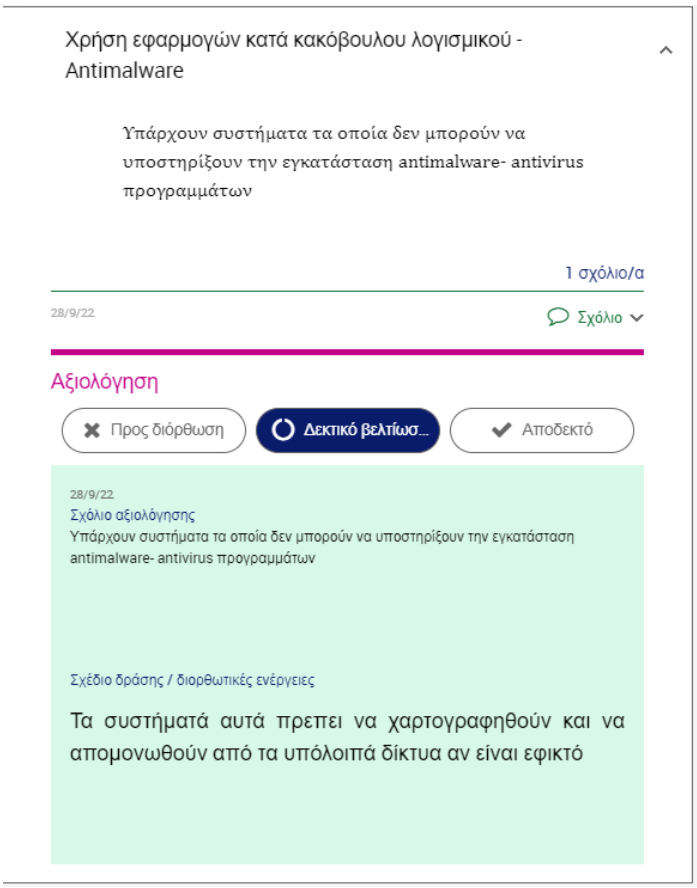
ΚΙΝΔΥΝΟΙ- Προγραμματισμένα η Υπάρχοντα Μέτρα : Αυτή η ενότητα μας επιτρέπει να εντοπίσουμε μέτρα (υπάρχοντα ή προγραμματισμένα) που συμβάλλουν στην ασφάλεια των δεδομένων.

Τα υπάρχοντα και προγραμματισμένα μέτρα που εισάχθηκαν στο εργαλείο είναι τα οργανωτικά , τεχνικά , οι πολιτικές και τα πρότυπα που αναφέρονται στο σημείο 3.4 της διατριβής (Διασφάλιση έξυπνων αεροδρομίων -Ελαχιστοποίηση Κίνδυνων).



Εικόνα 23 Εισαγωγή Μέτρων Προστασίας

Είναι σημαντικό να αναφέρουμε ότι τα μέτρα αυτά αξιολογούνται για την επάρκεια τους. Σύμφωνα με την παρούσα διατριβή τα μέτρα αυτά δεν μπορούν να εφαρμοστούν στην ολότητά τους, έτσι πρεπει να ληφθούν διορθωτικά και επιπλέον μέτρα για μετριασμό του κινδύνου όπως φαίνεται και στην εικόνα 24.



Εικόνα 24 Προτεινόμενα Βελτιωτικά Μέτρα

ΚΙΝΔΥΝΟΙ- Αθέμιτη Πρόσβαση στα Δεδομένα : Αναλύουμε τα αίτια και τις συνέπειες της αθέμιτης πρόσβασης στα προσωπικά δεδομένα και εκτιμούμε τη σοβαρότητα και την πιθανότητά της.

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων αν επέρχονταν ο κίνδυνος;

Η παραβίαση απορρήτου θα μπορούσε να επηρεάσει σε κάποιο βαθμό τα άτομα προκαλώντας τους κάποιο στρες η δυσφορία ειδικότερα των επιβατών ΑμεΑ. Η διαρροή

δεδομένων αλλά και η παράνομη εκμετάλλευση τους θα μπορούσε να οδηγήσει σε διακρίσεις και δυσμενή μεταχείριση προς τα υποκείμενα δεδομένων από άλλους οργανισμούς όπως οι τράπεζες και ασφαλιστικές εταιρείες.

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Οι Απειλές που θα μπορούσαν να παραβιάσουν την εμπιστευτικότητα των δεδομένων όπως παρουσιάζονται και στο Παράρτημα Α της υλοποίησης της εκτίμησης κίνδυνου OCATVE- Allegro είναι:

- Αδύναμοι ή επαναχρησιμοποιημένοι κωδικοί πρόσβασης
- Μη ενημερωμένα λογισμικά (Non-Updated Software)
- Επίθεση κακόβουλου Λογισμικού - Malware Attack
- Κακοδιαχείριση συσκευών IoT
- Ανασφαλής μεταφορά και αποθήκευση δεδομένων - Η έλλειψη κρυπτογράφησης
- Μη ασφαλείς υπηρεσίες δικτύου
- Η έλλειψη διαχωρισμού δικτύου
- Εκμετάλλευση από κακόβουλες συσκευές -Counterfeit by Malicious Devices
- Επιθέσεις κατά του - απορρήτου Privacy Attacks (Social Engineering)
- Διαρροή Δεδομένων από δυσαρεστημένους εργαζόμενους (Insider Threat)
- Man in the middle (Insider Threat)

Ποιές είναι οι πηγές κινδύνου:

Οι πήγες κινδύνου είναι :

- Εσωτερικές και εξωτερικές ανθρώπινες πήγες
- Hacktivists
- Κυβερνοεγκληματίες

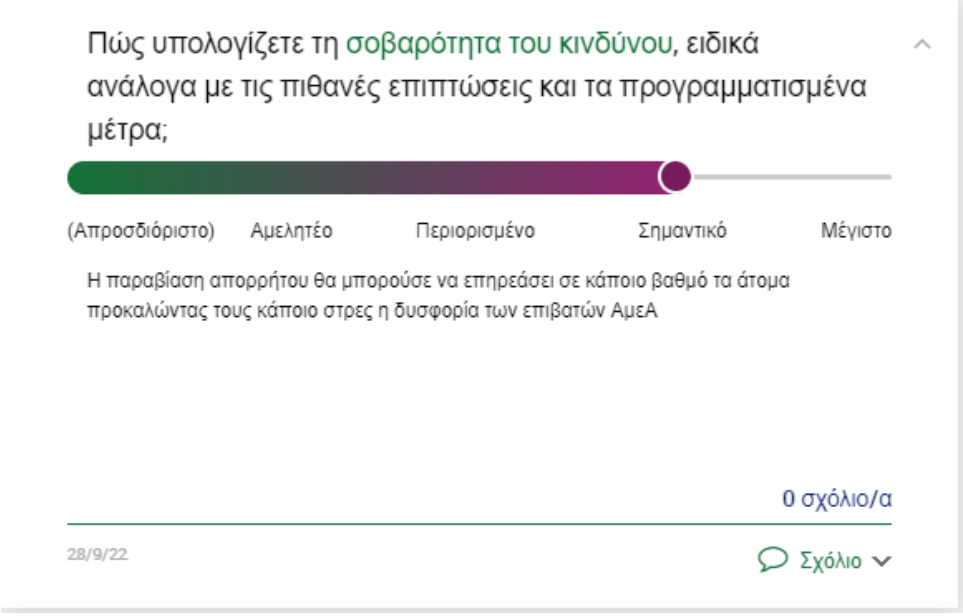
Ποιά από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

- Χρήση εφαρμογών κατά κακόβουλου λογισμικού (Antimalware)
- Αναβάθμισης λογισμικού και υλικού (Software and Hardware Updates)
- Firewalls και Τμηματοποίηση Δικτύου (Firewalls and Network Segmentation)
- Ισχυρές Μέθοδοι Αυθεντικοποίησης (Strong User Authentication)

- Αλλαγή Προκαθορισμένων διαπιστευτηρίων (Change Default Credentials)
- Κρυπτογράφηση Δεδομένων (Data Encryption)
- Ασφάλεια εφαρμογών & Ασφαλής σχεδιασμός (Application security & Secure design)
- Εκπαίδευση Προσωπικού Αεροδρομίου στην αντιμετώπιση περιστατικών σε Επιθέσεις κατά του απορρήτου (Privacy Attacks)

Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Η σοβαρότητα κινδύνου υπολογίζεται σαν σημαντικού βαθμού, όπως φαίνεται και στην εικόνα 25.

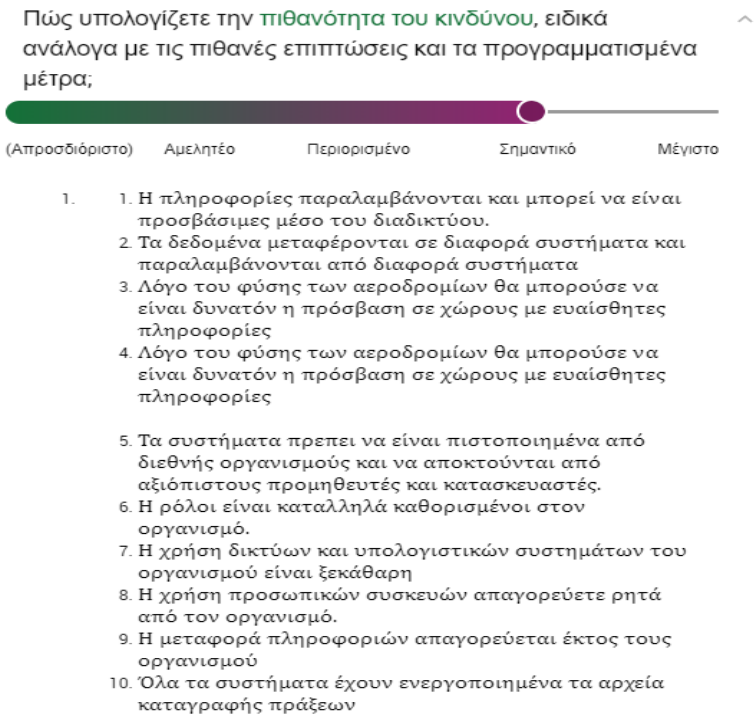


Εικόνα 25 Σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις

Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Σύμφωνα και με την εκτίμηση κινδύνου στο σημείο 6.1 της παρούσας διατριβής η πιθανότητα υλοποίησης κάποιας απειλής υπολογίζεται σαν σημαντικού βαθμού. Όπως απεικονίζεται και στην εικόνα 26 οι πιο κάτω πληροφορίες παρουσιάζονται για να υποστηρίξουν τον υψηλό βαθμό αξιολόγησης :

1. Η πληροφορίες παραλαμβάνονται και μπορεί να είναι προσβάσιμες μέσω του διαδικτύου.
2. Τα δεδομένα μεταφέρονται σε διάφορα συστήματα και παραλαμβάνονται αντίστοιχα από διάφορα συστήματα
3. Λόγω του φύσης των αεροδρομίων θα μπορούσε να είναι δυνατόν η πρόσβαση σε χώρους με ευαίσθητες πληροφορίες
4. Τα συστήματα πρέπει να είναι πιστοποιημένα από διεθνής οργανισμούς και να αποκτούνται από αξιόπιστους προμηθευτές και κατασκευαστές.
5. Οι ρόλοι πρεπει να είναι κατάλληλα καθορισμένοι στον οργανισμό.
6. Η χρήση δικτύων και υπολογιστικών συστημάτων του οργανισμού πρεπει είναι ξεκάθαρη.
7. Η χρήση προσωπικών συσκευών πρεπει να απαγορεύεται ρητά από τον οργανισμό.
8. Η μεταφορά πληροφοριών πρεπει να απαγορεύεται εκτός τους οργανισμού
9. Όλα τα συστήματα πρεπει έχουν ενεργοποιημένα τα αρχεία καταγραφής πράξεων
10. Λόγω της φύσεως των αεροδρομίων υπάρχει συχνή αυξομείωση στο προσωπικό.
11. Εκπαίδευσης προσωπικού σε θέματα ιδιωτικότητας αλλά και ασφάλειας πληροφοριών γίνονται ανά τακτά χρονικά διαστήματα μαζί με διάφορες ασκήσεις για την επαγρύπνηση του προσωπικού
12. Ναι είναι πολύ πιθανόν αρχεία να βρεθούν ανοικτά και προσβάσιμα.
13. Τα αεροδρόμια είναι στόχοι κυβερνοεπιθέσεων όπως είδαμε και από την σχετική βιβλιογραφία και λόγω της ανάπτυξης της τουριστικής βιομηχανίας καθώς επίσης και λόγο του ότι θωρούνται κρίσιμες υποδομές



Εικόνα 26 Υπολογισμός πιθανότητας υλοποίησης Απειλής

ΚΙΝΔΥΝΟΙ- Ανεπιθύμητη Τροποποίηση των Δεδομένων : Αναλύουμε τα αίτια και τις συνέπειες μιας ανεπιθύμητης αλλαγής των δεδομένων και εκτιμούμε τη σοβαρότητα και την πιθανότητά της.

Ποιές θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωση επέλευσης του κινδύνου;

Αν τα δεδομένα των επιβατών ΑμεΑ τροποποιηθούν τότε μπορεί να μην τους παρασχεθούν οι κατάλληλες υπηρεσίες και μπορεί να υπάρξουν επιπτώσεις στην υγεία τους. Κρίνεται όμως σαν υψίστης σημασίας γιατί το BRS είναι ένα σύστημα ασφάλειας που αντιστοιχεί κάθε αποσκευή σε έναν μοναδικό επιβάτη.

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Οι Απειλές που θα μπορούσαν να παραβιάσουν την ακεραιότητα των δεδομένων είναι:

- Αδύναμοι ή επαναχρησιμοποιημένοι κωδικοί πρόσβασης
- Μη ενημερωμένα λογισμικά (Non-Updated Software)
- Επίθεση κακόβουλου Λογισμικού (Malware Attack)

- Κακοδιαχείριση συσκευών IoT
- Ανασφαλής μεταφορά και αποθήκευση δεδομένων. Η έλλειψη κρυπτογράφησης
- Μη ασφαλείς υπηρεσίες δικτύου
- Η έλλειψη διαχωρισμού δικτύου
- Εκμετάλλευση από κακόβουλες συσκευές (Counterfeit by Malicious Devices)
- Επιθέσεις κατά του - απορρήτου Privacy Attacks (Social Engineering)
- Διαρροή Δεδομένων από δυσαρεστημένους εργαζόμενους (Insider Threat)
- Man in the middle

Ποιές είναι οι πηγές κινδύνου;

Οι πήγες κινδύνου είναι :

- Εσωτερικές και εξωτερικές ανθρώπινες πήγες
- Hacktivists
- Κυβερνοεγκληματίες
- Βλάβη συστημάτων (Corruption)

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

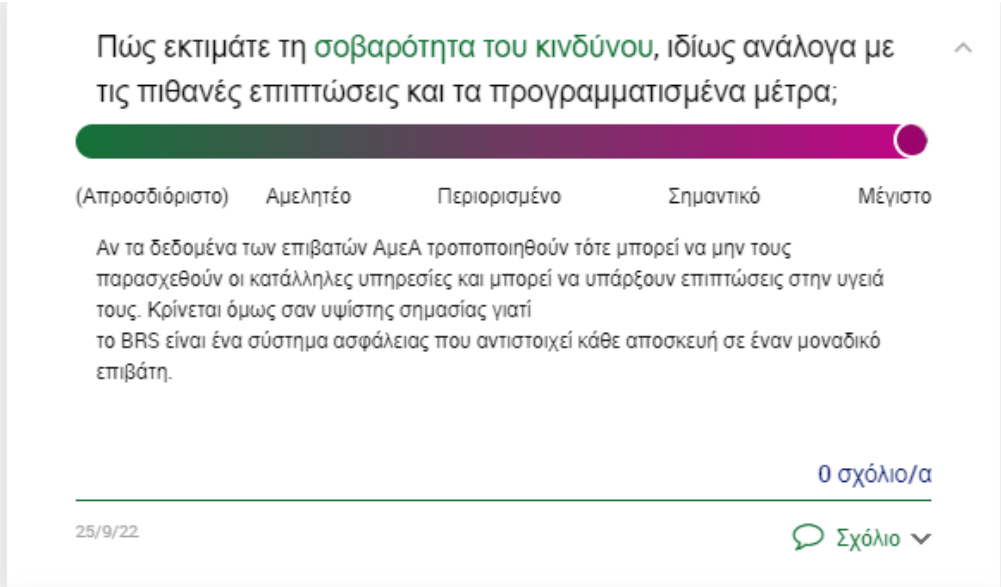
Τα προσδιορισθέντα μετρά αναλύονται στο σημείο 3.4 της παρούσας διατριβής

- Χρήση εφαρμογών κατά κακόβουλου λογισμικού (Antimalware)
- Αναβάθμισης λογισμικού και υλικού (Software and Hardware Updates)
- Firewalls και Τμηματοποίηση Δικτύου (Firewalls and Network Segmentation)
- Ισχυρές Μέθοδοι Αυθεντικοποίησης (Strong User Authentication)
- Αλλαγή Προκαθορισμένων διαπιστευτηρίων (Change Default Credentials)
- Κρυπτογράφηση Δεδομένων (Data Encryption)
- Ασφάλεια εφαρμογών & Ασφαλής σχεδιασμός (Application security & Secure design)
- Διορισμός ενός Υπεύθυνου Ασφάλειας Πληροφορικής (Appoint an IT Security Officer)
- Εφαρμογή πολιτικών για την εγκατάσταση προγραμμάτων (Enforce rules Governing Installation of Software)

- Συνεχής Επίβλεψη της Ασφάλειας Πληροφορικής (Continuous Monitoring of Information Security)
- Εγκαθίδρυση ενός προγράμματος διαχείρισης της ασφάλειας της Πληροφορικής και συμμόρφωση με τα διεθνή πρότυπα και κανονισμούς (ISMS, International standards, and compliance Audits)
- Συμμόρφωση με την Ασφάλεια πληροφορικής από εξωτερικούς συνεργάτες (Information Security Compliance from external providers)
- Διαχείριση πρόσβασης χρηστών (User Access Management)
- Εξειδικευμένη εκπαίδευση στην Ασφάλεια Πληροφοριών (Specialised Information Security training)
- Απαιτήσεις ασφάλειας προσωπικού για τρίτους παρόχους (Personnel security requirements for third party providers)
- Εκπαίδευση Προσωπικού Αεροδρομίου στην αντιμετώπιση περιστατικών για συστήματα πληροφορικής (Train Airport Personnel in incident response for IT systems)
- Διασφάλιση συμφωνίας πρόσβασης σε άτομα πριν από την παραχώρηση πρόσβασης (Ensure access agreement to individuals prior to grant access)
- Δοκιμή και άσκηση ικανότητας απόκρισης περιστατικού σε συστήματα πληροφορικής (Test and exercise incident response capability for IT systems)
- Βασική εκπαίδευση ευαισθητοποίησης για την ασφάλεια σε όλους τους χρήστες πληροφοριακών συστημάτων (Basic Security awareness training to all information system users)
- Έλεγχος ατόμων πριν από την εξουσιοδότηση πρόσβασης στο σύστημα πληροφορικής των αεροδρομίων (Screen individuals prior to authorize access to airports IT system)
- Τήρηση αντιγράφων ασφαλείας (Backup).

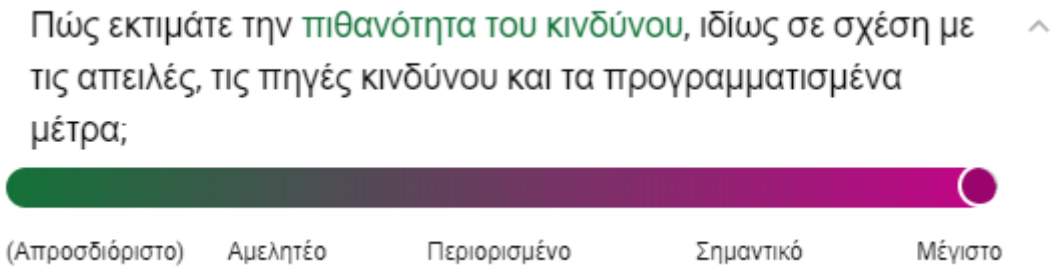
Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Σύμφωνα και με τα πιο πάνω η σοβαρότητα κινδύνου υπολογίζεται σαν Μέγιστου βαθμού.



Εικόνα 27 Προσδιορισμός Επιπτώσεων κινδύνου ως προς την ακεραιότητα των δεδομένων

Σύμφωνα και με την εκτίμηση κινδύνου στο Παράτημα Β οπού αναλύονται οι κίνδυνοι για την καταστροφή, τροποποίηση, διαρροή και τροποποίηση των προσωπικών δεδομένων αλλά όπως αναλύθηκε και πιο πάνω στην παρούσα διατριβή, η πιθανότητα υλοποίησης κάποιας απειλής υπολογίζεται σαν σημαντικού βαθμού. Όπως απεικονίζεται και στην εικόνα 28.



Εικόνα 28 Προσδιορισμός πιθανότητας υλοποίησης κάποιας απειλής κατά την ακεραιότητα των δεδομένων

ΚΙΝΔΥΝΟΙ -Εξαφάνιση Δεδομένων : Αναλύουμε τα αίτια και τις συνέπειες της απώλειας δεδομένων και εκτιμούμε τη σοβαρότητα και την πιθανότητά τους.

Η διαθεσιμότητα των συστημάτων είναι υψίστης σημασίας τόσο για την παροχή υπηρεσιών αλλά και για λογούς ασφάλειας

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Οι Απειλές είναι η ιδίες με τις οποίες καταγράφηκα πιο πάνω με μόνη διαφορά ότι η παροχή υπηρεσιών και τα δεδομένα να μην είναι διαθέσιμα από :

1. Άρνηση υπηρεσίας - DDos Attack (Αναλύεται και στο Παράρτημα Α)
2. Φυσικά αίτια (φωτιά, πλημμύρα , διακοπή ρεύματος)
3. Αστοχία υλικού ή λογισμικού

Ποιές είναι οι πηγές κινδύνου;

Οι πήγες κινδύνου είναι :

- Εσωτερικές και εξωτερικές ανθρώπινες πήγες
- Hacktivists
- Κυβερνοεγκληματίες
- Βλάβη συστημάτων (Corruption)
- Φυσικά αίτια

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

Τα συνολικά μέτρα κατά της πιθανότητας υλοποίησης του κινδύνου είναι τα ίδια με πιο πάνω με επιπρόσθετα μετρά τα :

- Συστήματα πυροσβέσεις ,γεννήτριες συστήματα αποχέτευσης

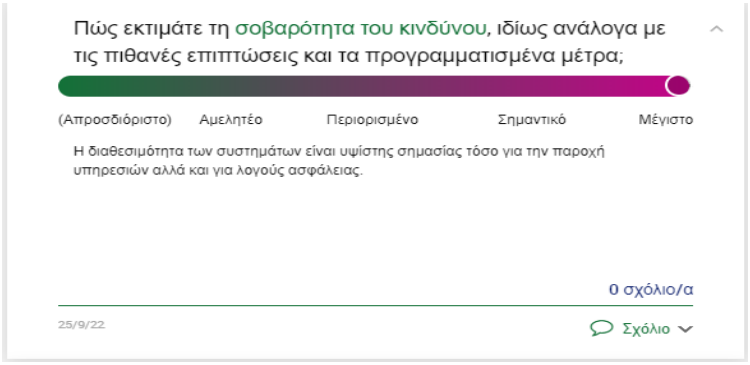
Κίνδυνος: Δεν υπάρχει καταγεγραμμένο σχέδιο διαχείρισης καταστροφών (Disaster Recovery Plan).

ΕΥΡΗΜΑ: Οi φορείς αεροδρομίων θα πρεπει να αναπτύξουν και να υλοποιήσουν σχέδιο αποκατάστασης καταστροφών του (Disaster Recovery Plan), η αποδοτικότητα και αποτελεσματικότητα του οποίου θα πρέπει να δοκιμαστεί.. Συνήθως τα σχέδια

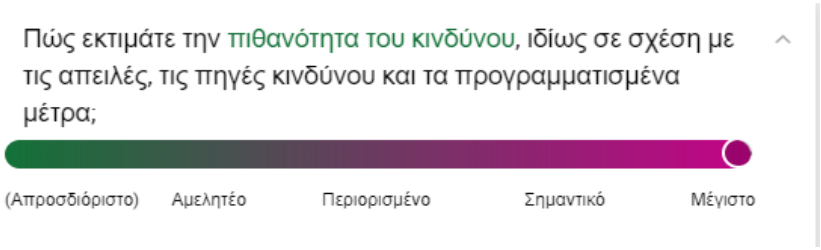
επιχειρησιακής συνέχειας αλλά και αποκατάστασης καταστροφών περιλαμβάνουν βασικές υπηρεσίες των αεροδρομίων.

Στις επόμενες δυο ερωτήσεις που καθορίζεται ο βαθμός επιπτώσεων των κίνδυνων αλλά και η πιθανότητα υλοποίησης της απειλής δίνουμε το μέγιστο βαθμό όπως απεικονίζεται στις εικόνες 29 και 30:

- **Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;**
- **Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;**

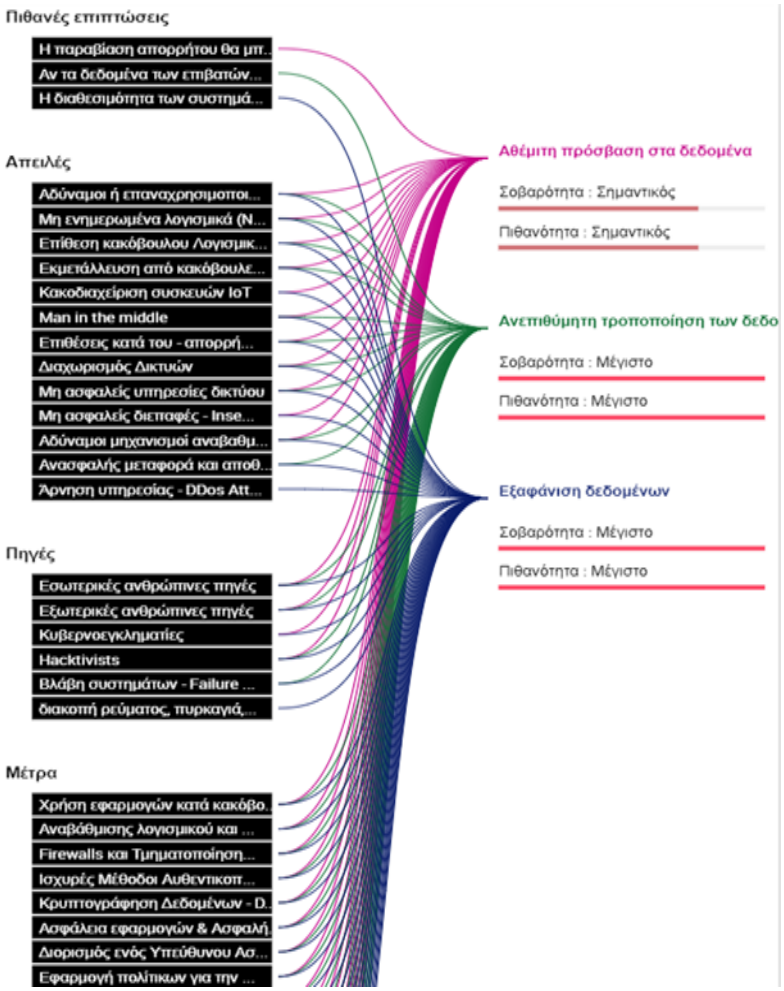


Εικόνα 29 Προσδιορισμός Επιπτώσεων κινδύνου ως προς την ακεραιότητα των δεδομένων



Εικόνα 30 Προσδιορισμός πιθανότητας υλοποίησης κάποιας απειλής κατά την διαθεσιμότητα των δεδομένων

ΚΙΝΔΥΝΟΙ- Επισκόπηση Κινδύνων: Αυτή η απεικόνιση σας παρέχει μια σφαιρική και συνθετική άποψη των επιπτώσεων των μέτρων στους κινδύνους που προέρχονται από την επεξεργασία.



Εικόνα 31 Αντιστοίχιση επιπτώσεων των μέτρων προς στους κινδύνους

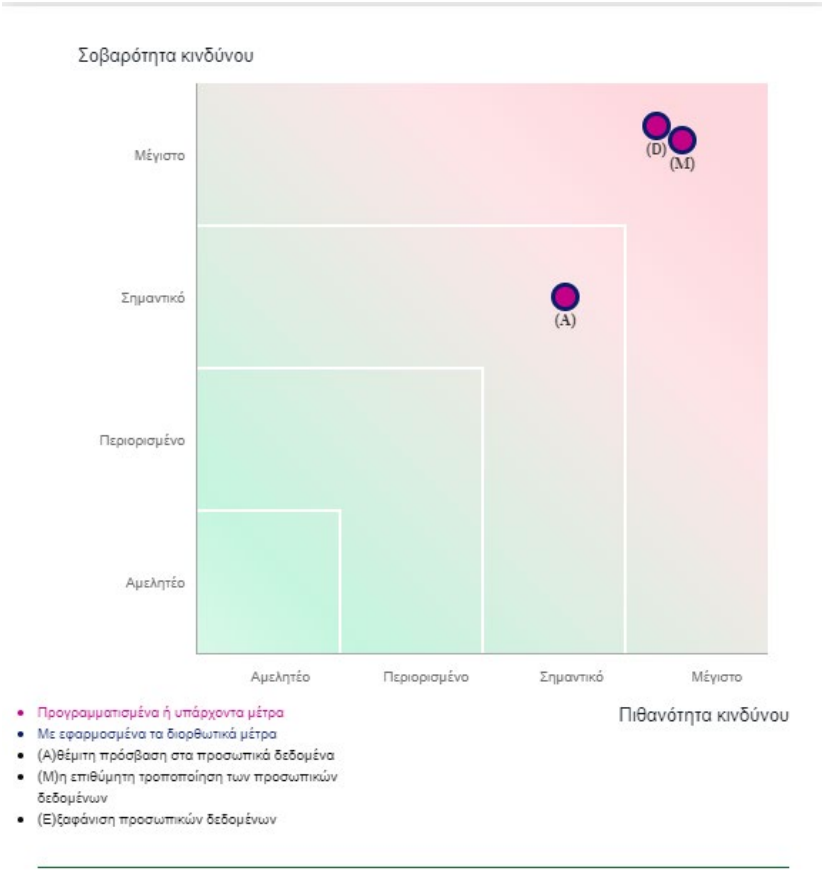
6.6 Επικύρωση

Αυτή η ενότητα μας επιτρέπει να προετοιμάσουμε και να επισημοποιήσουμε την επικύρωση της ΕΑ.

Πριν είναι δυνατόν να επικυρωθεί η εκτίμηση αντικτύπου πρεπει να γίνει η αξιολόγηση των θεμελιώδη αρχών και των μέτρων ασφάλειας που μειώνουν τους κίνδυνους. Στις περιπτώσεις που χρειάζονται περισσότερα μετρά τότε πρεπει να καταρτιστεί ένα σχέδιο δράσης για την εφαρμογή τους.

ΕΠΥΚΥΡΩΣΗ- Χαρτογράφηση κινδύνων : Αυτή η απεικόνιση μας επιτρέπει να έχουμε μια συνολική και συνθετική άποψη των κινδύνων, πριν και μετά την εφαρμογή των συμπληρωματικών μέτρων.

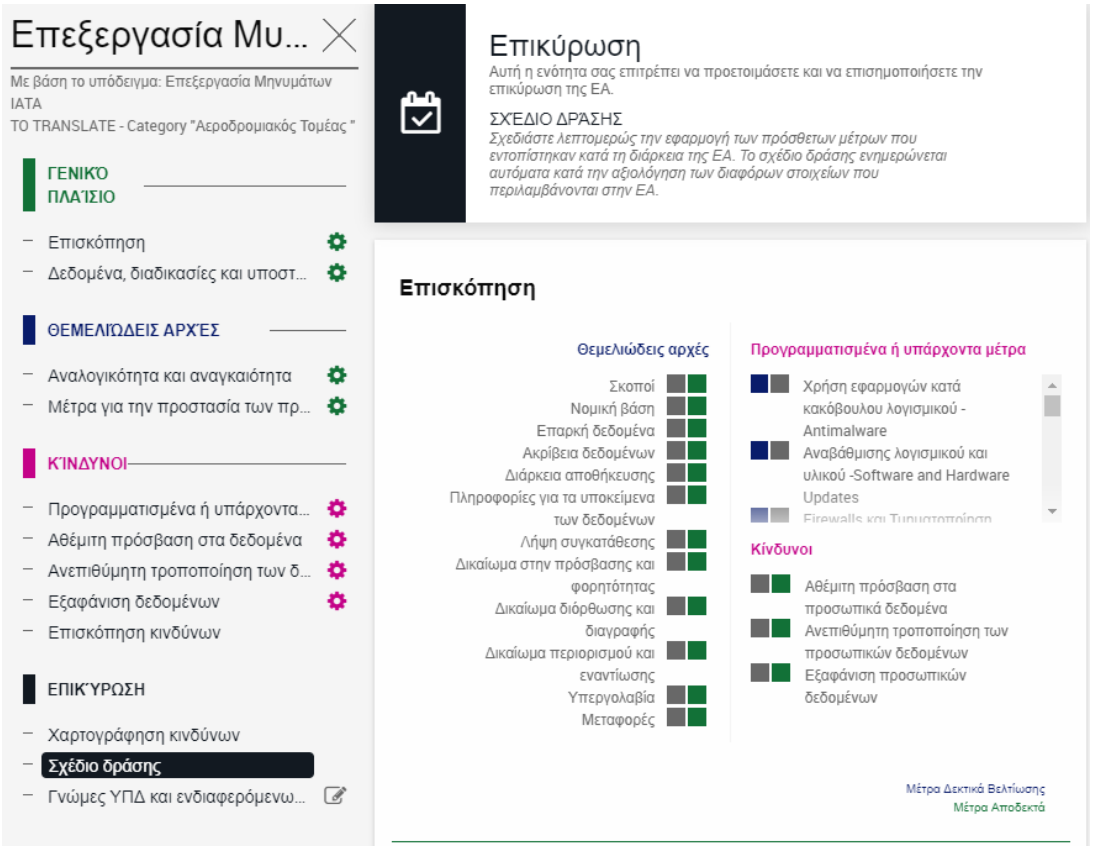
Από το γράφημα της εικόνας 32 πιο κάτω βλέπουμε ότι πιθανότητα και η σοβαρότητα του κινδύνου ως προς την τροποποίηση και καταστροφή των δεδομένων βρίσκεται στο μέγιστο βαθμό κινδύνου ενώ η αθέμιτη πρόσβαση στα δεδομένα ανέρχεται σε ένα σημαντικό βαθμό επικινδυνότητας.



Εικόνα 32 Σοβαρότητα και Πιθανότητα Κινδύνου

ΕΠΥΚΥΡΩΣΗ- Σχέδιο Δράσης

Σε αυτό το στάδιο για να επικυρωθεί η Εκτίμηση Αντίκτυπου (ΕΑ) πρεπει να σχεδιάσουμε λεπτομερώς την εφαρμογή των πρόσθετων μέτρων που εντοπίστηκαν κατά τη διάρκεια της ΕΑ. Το σχέδιο δράσης ενημερώνεται αυτόματα κατά την αξιολόγηση των διαφόρων στοιχείων που περιλαμβάνονται στην ΕΑ.



Εικόνα 33 Γενική Επισκόπηση ΕΑ

Στον πιο κάτω πίνακα παραθέτουμε τα επιπρόσθετα μέτρα ασφάλειας που θεωρούμε ότι πρεπει να πάρει ένα αεροδρόμιο για να διασφαλίσει τα προσωπικά δεδομένα των επιβατών

Υπάρχον Μέτρο	Διάφοροι Περιορισμοί	Σχέδιο Δράσης
Χρήση εφαρμογών κατά κακόβουλου λογισμικού – Antimalware	Υπάρχουν συστήματα τα οποία δεν μπορούν να υποστηρίξουν την εγκατάσταση Antimalware- antivirus προγραμμάτων	Τα συστήματά αυτά πρεπει να χαρτογραφηθούν και να απομονωθούν από τα υπόλοιπά δίκτυα αν είναι εφικτό

Αναβάθμισης λογισμικού και υλικού -Software and Hardware Updates	Υπάρχουν συστήματα παλαιάς τεχνολογίας αλλά μεγάλης χρησιμότητας που δεν μπορούν να αντικατασταθούν και δεν μπορούν να αναβαθμιστούν με τις τελευταίες ενημέρωσης ασφάλειας	Τα συστήματα αυτά πρεπει να χαρτογραφηθούν και να απομονωθούν από τα υπόλοιπά δίκτυα αν είναι εφικτό
Firewalls και Τμηματοποίηση Δικτύου – Firewalls and Network Segmentation	Σε πάρα πολλές περιπτώσεις χρησιμοποιείται λογική (VLANS) τμηματοποίηση των δικτυών λόγο των ειδικών τεχνολογιών. Επίσης δεδομένου ότι πάρα πολλά δίκτυα πρεπει να επικοινωνούν μεταξύ τους η παραμετροποιήσεις και η χρήσης τεχνολογιών trunk είναι συνηθισμένες σε δίκτυα με μεγάλο εύρος	Τα συστήματα αυτά πρεπει να χαρτογραφηθούν και να απομονωθούν από τα υπόλοιπά δίκτυα αν είναι εφικτό
Ισχυρές Μέθοδοι Αυθεντικοποίησης - Strong User Authentication	Αντιλαμβανόμαστε όμως ότι αυτό δεν μπορεί να εφαρμοστεί σε όλα τα συστήματά και ειδικότερα σε συσκευές IoT	Πρεπει να χρησιμοποιούνται τεχνολογίες IoT που να μπορούν να γίνουν integrated με κεντρικοποιημένα συστήματά διαχείρισης κωδίκων προσβάσεις
Κρυπτογράφηση Δεδομένων - Data Encryption	Το θέμα είναι κατεξοχήν ολόκληρης της βιομηχανίας και οφειλή να βρει την λύση	Τα δεδομένα πρεπει να κρυπτογραφούνται η τουλάχιστον να ανωνυμοποιούνται στη βάση δεδομένων που αποθηκεύονται κατά την επεξεργασία τους.
Ασφάλεια εφαρμογών & Ασφαλής σχεδιασμός - Application security & Secure design	Οι συσκευές IoT που χρησιμοποιούνται και στον τομέα Operational Technology OT δεν είναι αρκετά ώριμες για να σχεδιαστούν με βάση την ασφάλεια. Επιπλέων πολλά από τα συστήματά είναι πεπαλαιωμένα.	Οι Εφαρμογές πρεπει να περνούν από διαφόρους ελέγχους όπως Vulnerability Assessments και Penetration Tests.
Εφαρμογή πολιτικών για την εγκατάσταση προγραμμάτων - Enforce rules Governing Installation of Software	Η πολιτικές πρεπει να είναι σεβαστές αλλά πρεπει να υποστηρίζονται από τα καταλληλά τεχνικά μέσα για την εφαρμογή αλλά και την επιβολή τους.	Τεχνικά μέτρα όπως προγράμματα εγκατάστασης εφαρμογών αλλά και group policies μπορούν να εφαρμοστούν για την εφαρμογή των πολίτικων.
Συμμόρφωση με την Ασφάλεια	Οι εξωτερικοί συνεργάτες πρεπει να δεσμεύονται με συμβόλαια για την	Εγκαθίδρυση ελεγκτικού

πληροφορικής από εξωτερικούς συνεργάτες - Information Security Compliance from external sources	συμμόρφωση τους για να ακολουθούν τις πολιτικές ασφάλειας. Ο έλεγχος όμως από εξωτερικούς και εσωτερικούς εκλεκτές για την πιστοποίηση της συμμόρφωσης είναι απαραίτητος	προγράμματος (Internal and External Audits) για την πιστοποίησή συμμόρφωσης
Βασική εκπαίδευση ευαισθητοποίησης για την ασφάλεια σε όλους τους χρήστες πληροφοριακών συστημάτων - Basic Security.	Η εκπαίδευση είναι αναγκαστική.	Οι γνώσεις πρεπει να δοκιμάζονται με ασκήσεις τύπου social engineering (Phishing Attacks)
Disaster Recovery Plan	Συνήθως τα σχέδια επιχειρησιακής συνέχειας αλλά και αποκατάστασης καταστροφών περιλαμβάνουν βασικές υπηρεσίες των αεροδρομίων	Η φορείς αεροδρομίων θα πρεπει να συμπεριλάβουν στο, σχέδιο αποκατάστασης καταστροφών τους, σε περίπτωση που δεν το έχουν κάνει, τους μηχανισμούς εξυπηρετήσεις των επιβατών ΑμεΑ.

ΕΠΥΚΥΡΩΣΗ- Γνώμες ΥΠΔ και Ενδιαφερόμενων Προσώπων

Στο τελευταίο στάδιο παρουσιάζονται οι συμβουλές του υπεύθυνου προστασίας δεδομένων.

Η επεξεργασία των δεδομένων είναι αναγκαστική από νομικής και επιχειρησιακής άποψης για να μπορέσουν να παρασχεθούν όλες οι υπηρεσίες στους επιβάτες. Στη συγκεκριμένη περίπτωση εκ των πραγμάτων δεν μπορεί να ζητηθεί η άποψη των επιβατών για το πώς γίνεται η διαχείριση των δεδομένων τους.

Κεφάλαιο 7
Συμπεράσματα – Επίλογος

Τα έξυπνα αεροδρόμια είναι ένα τεράστιο περίπλοκο οικοσύστημα που αποτελείται από μια τεράστια γκάμα τεχνολογιών παλαιών και νέων που αλληλοεπιδρούν και συλλειτουργούν, κάποιες φορές όχι τόσο αρμονικά, με κύριο σκοπό την ασφαλή και ταχεία εξυπηρέτηση του επιβατικού κοινού. Ωστόσο, εκ των πραγμάτων συντελείται μία μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, από την οποία μπορεί να προκύψουν κίνδυνοι για θεμελιώδη ατομικά δικαιώματα και ελευθερίες. Ο Γενικός Κανονισμός Προσωπικών Δεδομένων έρχεται να διασφαλίσει και να προστατεύσει με την σειρά του ακόμα περισσότερο τα δικαιώματα και τις ελευθερίες του επιβατικού κοινού απαιτώντας μια πιο διαφανή επεξεργασία στα όποια προσωπικά δεδομένα συλλέγονται από ένα αεροδρόμιο.

Η παρούσα διατριβή έχει σκοπό να βοηθήσει τον αεροδρομιακό τομέα να κινηθεί προς την συμμόρφωση με τον ΓΚΠΔ και εστιάζει στην πεμπτουσία που κάνει τα αεροδρόμια να λειτουργούν και αυτή είναι τα μηνύματα ΙΑΤΑ.

Η Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων, λαμβάνει υπόψη τις ευπάθειες ασφάλειας, τους παράγοντες απειλών για την προστασία δεδομένων και τις τεχνολογίες που ισχύουν και εφαρμόζονται σε ένα αεροδρομιακό περιβάλλον, καθώς και τα μέτρα, τόσο τεχνικά όσο και οργανωτικά, που χρειάζονται για να προστατευτούνε αυτά τα δεδομένα.

Κατά την διάρκεια ανάλυσης της μεθοδολογίας της διαχείρισης κίνδυνου ασφάλειας, αναλύσαμε την διαφορά μεταξύ ασφάλειας και προστασίας των προσωπικών δεδομένων και είναι σημαντικό να αναφέρουμε ότι τα προσωπικά δεδομένα των επιβατών πρεπει να αποτελούν αναπόσπαστο κομμάτι των σχεδίων επιχειρησιακής συνέχειας αλλά και των σχεδίων αποκατάστασης από καταστροφές. Καταδείξαμε επίσης, στο πλαίσιο της παρούσας διατριβής, ότι είναι σημαντικό να γίνεται, πριν την εκπόνηση ΕΑΠΔ, μία συστηματική διαχείριση κινδύνων ασφαλείας, τα αποτελέσματα της οποίας θα τροφοδοτήσουν ακολούθως την ΕΑΠΔ.

Το αποτέλεσμα της ΕΑΠΔ είναι ότι η επεξεργασία αυτού του είδους δεδομένων είναι υψηλού κινδύνου και ότι η Βιομηχανία στο σύνολο της πρεπει να αναζητήσει λύσεις για την κατάλληλη διαφύλαξη αυτών των δεδομένων. Τα μέτρα τα οποία παρουσιάζονται για μετριασμό των κίνδυνων είναι μια αρχή προς την σωστή κατεύθυνση, αλλά λαμβάνοντας υπόψη την περιπλοκότητα και το εύρος των διασυνδέσεών μεταξύ των συστημάτων σίγουρα δεν μπορούν να ανταποκριθούν στις απαιτήσεις του ΓΚΠΔ.

Συνεπώς, η διατριβή κατέδειξε ότι μία ΕΑΠΔ είναι απαραίτητη για μία τέτοια επεξεργασία, αφού εντοπίζονται κίνδυνοι οι οποίοι δεν θα είχαν εντοπιστεί αν δεν ακολουθούνταν μία τέτοια συστηματική προσέγγιση για την εκτίμηση επιπτώσεων ως προς την προστασία προσωπικών δεδομένων.

Τέλος, μία σημαντική συνεισφορά επίσης της παρούσας διατριβής είναι ότι η μεθοδολογία που ακολουθήθηκε μπορεί να αποτελέσει οδηγό για οποιονδήποτε αεροδρομιακό φορέα πραγματοποιεί μία τέτοια επεξεργασία, αφού σε μεγάλο βαθμό οι επεξεργασίες αυτές έχουν κοινά χαρακτηριστικά ανεξαρτήτως του φορέα.

Παράρτημα Α
Εφαρμογή Εκτίμησης Κίνδυνου

Στο Παράρτημα Α « Εφαρμογή Εκτίμησης Κίνδυνου » πρόκειται να εφαρμόσουμε την μεθοδολογία εκτιμήσεων κίνδυνων OCTAVE- Allegro. Η εκτίμηση κίνδυνου έχει στόχο να υποστηρίξει την διεκπεραίωση της Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ).

Ακολουθώντας τα βήματα που αναλυθήκαν στο σημείο 5.5 της παρούσας διατριβής προχωράμε στην συμπλήρωση των αντίστοιχων φύλλων εργασίας.

Βήμα 1: Καθορίζουμε κριτήρια μέτρησης του κίνδυνου στις ανάλογες κατηγορίες και περιοχές, εδώ είναι καλό να αναφέρουμε ότι ο κάθε οργανισμός καθορίζει τα κριτήρια του ανάλογα με την διάθεση ανάληψης κινδύνων (risk appetite) που έχει ορίσει σαν οργανισμός.

Allegro Worksheet 1	**RISK MEASUREMENT CRITERIA – REPUTATION AND PASSENGER CONFIDENCE**		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Local public or customer attention quickly remedied.	Local media coverage for multiple days	International media coverage

Customer Loss	Minor impact to 1 stakeholder group	Loss of confidence of 1-2 key industrial customers	Loss of confidence in all stakeholder groups

Allegro Worksheet 2	**RISK MEASUREMENT CRITERIA – FINANCIAL**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 10% in yearly operating costs	Yearly operating costs increase by 10 to 30%.	Yearly operating costs increase by more than 30%.
Revenue Loss	Less than 5% yearly revenue loss	10 to 30% yearly revenue loss	Greater than 30% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $ 400.00	One-time financial cost of $ 500.00 to $ 2,000.00	One-time financial cost greater than $ 2500,00

Allegro Worksheet 3	**RISK MEASUREMENT CRITERIA – PRODUCTIVITY**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 10% for 1 to 2 day(s).	Staff work hours are increased between 20% and 40% for 2 to 4 day(s).	Staff work hours are increased by greater than 50% for 2 to 5 day(s).

Allegro Worksheet 4	**RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH**		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minor injuries or health affect to employees, contractors or public First Aid cases	Lost time injury In-patient medical care required for employees, contractors or public	Permanent impairment of significant aspects of passengers or staff members' health

Safety	Safety questioned	Safety affected	Safety violated

Allegro Worksheet 5	**RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than > 100,000 K are levied.	Fines between 1000,000 K and 500,000 K are levied.	GDPR sets forth fines of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year,
Lawsuits	Non-frivolous lawsuit or lawsuits less than 100,000 K are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between 1000,000 K and 500,000 K are levied are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than 10% are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
1	**Reputation and Customer Confidence**
3	**Financial**
2	**Productivity**
5	**Safety and Health**
4	**Fines and Legal Penalties**

Βήμα 2: Καταρτισμός προφίλ των Μηνυμάτων ΙΑΤΑ

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Μηνύματα ΙΑΤΑ	Ο σκοπός επεξεργασίας τους είναι για να μπορεί Ο διαχειριστής των αεροδρομίων να είναι σε θέση να προσεφέρει στους επιβάτες τις κατάλληλές υπηρεσίες που χρειάζονται μέσα στον χώρο του αεροδρομίου ώστε να ταξιδέψουν με ασφάλεια. Η επεξεργασία των πιο πάνω μηνυμάτων που εμπίπτουν και στις ειδικές κατηγορίες	**Οι πληροφορίες αυτές που εμπεριέχουν ευαίσθητα προσωπικά δεδομένα τροφοδοτούνται σε μορφή μηνυμάτων Passenger Service Message (PSM), Passenger Assistance List(PAL), Change Assistance List (CAL) σε διαφορά πληροφοριακά συστήματα.**

(4) Owner(s) *Who owns this information asset?*		
Διαχειριστής/Φορέας - Αεροδρομίων		
(5) Security Requirements *What are the security requirements for this information asset?*		
✓ **Confidentiality**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, δεδομένου ότι μπορεί να περιέχουν πολύ ευαίσθητα προσωπικά δεδομένα.	**Στις Πληροφορίες πρεπει να έχει πρόσβαση το ενδεδειγμένο προσωπικό του αεροδρομίου και εξωτερικοί συνεργάτες που καθορίζονται μέσω σύμβασης**
✓ **Integrity**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει αυτές τις πληροφορίες. Η τήρηση ακριβών αρχείων των δεδομένων είναι σημαντική για την σωστή εξυπηρέτηση των επιβατών με κινητικά προβλήματα ή επιβατών με αναπηρία	**Μόνο εξουσιοδοτημένο προσωπικό του αεροδρομίου και των συνεργατών του, που καθορίζονται μέσω σύμβασης, αλλά και των αεροπορικών εταιρειών πρεπει να μπορούν τροποποιήσουν τις πληροφορίες**
✓ **Availability**	Οι πληροφορίες πρεπει να είναι διαθέσιμες στον φορέα για να μπορεί να διεκπεραιώνει τις εργασίες του , ως εξής:	**Η διαθεσιμότητα των συστημάτων είναι υψίστης σημασίας τόσο για την παροχή υπηρεσιών αλλά και για λογούς ασφάλειας**
	Οι πληροφορίες πρέπει να είναι διαθέσιμες για 24 ώρες, 7 ημέρες/εβδομάδα, 52 εβδομάδες/έτος	**Τα αεροδρόμια είναι ανοικτά και λειτουργούν επί 24ωρου βάσεως.**

✓ **Other**	This asset has special regulatory compliance protection requirements, as follows:	**Επειδή τα πιο πάνω μηνύματα εμπεριέχουν ευαίσθητα προσωπικά δεδομένα υπόκεινται στον ΓΚΠΔ.**

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
✓ Confidentiality	✓ Integrity	✓ Availability	Other

Βήμα 3: Χαρτογράφηση του «κύκλου ζωής» των Μηνυμάτων ΙΑΤΑ

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. SITA Designated address: Τα μηνύματα PAL./ CAL μπορεί αποστέλνονται σε μια αποκλειστική διεύθυνση SITA του αεροδρόμιου	Τμήμα Πληροφορική Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων
2. Email address Τα μηνύματα PAL./ CAL μπορεί αποστέλνονται σε μια ηλεκτρονική διεύθυνση (email)	Τμήμα Πληροφορική Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων
3. Airport Operational Database (AODB): Υπάρχουν AODB εφαρμογές οι οποίες μπορεί να λαμβάνουν μηνύματα PAL/CAL, με αυτόν τον τρόπο ο διαχειριστής του αεροδρομίου μπορεί να έχει μια σφαιρική εικόνα για τους αναμενομένους PRM επιβάτες και πως να τους εξυπηρέτηση.	Τμήμα Πληροφορική Αεροδρομίων
	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων

4. **Baggage Reconciliation System (BRS): Κατά την διάρκεια του Check-in τα συστήματα αυτά λαμβάνουν πληροφορίες όπως όνομα του επιβάτη, αριθμό και ημερομηνία πτήσης, την θέση του επιβάτη των αριθμό αποσκευών του επιβάτη, αριθμός ακολουθίας επιβατών (SQNR).**	Τμήμα Πληροφορικής Αεροδρομίων
5. **Common Use Passenger Processing Systems (CUPPS): Είναι εύκολο να αντιληφθούμε ότι αυτή η κοινή πλατφόρμα μπορεί για σκοπούς υποστήριξης να συλλεγεί διαφορά στοιχεία σε μορφή αρχείων (logs). Τα αρχεία αυτά εμπεριέχουν τα προσωπικά στοιχεία επιβατών όπως για παράδειγμα όνομα, επίθετο, αριθμό πτήσης, την αερογραμμή αλλά και αριθμούς πιστωτικών καρτών.**	Τμήμα Πληροφορικής Αεροδρομίων
6. **Message Broker ένας message broker μπορεί να στέλνει μηνύματα PAL/CAL, BSM αλλά και άλλους τύπους μνημάτων σε διαφορά αεροδρομιακά συστήματα.**	Τμήμα Πληροφορικής Αεροδρομίων
7. **Network and Systems Infrastructure: Τα μηνύματα μεταφέρονται στα διαφορά συστήματα μέσο τη υποδομής του δικτύου και των συστημάτων του αεροδρομίου**	Τμήμα Πληροφορικής Αεροδρομίων
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. **Departure Control Systems (DCS)/ Passenger Processing Systems (PSS) / συστήματα κρατήσεων αεροπορικών εταιρειών (CRS): Είναι τα πρωτογενή συστήματα που δημιουργούνται και διανέμονται η πληροφορίες.**	Αερογραμμές
2. **Internet: Τα μηνύματα IATA λαμβάνονται μέσω του διαδικτύου στις ενδεδειγμένες ηλεκτρονικές διευθύνσεις**	Άγνωστος

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Data Centres 2. Υπολογιστές που χρησιμοποιούνται από το προσωπικό	Τμήμα Πληροφορικής Αεροδρομίων
	Προσωπικό
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Υπολογιστές που χρησιμοποιούνται από εξωτερικούς συνεργάτες	Προσωπικό

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
1. Προσωπικό Τμήματος Πληροφορικής και Τηλεπικοινωνιών	Τμήμα Πληροφορικής Αεροδρομίων
2. Προσωπικό Τμήματος Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων	Τμήμα Επιχειρησιακών Δραστηριοτήτων Αεροδρομίων
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	**ORGANIZATION**
1. Προσωπικό εξωτερικού συνεργάτη	Άγνωστος
2. Προσωπικό αερογραμμών	Άγνωστος

Βήμα 4: Προσδιορισμός περιοχών ανησυχίας (Area of Concern)

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk		Information Asset	Μηνύματα IATA
		Area of Concern	Η διαθεσιμότητα των μηνυμάτων IATA είναι υψίστης σημασίας τόσο για την παροχή υπηρεσιών αλλά και για λογούς ασφάλειας. Μια επίθεση τύπου Denial of Service θα μπορούσε να σταματήσει την λήψη αυτών των μηνυμάτων.
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Κυβερνοεγκληματίες, Hacktivists.
		(2) Means *How would the actor do it? What would they do?*	Μια επίθεση άρνησης υπηρεσίας (DDos) είναι μια κακόβουλη προσπάθεια να διακοπεί η κίνηση του δικτύου προς ένα server, προς μια υπηρεσία ή ένα άλλο δίκτυο συντρίβοντας τον στόχο ή την υποδομή του με μια διαδικτυακή κίνηση (Internet Traffic) που ονομάζεται πλημμύρα (flood) .
		(3) Motive *What is the actor's reason for doing it?*	Οι κυβερνοεγκληματίες έχουν οικονομικά κίνητρα και ποικίλλουν σε επίπεδο δεξιοτήτων και πόρων. Hacktivists: Άτομα ή ομάδες που παρακινούνται από έναν πολιτικό, κοινωνικό ή θρησκευτικό σκοπό
		(4) Outcome *What would be the resulting effect on the information asset?*	**Disclosure** **Destruction** **Modification** ✓ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Οι επιθέσεις DDoS είναι αποτελεσματικές χρησιμοποιώντας πολλαπλά παραβιασμένα συστήματα υπολογιστών ως πηγές επιθέσεων, που μπορεί να περιλαμβάνουν υπολογιστές και άλλους δικτυωμένους πόρους, όπως συσκευές IoT.

		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	**Medium**	**Low**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*			(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*	
				Impact Area	**Value**	**Score**
	Διακοπή υπηρεσιών αεροδρομίου. Το επιβατικό κοινό θα υποστεί ταλαιπωρία και καθυστερήσεις.			Reputation & Customer Confidence	Medium (2)	2
	Οι οικονομικές συνέπειες υπολογίζονται να είναι χαμηλού βαθμού.			Financial	Low (1)	3
	Το προσωπικό θα πρεπει να καταφύγει σε manual διαδικασίες για να διεκπεραίωση των εργασιών του.			Productivity	Medium (2)	4
	Τα ΑμεΑ πρόκειται να υποστούν σωματική και πνευματική ταλαιπωρία που θα τους επηρεάσει σε σημαντικό βαθμό			Safety & Health	High (3)	15
	Αν η εταιρεία δεν έχει λάβει τα κατάλληλα τεχνολογικά και οργανωτικά μέτρα υπόκειται σε κυρώσεις σύμφωνα με το NIS Directive			Fines & Legal Penalties	High (3)	12
				User Defined Impact Area	N/A	
					Relative Risk Score	**36**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Network and Systems Infrastructure.	**Αγορά υπηρεσιών προστασίας δικτύου από έναν Internet Service Provider (ISP).** Οι επιθέσεις DDoS στα δίκτυα των εταιρειών και στην υποδομή IT αυξάνονται σε μέγεθος, συχνότητα και πολυπλοκότητα. Απλές λύσεις όπως, firewalls και Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS) δεν είναι πλέον επαρκής για να σταματήσουν τέτοιου είδους επιθέσεις. Επίσης, οι απλές διαδικτυακές λύσεις ασφάλειας δεν μπορούν να σταματήσουν μια έξυπνη επίθεση DDoS αφού δεν μπορούν να χειριστούν επιθέσεις που υπερβαίνουν την ικανότητα σύνδεσής τους και οι χάκερ χρησιμοποιούν αυτές τις επιθέσεις για να υπονομεύσουν την άμυνα του δικτύου και στη συνέχεια να διεισδύσουν στο δίκτυο της εταιρείας.		

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Μηνύματα IATA
		Area of Concern	Μη εξουσιοδοτημένη πρόσβαση , και διαρροή δεδομένων των επιβατών.
		(1) Actor *Who would exploit the area of concern or threat?*	Κυβερνοεγκληματίες, Hacktivists, Insiders
		(2) Means *How would the actor do it? What would they do?*	• Επίθεση κακόβουλου Λογισμικού - Malware Attack • Εκμετάλλευση από κακόβουλες συσκευές -Counterfeit by Malicious Devices • Man in the middle attacks • Επιθέσεις κατά του απορρήτου - Privacy Attacks

			• Phishing attacks.		
		(3) Motive *What is the actor's reason for doing it?*	Οι κυβερνοεγκληματίες έχουν οικονομικά κίνητρα και ποικίλλουν σε επίπεδο δεξιοτήτων και πόρων. Hacktivists: Άτομα ή ομάδες που παρακινούνται από έναν πολιτικό, κοινωνικό ή θρησκευτικό σκοπό Insiders: Υπάλληλοι που κατά λάθος ή κακόβουλα μπορεί προκαλέσουν κάποιου είδους ζημία σε έναν οργανισμό		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	✓ **Destruction** ✓ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	• Αδύναμοι ή επαναχρησιμοποιούμενοι κωδικοί πρόσβασης (Weak password protection) • Αδύναμοι μηχανισμοί αναβαθμίσεων ασφάλειας - Lack of regular patches and updates and weak update mechanism • Κακοδιαχείριση συσκευών IoT - Poor IoT Device management που χρησιμοποιούν default κωδικούς • Ανεπάρκεια Δεξιοτήτων στον τομέα IoT - The IoT skills gap • Ανασφαλής μεταφορά και αποθήκευση δεδομένων - Insecure Data Transfer and Storage • Τροποποίηση Συσκευών - Device Modification • Μη κατάλληλος Διαχωρισμός Δικτυών - Network Segregation		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	**Medium**	**Low**
	(7) Consequences			(8) Severity *How severe are these consequences to the*	

	What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	Η φήμη του Οργανισμού που παρέχει διάφορες υπηρεσίες θα πληγεί σε μεγάλο βαθμό, επίσης η «αυτοπεποίθηση» του επιβατικού κοινού προς τον φορέα μπορεί να πληγεί ανεπανόρθωτά.	Reputation & Passenger Confidence	High (3)	3
	Η ανάκαμψη από τέτοιου είδους επιθέσεις είναι συνήθως πολυδάπανοι προς τον φορέα	Financial	High (3)	9
	Η παραγωγικότητα του προσωπικού χωρίς την χρήση συστημάτων πληροφορικής θα μειωθεί κατακόρυφα.	Productivity	High (3)	6
	Τα ΑμεΑ πρόκειται να υποστούν σωματική και πνευματική ταλαιπωρία που θα τους επηρεάσει σε σημαντικό βαθμό. Επίσης, μπορεί να υποστούν διακρίσεις ως προς τους χρόνους αλλά και την ποιότητα εξυπηρέτησης	Safety & Health	High (3)	15
	Αν η εταιρεία δεν έχει λάβει τα κατάλληλα τεχνολογικά και οργανωτικά μέτρα υπόκειται σε κυρώσεις σύμφωνα με το NIS Directive αλλά και από τον ΓΚΠΔ σε περίπτωση διαρροής των προσωπικών δεδομένων	Fines & Legal Penalties	High (3)	12
		User Defined Impact Area	N/A	
		Relative Risk Score		**45**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical Containers	**Τεχνικά μετρά Πρόληψης** • Δοκιμή διείσδυσης (Penetration Test) • Ανίχνευση ευπαθειών (Vulnerability Scanning) • Απαιτήσεις συμμόρφωσης (Compliance Requirements) • Ανακάλυψη δικτύου, Αναγνώριση θύρας και πρωτοκόλλου (Network Discovery, Port and Protocol Identification) • Ανασκόπηση διαμόρφωσης συστήματος (System Configuration Review) • Χρήση εφαρμογών κατά κακόβουλου λογισμικού - Antimalware • Αναβάθμιση λογισμικού και υλικού -Software and Hardware Updates • Firewalls και Τμηματοποίηση Δικτύου – Firewalls and Network Segmentation με την χρήση εσωτερικών firewalls και όχι μόνο με την χρήση VLANs (Λογικού διαχωρισμού) • Ισχυρές Μέθοδοι Αυθεντικοποίησης - Strong User Authentication • Αλλαγή Προκαθορισμένων διαπιστευτηρίων - Change Default Credentials • Κρυπτογράφηση Δεδομένων - Data Encryption • Έλεγχοι για την διαχείριση ιδιωτικών συσκευών- Bring your own device controls • Ασφάλεια εφαρμογών & Ασφαλής σχεδιασμός - Application security & Secure design • Σχέδια αποκατάστασης από καταστροφές- Disaster Recovery Plans		

People containers	**Οργανωτικά μέτρα Ασφάλειας** • Διορισμός ενός Υπεύθυνου Ασφάλειας Πληροφορικής - Appoint an IT Security Officer. • Εφαρμογή πολιτικών για την εγκατάσταση προγραμμάτων - Enforce rules Governing Installation of Software • Συνεχής Επίβλεψη της Ασφάλειας Πληροφορικής - Continuous Monitoring of Information Security • Εγκαθίδρυση ενός προγράμματος διαχείρισης της ασφάλειας της Πληροφορικής και συμμόρφωση με τα διεθνή πρότυπα και κανονισμούς - ISMS, International standards, and compliance Audits • Συμμόρφωση με την Ασφάλεια πληροφορικής από εξωτερικούς συνεργάτες - Information Security Compliance from external providers • Εξιδεικευμένη εκπαίδευση στην Ασφάλεια Πληροφοριών - Specialized Information Security training • Εκπαίδευση Προσωπικού Αεροδρομίου στην αντιμετώπιση περιστατικών για συστήματα πληροφορικής- Train Airport Personnel in incident response for IT systems • Βασική εκπαίδευση ευαισθητοποίησης για την ασφάλεια σε όλους τους χρήστες πληροφοριακών συστημάτων - Basic Security awareness training to all information system users **Πολίτικες και διεθνή πρότυπα** • Διαχείριση πρόσβασης χρηστών (User Access Management) • Απαιτήσεις ασφάλειας προσωπικού για τρίτους παρόχους - Personnel security requirements for third party providers • Διασφάλιση συμφωνίας πρόσβασης σε άτομα πριν από την παραχώρηση πρόσβασης - Ensure access agreement to individuals prior to grant access • Δοκιμή και άσκηση ικανότητας απόκρισης περιστατικού σε συστήματα πληροφορικής - Test and exercise incident response capability for IT systems • Έλεγχος ατόμων πριν από την εξουσιοδότηση πρόσβασης στο σύστημα πληροφορικής των αεροδρομίων - Screen individuals prior to authorize access to airports IT system.
Physical Containers	**Φυσικά Μέτρα προστασίας** Η είσοδος σε όλες τις τοποθεσίες που φιλοξενούν network and system infrastructure components πρεπει να ελέγχεται μέσω συστημάτων access control και CCTV

Βήμα 5 : Προσδιορισμός Σεναρίων Απειλών (Identify Threat Scenarios)

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
<u>Scenario 1:</u> Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
<u>Scenario 2:</u> Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**

Interrupted so that it cannot be accessed for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	✓ **Yes (accidentally)**	✓ **Yes (intentionally)**

Threat Scenario Questionnaire – 1 (cont.)	Technical Containers

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

Unintended disclosure of your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	No	✓ Yes (disclosure)	✓ Yes (modification)	✓ Yes (interruption)	✓ Yes (loss)
A system crash of known or unknown origin occurs	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	Yes (loss)
A hardware defect occurs	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	Yes (loss)
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	No	✓ Yes (disclosure)	✓ Yes (modification)	✓ Yes (interruption)	✓ Yes (loss)

Power supply to technical containers is interrupted	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	Yes (loss)
Problems with telecommunications occur	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	Yes (loss)
Other third-party problems or systems	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	Yes (loss)
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	✓ Yes (loss)

Threat Scenario Questionnaire – 2	Physical Containers

This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1:

Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, accidentally or intentionally, causing your information asset to be:

Disclosed to unauthorized individuals?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Modified so that it is not usable for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)

Interrupted so that it cannot be accessed for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, accidentally or intentionally, causing your information asset to be:			
Disclosed to unauthorized individuals?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Modified so that it is not usable for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Interrupted so that it cannot be accessed for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)

Threat Scenario Questionnaire -2 (cont.)	Physical Containers

Scenario 3:

In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

Unintended disclosure of your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	No	✓ Yes (disclosure)	✓ Yes (modification)	✓ Yes (interruption)	✓ Yes (loss)
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	No	Yes (disclosure)	Yes (modification)	✓ Yes (interruption)	✓ Yes (loss)

Threat Scenario Questionnaire – 3	People

This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1:

Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, accidentally or intentionally, cause the information asset to be:

Disclosed to unauthorized individuals?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Modified so that it is not usable for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)

Interrupted so that it cannot be accessed for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	✓ Yes (accidentally)	✓ Yes (intentionally)
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, accidentally or intentionally, cause your information asset to be:			
Disclosed to unauthorized individuals?	No	✓ Yes (accidentally)	✓ Yes (intentionally)

Βήμα 8: Κατηγοριοποίηση κίνδυνων σε 4 κατηγορίες (POOL) όπως φαίνεται κα στην εικόνα πιο κάτω και στρατηγικές μετριασμού κινδύνου

RELATIVE RISK MATRIX			
PROBABILITY	RISK SCORE		
	30 TO 45	16 TO 29	0 TO 15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Εικόνα 34 Αποτέλεσμα Κατηγοριοποίησης κινδύνων / Αποτέλεσμα αντιστοίχησες ι κατηγοριών σπουδαιότητας κινδύνου με στρατηγική διαχείρισης του ρίσκου

Παράρτημα Β Πρόσφατες Κυβερνοεπιθέσεις στην Βιομηχανία Αεροναυτιλίας

Ο πιο κάτω πίνακας παραθέτει πληροφορίες σχετικά με τις πιο πρόσφατες επιθέσεις που έγιναν στην Βιομηχανία Aviation . Η πληροφορίες αναφέρουν το είδος της επίθεσης που διεκπεραιώθηκε, την πηγή των απειλών όπως αναλύθηκε στο σημείο 3.3 της παρούσας διατριβής αλλά και τις επιπτώσεις, όπως την διαρροή προσωπικών δεομένων

Date	Airline/Organisation	Details of the event
May 2022	SpiceJet	Following a massive ransomware attack on SpiceJet, hundreds of passengers were stranded at airports across India, particularly those airports where restrictions on night operations were in place. SpiceJet has not revealed which systems were targeted or what it did to overcome the attacks, but whatever SpiceJet did was effective as services were resumed within hours of the attack beginning, rather than in days as was the case with the ransomware attack on Colonial Pipeline in 2021.

April 2022	SunWing Airlines Inc.	Canadian low-cost airline Sunwing Airlines faced four days of extensive flight delays after the third-party software system it used for check-in and boarding was breached by hackers. The attack forced Sunwing to resort to manually checking in passengers in an effort to minimize disruption to its schedule and caused the Canadian authorities to suspend operations temporarily to ensure that the breach was remedied before flights could resume.
March 2022	Russian CAA	In what appears to have been a retaliatory strike in response to Russia's invasion of Ukraine, an unidentified group (presumed to be the Anonymous Hacking Group) carried out an extremely effective attack on the Russian Federal Air Transport Agency. As part of the attack, all aircraft registration data and emails, totalling approximately a massive 65 terabytes of data, were deleted from the Agency's servers. The attack was so successful that until back-up copies of the electronic data could be found the Agency was forced to resort to using pen and paper and to sending information in hard copy through the post.

March 2021	SITA	SITA, an airline technology and communication provider that operates passenger processing systems for airlines, was the victim of a cyber-attack involving passenger data. SITA serves 90% of the world's airlines and disclosed that among the airlines affected were various major airlines including Air India, Finnair, Japan Airlines, Jeju Air, Lufthansa, Malaysia Airlines, Singapore Airlines and Cathay Pacific. Singapore Airlines reported that 580,000 of its frequent flyer members were compromised in the attack and Air India estimated that personal data relating to 4.5 million of its passengers was stolen.
2020	VT San Antonio Aerospace	Demonstrating the importance of maintaining security throughout the entirety of the supply chain, VT San Antonio Aerospace fell victim to a sophisticated attack by the Maze Ransomware Group when the criminal group gained access to and encrypted the San Antonio network. The system in question was reportedly recovered within three days but by that time a vast amount of data (1 terabyte) had already been stolen.
January 2020	easyJet	easyJet was the victim of a cyber-attack in which hackers obtained the credit-card information of 2,208 customers.

		The carrier did not notify passengers of the attack until 4 months after the incident, in May 2020 and as a result they are now facing a class-action suit from 10,000 passengers, seeking around £18 billion in damages.
February 2019	Ben Gurion Airport	In an example of the immense pressures that aviation industry stakeholders can come under when defending themselves from cyber-attacks, a spokesperson for Ben Gurion Airport revealed that they were blocking three million attempts per day by bots to breach their systems. To deal with these attacks Ben Gurion Airport has established a Security Operation Centre to coordinate defenses; it is believed that the Airport is one of the first in the world to do so.
December 2019	Albany International Airport	A criminal gang succeeded in gaining access to Albany International Airport's database, which was then encrypted and ransomed back to the airport by the gang for a five-figure sum that was paid in Bitcoin. Fortunately, the attack did not affect operations at the airport, and it is understood that the ransom was reimbursed by the Airport's insurer, thus demonstrating the necessity of having robust procedures and comprehensive insurance in place to deal with attacks like these.

August 2019	Air New Zealand	Personal data of over 120,000 customers was compromised following a successful phishing attack on two members of staff. The attackers used the information gained through phishing to access Air New Zealand's frequent flyer programme, from where they were then able to obtain extensive personal data relating to passengers on the programme. Fortunately, no passport or credit-card information were stolen on this occasion.
August 2018	British Airways	British Airways' system was infected with a malicious code, resulting in the theft of personal data relating to 429,612 customers and members of staff from its servers. The information extracted included names, addresses and credit-card information relating to 244,000 customers. A subsequent investigation by the Information Commissioner's Office (the "ICO") found that the airline lacked adequate security measures to protect the personal data under its control. As a result, British Airways received a record-breaking fine of £20 million for its failure to protect its customers.
August 2018	Air Canada	Air Canada's mobile application software was hacked, resulting in the potential leak of highly sensitive

		personal data relating to its customers' passport information.
August 2018	Cathay Pacific	A cyber-attack led to 9.4 million accounts being breached and the theft from within the compromised accounts of extensive personal data regarding the airline's customers. An investigation by the ICO revealed that Cathay Pacific's system lacked any password protection for backup files and that the OS was out of date. After the attack, Cathay Pacific introduced multi-factor authentication to prevent future attacks. As a result of this failure the ICO issued Cathay Pacific with a fine for £500,000.
September 2017	Data Airlines	Delta and Sears Department Store were both involved in an extensive data breach in April 2018 when an online support service used by both organizations suffered from an extensive malware attack. The attack lasted from September to October 2017, but Delta and Sears only became aware of the attack in the following year. As a result of the attack the credit-card information belonging to approximately 100,000 customers was lost.

September 2018	Bristol Airport	In a dramatic ransomware attack, the electronic flight information at the airport was disabled and the screens showing all flight information were taken offline in order to contain the threat. Bristol Airport did not pay the ransom to the perpetrators of the attack and instead used whiteboards that were updated manually to keep passengers informed of flight details until the attack was thwarted.
November 2015	Sweden Air traffic Control	Sections of Sweden's air traffic control capabilities were blocked for five days following a successful attack by "Fancy Bear", otherwise known as APT28, a Russian cyber espionage organization that is believed by some industry analysts to be associated with GRU, the Russian military intelligence agency. Sweden initially blamed a solar flare for the outage, but has since confirmed that the event, which caused huge disruption to air traffic travelling to, from and across Sweden, was a result of a malicious attack.

Πίνακας 14 Πρόσφατες κυβερνοεπιθέσεις στην Βιομηχανία Aviation [12]

Βιβλιογραφία

[1] G. Lykou, A. Anagnostopoulou και D. Gritzalis, «Implementing Cyber-Security Measures in Airports,» σε *2018 Global Internet of Things Summit (GIoTS)*, Bilbao, 2018.

[2] ENISA, «Securing Smart Airports,» European Union Agency for Network and Information Security Science and Technology Park of Crete, Athens, 2016.

[3] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram και H. Janicke, «A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports,» *IEEE Access,* τόμ. 8, pp. 209802-209834, 2020.

[4] E. Ukwandu, M. B. Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis και X. Bellekens, «Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends,» *arXiv,* τόμ. 1, 2021.

[5] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson και B. M. Phares, «CYBER SECURITY FOR AIRPORTS,» *International Journal for Traffic and Transport Engineering,* τόμ. 3, αρ. 4, pp. 365-376, 2013.

[6] ENISA, Baseline Security Recommendations for IoT, Athens: European Union Agency For Network And Information Security, 2017.

[7] ENISA, «Baseline Security Recomendations for IoT in the context of Critical Information Infrastructures,» ENISA, Athens, 2017.

[8] D. Schaar και S. Lance, «Analysis of Airport Stakeholders,» σε *Conference: Integrated Communications Navigation and Surveillance Conference (ICNS), 2010*, Herndon, 2010.

[9] J. P. R. Hough, R. White, S. Gonzalez, F. Haley, M. Hyde, J. Willis, G. de Grandis και J. Walfish, «ACRP REPORT 59,» National Academy of Sciences, WASHINGTON, D.C., 2012.

[10] SITA 2018 Air Transport, «2018 AIR TRANSPORT CYBER SECURITY INSIHTS,» 2018.

[11] EUROCONTROL, Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?, BRUSSELS: EUROCONTROL, 2021.

[12] STEPHERSON HARWOOD, «https://www.shlegal.com/,» 8 2022. [Ηλεκτρονικό]. Available: https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-

covid#:~:text=This%20data%20showed%20that%20cyber,all%202020%20aviation%20cyber%2Dattacks..

[13] ENISA, «ENISA THREAT LANDSCAPE 2021,» ENISA, ATHENS, 2021.

[14] Airport Business, The Leading Airport Magazine, «http://www.airport-business.com/,» 1 10 2008. [Ηλεκτρονικό]. Available: http://www.airport-business.com/2008/05/prm-notification-tool-advice-for-airports/.

[15] Aerocrs, «https://www.aerocrs.com/,» 26 May 2019. [Ηλεκτρονικό]. Available: https://support.aerocrs.com/hc/en-us/articles/360028504072-26-MAY-2019-PAL-CAL-messages.

[16] TAV Technologies , «https://tavtechnologies.aero/,» 2022. [Ηλεκτρονικό]. Available: https://tavtechnologies.aero/en-EN/products/passenger-baggage-processing/pages/cupps-products-services.

[17] «https://gdpr.eu/,» Proton AG, 2022. [Ηλεκτρονικό]. Available: https://gdpr.eu/what-is-gdpr/.

[18] International Association of Privacy Professionals (IAPP), European Data Protection Law and PRactice, Portsmouth: IAPP, 2018.

[19] Office of the Commissioner for Personal Data Protection, «https://www.dataprotection.gov.cy/,» Department of Information Technology Services, 2018. [Ηλεκτρονικό]. Available: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_gr/page2c_gr?opendocument.

[20] Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether, Brussels, 2017.

[21] CNIL, «https://www.cnil.fr,» February 2018. [Ηλεκτρονικό]. Available: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.

[22] European Union, «REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,» *Official Journal of the European Union,* 2016.

[23] R. A. Caralli, J. F. Stevens, L. R. Young και W. R. Wilson, «Introducing OCTAVE Allegro:,» Carnegie Mellon University., Hanscom , 2007.

[24] CNIL, «https://www.cnil.fr/,» 30 June 2021. [Ηλεκτρονικό]. Available: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment.

[25] «DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» *Official Journal of the European Union* , 2016.

[26] D. Ancell, «THE PARADOX OF COMPETITION FOR AIRLINE PASSENGERS,» *Journal of Air Transport Studies,* τόμ. 7, αρ. 1, pp. 111-129, 2016.

[27] ENISA, Handbook on Security of Personal Data Processing, Athens : European Union Agency For Network and Information Security, 2017.