ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. "ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"ΠΡΟΤΥΠΑ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΕΣ ΔΙΟΙΚΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΙΣ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ ΤΟΥ ΑΕΡΟΠΟΡΙΚΟΥ ΤΟΜΕΑ"

(INFORMATION SECURITY MANAGEMENT STANDARDS AND METHODOLOGIES IN CRITICAL INFRASTRUCTURES OF THE AVIATION INDUSTRY)

Τσόγκα Ελένη Α.Μ. ΜΤΕ 2226

Επιβλέπων Καθηγητής: Γκρίτζαλης Στέφανος

Πειραιάς, Απρίλιος 2024

ΠΕΡΙΛΗΨΗ

Η εγκατάσταση και ανάπτυξη ενός συστήματος διαχείρισης ασφάλειας πληροφοριών, αποτελεί κύριο στοιχείο της πολιτικής ασφάλειας των σύγχρονων οργανισμών. Σημαντικό τμήμα του ΣΔΑΠ είναι η διαχείριση επικινδυνότητας, μια διεργασιοκεντρική διαδικασία, που βασίζεται σε συγκεκριμένη μεθοδολογία και περιλαμβάνεται σε δημοφιλή πρότυπα, τα οποία παρατίθενται ενδεικτικά. Η διαχείριση της ασφάλειας πληροφοριών, έχει ιδιαίτερη σημασία στους οργανισμούς που συνιστούν κρίσιμες υποδομές, παρέχοντας αγαθά και υπηρεσίες ζωτικής σημασίας για το κοινωνικό σύνολο. Ο υψηλός βαθμός εξάρτησης των κρίσιμων υποδομών από τα πληροφοριακά συστήματα, καθώς και η διασύνδεση των συστημάτων, είναι παράγοντες που αυξάνουν τις απειλές σε βάρος τους, με εντονότερες αυτές του κυβερνοχώρου. Για την αποφυγή της διατάραξης της λειτουργίας τους, απαιτείται η ανάπτυξη κατάλληλων μεθοδολογιών που θα λαμβάνουν υπόψη τις αλληλεξαρτήσεις μεταξύ των κρίσιμων υποδομών, τις ευρύτερες κοινωνικές και οικονομικές συνέπειες και το επίπεδο ανθεκτικότητας της υποδομής. Οι κρίσιμες υποδομές του αεροπορικού τομέα, αποτελούν μια χαρακτηριστική περίπτωση, στην οποία η ανάπτυξη των νέων τεχνολογιών, δημιουργεί αντίστοιχα νέου τύπου απειλές, που στοχεύουν στην εκμετάλλευση των ευπαθειών των πληροφοριακών τους συστημάτων. Η πρόκληση για τους φορείς προστασίας της πολιτικής αεροπορίας σε εθνικό, ενωσιακό και διεθνές επίπεδο, είναι η χάραξη αποτελεσματικής στρατηγικής για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών και οντοτήτων, σε συνδυασμό με την ασφαλή χρήση της τεχνολογίας.

Λέξεις κλειδιά: Ασφάλεια πληροφοριών, διαχείριση επικινδυνότητας, κρίσιμες υποδομές/οντότητες, ανθεκτικότητα, αεροπορικός τομέας, κυβερνοασφάλεια

ABSTRACT

The implementation and development of an Information Security Management System (ISMS) is a key element of the security policy of modern organizations. An important part of the ISMS is risk management, a process-oriented procedure that is based on a specific methodology and is included in popular standards, which are listed as examples. Information security management is of particular importance for organizations that constitute critical infrastructures, providing goods and services of vital importance to society. The heightened reliance of critical infrastructure on information systems, coupled with the increasing interconnection of these systems, presents a significant escalation of potential threats. Among these threats, cyberattacks pose the most substantial risk**.** In order to avoid operational disruption, it is necessary to develop appropriate methodologies that will take into account the interdependencies between critical infrastructures, the broader social and economic consequences and the level of resilience of the infrastructure. The aviation sector's dependence on evolving technologies, creates a growing risk landscape, with attackers targeting information system vulnerabilities. Aviation security stakeholders at national and international levels, face the dual challenge of enhancing the resilience of critical infrastructure and entities, while ensuring the safe integration of new technologies.

Key words: Information security management, risk management, critical infrastructures/entities, resilience, aviation industry, cybersecurity

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ

Στο σύγχρονο κοινωνικοοικονομικό περιβάλλον, οι οργανισμοί αντιμετωπίζουν σύνθετα προβλήματα, προκειμένου να διασφαλίσουν τις πληροφορίες που διαχειρίζονται. Η τεχνολογική εξέλιξη, δημιουργεί νέες προοπτικές, αλλά και κινδύνους, οι οποίοι δεν μπορούν να ελαχιστοποιηθούν, παρά μόνο μέσα από τη καθιέρωση ολοκληρωμένων συστημάτων ασφαλείας, που περιλαμβάνουν διεργασίες αποτίμησης της επικινδυνότητας. Η προτυποποίηση στον τομέα της διαχείρισης επικινδυνότητας πληροφοριών, παίζει σημαντικό ρόλο για την ομοιομορφία και την αποτελεσματικότητα των πρακτικών ασφαλείας. Λόγω των ραγδαίων τεχνολογικών εξελίξεων, τα τελευταία χρόνια υπάρχει έντονη κινητοποίηση των εμπλεκόμενων φορέων για την αναθεώρηση και προσαρμογή τόσο των Προτύπων και Πλαισίων, όσο και των θεσμικών κανονιστικών κειμένων στο χώρο της της ασφάλειας πληροφοριών, με έμφαση στην Κυβερνοασφάλεια. Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), με πρόσφατες μελέτες του, εστιάζει στη διαλειτουργικότητα προτύπων, πλαισίων και μεθοδολογιών, ώστε να είναι δυνατή η διαμόρφωση μιας κοινής παγκόσμιας γλώσσας στο ζήτημα της διαχείρισης επικινδυνότητας.

Ο ρόλος της Τεχνολογίας Πληροφοριών στη λειτουργία των κρίσιμων υποδομών, σε ένα περιβάλλον εντατικής ψηφιοποίησης, χρήσης του Διαδικτύου των πραγμάτων (IoT) και της τεχνολογίας επιχειρησιακής λειτουργίας (OT), καθώς και των αναδυόμενων τεχνολογιών, όπως η τεχνητή νοημοσύνη, αποκτά ολοένα και μεγαλύτερη σημασία για την ασφάλειά τους. Μετά από περιστατικά επιθέσεων κατά κρίσιμων υποδομών, με εκμετάλλευση των ευπαθειών των πληροφοριακών τους συστημάτων, αναδείχθηκε η ανάγκη ανάπτυξης ολοκληρωμένων πολιτικών προστασίας τους, τόσο από τις ίδιες τις οντότητες που τις διαχειρίζονται, όσο και σε εθνικό και διεθνές επίπεδο. Η αποτίμηση της κρισιμότητας και της επικινδυνότητας, ώστε να ληφθούν τα κατάλληλα μέτρα, στηρίζεται στη κατανόηση των ιδιομορφιών των κρίσιμων υποδομών, με κυριότερη τις αλληλεξαρτήσεις τους, σε συνδυασμό με το είδος και το εύρος των συνεπειών που επιφέρει η διατάραξη της λειτουργίας τους. Η όλο και εντονότερη έκθεση των πληροφοριακών συστημάτων στους κινδύνους του κυβερνοχώρου, επιβάλλει την υιοθέτηση μιας μακρόπνοης στρατηγικής για την Κυβερνοασφάλεια σε παγκόσμιο επίπεδο, σαν θεμελιώδες στοιχείο της προστασίας των κρίσιμων υποδομών.

Η περίπτωση των αερολιμένων, μιας κρίσιμης υποδομής του τομέα των μεταφορών, καταδεικνύει τη σημασία της Κυβερνοασφάλειας. Από το στάδιο της προστασίας τους σε επίπεδο φυσικών εγκαταστάσεων και υλικού, έχουμε μεταβεί με ραγδαίους ρυθμούς στο στάδιο των ψηφιοποιημένων "έξυπνων" αεροδρομίων που χρειάζονται υψηλής τεχνολογίας λογισμικά για να αποκρούσουν τις εξελιγμένες απειλές. Η αύξηση των περιστατικών κυβερνοεπιθέσεων στο σύνθετο δίκτυο ψηφιακών συστημάτων που υποστηρίζουν τη λειτουργία τους και οι αλυσιδωτές πολυεπίπεδες επιδράσεις τους, δείχνουν την ανάγκη της αποτελεσματικής θωράκισής τους από τις απειλές του κυβερνοχώρου. Στόχος είναι η διαμόρφωση θεσμικών και

ρυθμιστικών πλαισίων, η παροχή καθοδήγησης και η λήψη μέτρων, ώστε τα αεροδρόμια, όπως και το σύνολο των κρίσιμων υποδομών, να αναπτύξουν ανθεκτικότητα απέναντι στις επιθέσεις, συνεχίζοντας απρόσκοπτα να παρέχουν στο κοινωνικό σύνολο τις ζωτικές τους υπηρεσίες.

Η παρούσα εργασία είναι διαρθρωμένη σε πέντε κεφάλαια, από τα οποία το πρώτο αναφέρεται σε γενικές γραμμές στις έννοιες της διοίκησης και της διαχείρισης επικινδυνότητας πληροφοριών, με σύντομη παρουσίαση των δημοφιλέστερων Προτύπων και Πλαισίων. Στο δεύτερο κεφάλαιο εξετάζεται η έννοια της κρίσιμης υποδομής, οι ιδιομορφίες και το πλαίσιο προστασίας της, σε συνάρτηση με τη διαχείριση επικινδυνότητας. Τα δύο επόμενα κεφάλαια εστιάζουν στον αεροπορικό τομέα. Στο τρίτο κεφάλαιο παρουσιάζονται τα ειδικά χαρακτηριστικά των αεροδρομίων ως κρίσιμων υποδομών, ενώ στο τέταρτο αναπτύσσεται το ζήτημα της Κυβερνοασφάλειας των αεροδρομίων. Τα συμπεράσματα που συνάγονται από την παραπάνω ανάλυση, εκτίθενται στο πέμπτο κεφάλαιο της εργασίας.

ΚΕΦΑΛΑΙΟ 1 : ΔΙΟΙΚΗΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

1.1. Η Διοίκηση ασφάλειας πληροφοριών

1.1.1. Σημασία και Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ)

Η πληροφορία αποτελεί περιουσιακό αγαθό του οργανισμού, ο οποίος για την επίτευξη των στόχων του συλλέγει, επεξεργάζεται και αποθηκεύει πληροφορίες, μέσω των πληροφοριακών του συστημάτων. Η ασφάλεια των πληροφοριών, συνάπτεται με την ασφάλεια των συστημάτων, που δεν αξιολογούνται μεμονωμένα ως τεχνολογικά αγαθά, αλλά ως στοιχεία της οργανωσιακής δομής του συγκεκριμένου οργανισμού. Η αντιμετώπιση των ζητημάτων ασφάλειας, δεν συνδέεται επομένως μόνο με την εφαρμογή της τεχνολογίας, αλλά ανάγεται ευρύτερα στο επίπεδο της διοίκησης και της ανάπτυξης της στρατηγικής του οργανισμού για την προστασία της πληροφορίας. Η προστασία των πληροφοριών ώστε να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητά τους, περιλαμβάνει τη συγκρότηση πολιτικών και τη πρόβλεψη μηχανισμών για την εφαρμογή τους και δεν αποτελεί ένα τεχνικής φύσης ζήτημα. Οι παραπάνω διεργασίες, στο σύγχρονο επιχειρηματικό περιβάλλον αποδίδονται με τους όρους διακυβέρνηση και διοίκηση της ασφάλειας των πληροφοριών.

Η διακυβέρνηση ασφάλειας πληροφοριών αναφέρεται στην πρόβλεψη ενός πλαισίου (framework), που περιλαμβάνει τις στρατηγικές μέσω των οποίων ο οργανισμός διαχειρίζεται τους κινδύνους στον τομέα των πληροφοριών, καθώς και τις οργανωτικές δομές που θα αναλάβουν την επίτευξη των στόχων στο πεδίο της ασφάλειας. Οι στρατηγικές αυτές, διαμορφώνονται σύμφωνα με τα ισχύοντα κανονιστικά και ρυθμιστικά πλαίσια και υλοποιούνται μέσω διαδικασιών, που αποτελούν αντίστοιχα το αντικείμενο της διοίκησης στον τομέα της

ασφάλειας πληροφοριών. Η διοίκηση ειδικότερα αφορά στο σχεδιασμό και την εφαρμογή ενός αποτελεσματικού συστήματος διαχείρισης της ασφάλειας πληροφοριών (ΣΔΑΠ /ISMS), το οποίο δεν παραμένει στατικό, αλλά συνεχώς συντηρείται και βελτιώνεται.[1] Περαιτέρω σκοπός του οργανισμού που εφαρμόζει ένα ΣΔΑΠ, είναι η συμμόρφωση με τις υφιστάμενες ρυθμιστικές και κανονιστικές απαιτήσεις, καθώς και τις απαιτήσεις προτύπων και πλαισίων ασφάλειας πληροφοριών, ώστε να εξασφαλίσει τις αντίστοιχες πιστοποιήσεις, που συμβάλλουν στην αξιοπιστία του.

Το ΣΔΑΠ πρέπει να εναρμονίζεται με τους προσδιορισμένους στόχους του οργανισμού, να διασφαλίζει την επιχειρησιακή συνέχεια και να ικανοποιεί τις απαιτήσεις ασφαλείας που έχουν τεθεί, με βάση διαδικασίες ανάλυσης και διαχείρισης κινδύνου. Ουσιώδες στοιχείο επιτυχίας του, είναι η υποστήριξή του από τον ανθρώπινο παράγοντα του οργανισμού, δηλαδή μιας διοίκησης που δεσμεύεται στην υλοποίησή του, παρέχοντας υλικούς και ανθρώπινους πόρους, καθώς και ενός καταρτισμένου και ικανού προσωπικού. Η εφαρμογή του, αποτελεί ευθύνη της διοίκησης, που θέτει τις κατευθύνσεις και καθορίζει δεσμευτικές διαδικασίες για το προσωπικό που το υλοποιεί (top down approach). Αν η διοίκηση δεν υποστηρίξει την ανάπτυξη του ΣΔΑΠ, εντάσσοντάς το στην οργανωσιακή δομή του οργανισμού, η εφαρμογή του συναντά εμπόδια που δεν είναι εύκολο να ξεπεραστούν. Αναγκαία τέλος είναι η πρόβλεψη ενός σταδίου επανεκτίμησης και ελέγχου, ώστε να προσαρμόζεται συνεχώς προς τη βέλτιστη κατεύθυνση. Το ΣΔΑΠ ενσωματώνει έτσι τρεις οπτικές, μέσω των οποίων προσεγγίζονται οι στόχοι του.

- Η οπτική της διακυβέρνησης, αναφέρεται στο ρόλο της διοίκησης του οργανισμού και εκφράζεται με τις στρατηγικές και τη στοχοθεσία, τις πολιτικές, τη κατανομή αρμοδιοτήτων και τον καθορισμό των οργανωσιακών δομών.
- Η οπτική της διακινδύνευσης, αναφέρεται στις αποφάσεις για την ιεράρχηση του κινδύνου και αποτελεί τη βάση για την οργάνωση της διαδικασίας της διαχείρισης επικινδυνότητας (risk management).
- Η οπτική της συμμόρφωσης, αναφέρεται στον καθορισμό των απαιτήσεων, εξωτερικών και εσωτερικών και τη διαδικασία ικανοποίησής τους, καθώς και των μηχανισμών παρακολούθησης και ελέγχου.[2]

1.1.2. Το Πρότυπο ISO/IEC 27001

Από το 2000 που εγκρίθηκε το αρχικό Πρότυπο της σειράς ISO27000 σχετικά με την ανάπτυξη ενός ΣΔΑΠ από τον Διεθνή Οργανισμό Προτυποποίησης (ISO) σε συνεργασία με την Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC), το Πρότυπο ISO/IEC 27001, με μια διαρκή διαδικασία

[1]Κοκολάκης Σ. "Διακυβέρνηση και Διοίκηση Ασφάλειας Πληροφοριών" σε Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, 2021 σελ. 50 επ.

[2] ISACA Implementation Guide ISO/IEC 27001:2022 Practical guide for the implementation of an information security management system (ISMS) according to ISO/IEC 27001:2022 ISACA Germany σελ.7 επ. https://isaca.de/publikationen/publikationen/leitfaeden/implementierungsleitfaden-iso-iec-27001-2022.html

επικαιροποίησής του, μέχρι την τελευταία εκδοχή του 2022[3], κυριαρχεί στο χώρο των προτύπων που επιλέγουν οι οργανισμοί και οι επιχειρήσεις για εφαρμογή ενός ΣΔΑΠ. Το ISO του 2022, που θα αντικαταστήσει πλήρως την προηγούμενη εκδοχή του 2013, το 2025, όπως φαίνεται και από τον τίτλο του, που διαφοροποιήθηκε σε σχέση με το ISO του 2013, δίνει έμφαση στη κυβερνοασφάλεια και στη διαφύλαξη της ιδιωτικότητας των δεδομένων. Χωρίς να καταργεί κάποια διεργασία, απλουστεύει τους ελέγχους, ομαδοποιώντας τους. Πρόκειται για το δημοφιλέστερο Πρότυπο που καθορίζει τις απαιτήσεις για τη θέσπιση, υλοποίηση, συντήρηση και συνεχή βελτίωση του ΣΔΑΠ στο πλαίσιο ενός οργανισμού, ενώ παράλληλα θέτει απαιτήσεις για την εκτίμηση και τη διαχείριση του κινδύνου. Απευθύνεται σε όλους ανεξαιρέτως τους οργανισμούς, ανεξάρτητα από το αντικείμενο και το μέγεθός τους. Εάν επιθυμεί ο οργανισμός, οδηγεί στη πιστοποίηση του για συμμόρφωση με τις απαιτήσεις που προβλέπει. Μια σειρά άλλων προτύπων της σειράς, παρέχει κατευθύνσεις για την υποβοήθηση εφαρμογής του ΣΔΑΠ σε ειδικότερα πεδία. [4]

Το ISO/IEC 27001:2022, στις δέκα "προτάσεις"του (clauses), περιγράφει τον κύκλο ζωής ενός ΣΔΑΠ, αναλύοντας επτά ενότητες απαιτήσεων που αφορούν:

- Στο γενικό πλαίσιο του οργανισμού (context of organisation)→ κατανόηση του οργανισμού και του πλαισίου του, των αναγκών και των προσδοκιών των ενδιαφερομένων μερών, καθορισμός των ορίων του ΣΔΑΠ και κατάρτισή του(ενότητα 4)
- Στην ηγεσία (leadership)→ ηγεσία και δέσμευση, πολιτική, οργανωσιακοί ρόλοι, αρμοδιότητες και καθήκοντα (ενότητα 5)
- Στον σχεδιασμό (planning)→ δράσεις για αντιμετώπιση κινδύνων και αξιοποίηση ευκαιριών, στόχοι της ασφάλειας πληροφοριών και σχεδιασμός για την επίτευξή τους, σχεδιασμός αλλαγών (ενότητα 6)
- Στην υποστήριξη (support)→ πόροι, ικανότητες, επίγνωση, επικοινωνία και τεκμηρίωση (ενότητα 7)
- Στη λειτουργία (operation)→λειτουργικός σχεδιασμός και έλεγχος, αποτίμηση επικινδυνότητας ασφάλειας πληροφοριών , διαχείριση επικινδυνότητας (ενότητα 8)
- Στην αξιολόγηση επίδοσης (Performance evaluation)→ παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση, εσωτερικός έλεγχος και επισκόπηση ενεργειών διοίκησης (ενότητα 9)
- Στη βελτίωση (Improvement) → Συνεχής βελτίωση, μη συμμόρφωση και διορθωτικές ενέργειες (ενότητα 10)

Οι παραπάνω ενότητες και υποενότητες, καθορίζουν τις διεργασίες για καθεμία απαίτηση ασφαλείας, διαμορφώνοντας μια διεργασιοκεντρική προσέγγιση στη διαχείριση της ασφάλειας πληροφοριών (process-based approach). Δομικό στοιχείο της, είναι η διενέργεια ελέγχων και η συνεχής βελτίωση των διεργασιών, με τη χρήση κάποιας μεθόδου που θα επιλέξει ο οργανισμός, προσαρμοσμένη στις απαιτήσεις που θέτει το Πρότυπο, όπως η μέθοδος PDCA

[3] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection-Information security management systems,Requirements https://www.iso.org/standard/27001

[4] Κάτσικας Σ. Διαχείριση της ασφάλειας πληροφοριών, 2014 σελ.61 επ.

(Plan-Do-Check-Act) ή η μέθοδος DMAIC (Define-Measure-Analyze-Improve-Control). Η μέθοδος PDCA (Deming wheel), προβλέπει τέσσερις κυκλικά επαναλαμβανόμενες φάσεις: σχεδιασμού, υλοποίησης, ελέγχου και διόρθωσης, οι οποίες εμπεριέχουν τις διεργασίες αντίστοιχων ενοτήτων απαιτήσεων του ISO 27001 ως εξής:

- Σχεδιασμός → Απαιτήσεις ενοτήτων 4,5,6
- Υλοποίηση → Απαιτήσεις ενοτήτων 7,8
- Έλεγχος → Απαιτήσεις ενότητας 9
- Διόρθωση → Απαιτήσεις ενότητας 10

Στο Παράρτημα Α΄ (Annex A) του Προτύπου, παρατίθενται τα αντίμετρα, τα οποία στη νέα εκδοχή του 2022, αντί για τη ταξινόμηση σε 14 κατηγορίες με 114 ελέγχους του ISO 2013, οργανώνονται στις παρακάτω τέσσερις κατηγορίες που περιλαμβάνουν 93 επιμέρους ελέγχους:

- Οργανωτικά αντίμετρα, που αντιστοιχούν σε 37 ελέγχους
- Αντίμετρα για τον ανθρώπινο παράγοντα που αντιστοιχούν σε 8 ελέγχους
- Φυσικά που αντιστοιχούν σε 14 ελέγχους
- Τεχνολογικά που αντιστοιχούν σε 34 ελέγχους

Παράλληλα, το 2022 αναθεωρήθηκε και το υποστηρικτικό πρότυπο ISO/IEC 27002, το οποίο αποτελεί αναπόσπαστο κομμάτι του ISO27001, παρέχοντας τις κατευθυντήριες γραμμές για την υλοποίηση των ελέγχων ασφαλείας του ISO27001.[5] Ενώ το ISO27001 εξειδικεύει τις απαιτήσεις προκειμένου να θεσπιστεί ένα ΣΔΑΠ, το ISO27002 εξειδικεύει τις πρακτικές και τον τρόπο υλοποίησης των ελέγχων που θα εφαρμοστούν μέσω του ΣΔΑΠ. Αν και ο αριθμός των ελέγχων που προβλέπονται μειώθηκε, στη πράξη πρόκειται για συγχώνευση διαδικασιών, αφού προστέθηκαν 11 νέοι έλεγχοι, κυρίως στη κατηγορία των τεχνολογικών αντιμέτρων (όπως Data masking, Data leakage prevention, Web filtering, Secure coding), ενώ έχει προστεθεί έλεγχος σχετικά με την ασφάλεια των υπηρεσιών Cloud. Μια νέα ταξινόμηση των ελέγχων ασφαλείας στην αναθεωρημένη έκδοση του ISO 27002, αποτελεί η απόδοση πέντε τύπων χαρακτηριστικών (attributes) σε κάθε έλεγχο, μέσω αντίστοιχων hashtags, ώστε να είναι άμεσα αντιληπτό, ποιές λειτουργίες επιτελεί κάθε αντίμετρο, στο πλαίσιο του ΣΔΑΠ. Τα χαρακτηριστικά αυτά είναι:

- Ο τύπος του ελέγχου (control types) → αποτρεπτικός, ανιχνευτικός, διορθωτικός

- Οι ιδιότητες για την ασφάλεια της πληροφορίας (information security properties) → εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα

- Η λειτουργία κυβερνοασφάλειας (cybersecurity concepts) → ταυτοποίηση, προστασία, ανίχνευση, αντίδραση, ανάκτηση)

[5] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls https://www.iso.org/standard/75652.html

- Οι λειτουργικές ικανότητες (operational capabilities)→διακυβέρνηση, διοίκηση αγαθών,ασφάλεια πληροφοριών, φυσική ασφάλεια, διοίκηση απειλών και ευπαθειών κ.ά.

- Ο τομέας ασφάλειας (security domains)→ Διακυβέρνηση και οικοσύστημα, προστασία, ανθεκτικότητα

Με την απόδοση των χαρακτηριστικών αυτών σε κάθε αντίμετρο, εισάγεται μια νέα αντίληψη στη διεργασία των ελέγχων, αφού διευκολύνεται η κατηγοριοποίηση των απαιτήσεων σε σχέση με τα αντίμετρα και δίνεται η δυνατότητα προσαρμογής ανάλογα με το χαρακτηριστικό στο οποίο εστιάζει ο κάθε οργανισμός. Η ομαδοποίηση των αντίμετρων κατά τομείς και χαρακτηριστικά, διευκολύνει τον οργανισμό ώστε να ελέγξει την συμμόρφωσή του με απαιτήσεις που θέτουν διαφορετικά πλαίσια και γενικότερα τη συμφωνία του ΣΔΑΠ που έχει υιοθετήσει, με άλλα Πρότυπα. Η δυνατότητα αυτή είναι σημαντική σε ένα διεθνοποιημένο επιχειρηματικό περιβάλλον. Ενδεικτικό παράδειγμα αποτελεί το χαρακτηριστικό "cybersecurity concepts" του ISO27001, το οποίο είναι όμοιο και στο Πλαίσιο NIST για την κυβερνοασφάλεια. [6]

1.1.3. Το Πλαίσιο ISACA COBIT (A Business Framework for the Governance and Management of Enterprise IT)

Η υιοθέτηση ενός ΣΔΑΠ, δεν γίνεται ανεξάρτητα από τα υπάρχοντα συστήματα διοίκησης, με τις απαιτήσεις των οποίων πρέπει να υπάρχει σύγκλιση. Η συμμόρφωση με ένα Πρότυπο, δεν πρέπει να αντιμετωπίζεται σαν μια αποσπασματική διαδικασία, αλλά να εντάσσεται στο συνολικό σύστημα διοίκησης του οργανισμού. Υπάρχει ένα δεύτερο επίπεδο λειτουργίας των προτύπων, στο οποίο σημαντική είναι η συνέργεια κατά τομείς και θεματικές, με βάση ένα οργανωτικό μοντέλο που συντονίζει κεντρικά τα συστήματα διοίκησης του οργανισμού. Ένα τέτοιο μοντέλο αποτελεί το Πλαίσιο COBIT του διεθνούς οργανισμού ISACA.

Το COBIT είναι ένα πλαίσιο για τη διακυβέρνηση της Τεχνολογίας της Πληροφορίας (IT), που εστιάζει στην εναρμόνιση με τους γενικότερους στόχους του οργανισμού και την καλύτερη δυνατή αξιοποίηση των επενδύσεων στον τομέα της πληροφορικής, ώστε να προσδώσουν αξία στον οργανισμό. Καθορίζει τις αρχές που διέπουν τις απαιτήσεις ενός συστήματος διακυβέρνησης για το IT του οργανισμού και λειτουργεί συνδυαστικά με τις αρχές ενός πλαισίου διακυβέρνησης. Την παλαιότερη εκδοχή του COBIT 5, έχει πλέον αντικαταστήσει η νέα έκδοση του COBIT 2019[7], που είναι ενημερωμένη με τις τεχνολογικές εξελίξεις. Ειδικότερα στη νέα έκδοση, έχουν επαναπροσδιορισθεί οι αρχές για τη διακυβέρνηση και τις διεργασίες ελέγχων, καθώς και οι παράγοντες που επηρεάζουν τον σχεδιασμό του συστήματος διακυβέρνησης IT.

---

[6] ISACA Implementation Guide ISO/IEC 27001:2022 Practical guide σελ.57 επ.
[7] Πλαίσιο ISACA COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY
https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

Ειδικότερα οι αρχές του συστήματος διακυβέρνησης είναι:

- Η δημιουργία αξίας για τα ενδιαφερόμενα μέρη από τη χρήση IT(stakeholder value)
- Η ολιστική προσέγγιση
- Το δυναμικό σύστημα διακυβέρνησης (συνεχής επανεκτίμηση και αλλαγή των παραγόντων σχεδιασμού)
- Η διάκριση μεταξύ διακυβέρνησης και διοίκησης (διακριτές δομές και δραστηριότητες)
- Η προσαρμογή στις ανάγκες του οργανισμού
- Η καθολική κάλυψη κάθε δραστηριότητας του οργανισμού σε σχέση με την τεχνολογία της πληροφορίας (end-to-end governance system)

Το πλαίσιο διακυβέρνησης πρέπει: ➢ Να βασίζεται σε ένα εννοιολογικό μοντέλο

➢Να είναι δεκτικό σε αλλαγές και ευέλικτο

➢Να εναρμονίζεται με κανονισμούς/ πρότυπα /πλαίσια

Τα αντικείμενα της διακυβέρνησης του IT, ομαδοποιούνται σε τομείς (domains). Ο τομέας της διακυβέρνησης θέτει, υλοποιεί και παρακολουθεί τους στρατηγικούς στόχους (Evaluate, Direct and Monitor-EDM). Τα αντικείμενα της διοίκησης IT, κατανέμονται σε τέσσερις τομείς που σχετίζονται με τον σχεδιασμό και την οργάνωση (Align, Plan and Organize- APO), την εγκατάσταση, απόκτηση και εφαρμογή (Build, Acquire and Implement - BAI), την υλοποίηση, την εξυπηρέτηση και την υποστήριξη (Deliver, Service and Support -DSS), και τον έλεγχο, την εκτίμηση και την αποτίμηση (Monitor, Evaluate and Assess -MEA). Για την ικανοποίηση των στόχων αυτών, ο οργανισμός θεσπίζει ένα σύστημα διακυβέρνησης που βασίζεται σε ένα αριθμό συντελεστών (components), όπως οι υποδομές, τα πλαίσια, οι διεργασίες και οι οργανωσιακές δομές, οι αρχές και οι πολιτικές, καθώς και το ανθρώπινο δυναμικό και η οργανωσιακή κουλτούρα του οργανισμού. Μεταξύ αυτών, σημαντική θέση έχουν οι πληροφορίες και ειδικότερα οι σχετικές με τη διακυβέρνηση του οργανισμού, στις οποίες εστιάζει το COBIT.[8] Το πλαίσιο καθορίζει επίσης λεπτομερώς τους παράγοντες που επηρεάζουν τον σχεδιασμό ενός συστήματος διακυβέρνησης, με κυριότερους τη στρατηγική και τους στόχους του οργανισμού, το προφίλ επικινδυνότητας (IT Risk) που έχει σε συνάρτηση με τις απειλές που αντιμετωπίζει και τα ειδικότερα προβλήματα στον τομέα του IT.

Σημαντικός είναι ο ρόλος που έχει η τεχνολογία της πληροφορίας για τον οργανισμό, το μοντέλο που ακολουθείται (outsourcing, cloud, hybrid) καθώς και το επίπεδο των απαιτήσεων συμμόρφωσης (χαμηλό, μέτριο, υψηλό). Τα αντικείμενα και οι συντελεστές τους, συνθέτουν ευρύτερες περιοχές ενδιαφέροντος (focus areas), που σχηματίζονται δυναμικά κατά την εφαρμογή του πλαισίου, όπως είναι η περιοχή της ασφάλειας πληροφοριών, για την οποία

[8] COBIT 2019 and COBIT 5 Comparison, Harisaiprasad K.,27 April 2020
www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

υπάρχει ξεχωριστή έκδοση. Εξειδικεύονται σε αυτή οι αρχές της ασφάλειας πληροφοριών από την οπτική της διακυβέρνησης και της διοίκησης και χωρίζονται σε αυτές που σχετίζονται με την υποστήριξη του οργανισμού, την άμυνα και την ανάπτυξη υπεύθυνης συμπεριφοράς διαχείρισης των πληροφοριών. Καθορίζονται οι στόχοι των πολιτικών που πρέπει να αναπτυχθούν και παρέχεται εξειδικευμένη καθοδήγηση για τη λειτουργία των παραπάνω τομέων που θέτει το βασικό Πλαίσιο. [9]

Το Πλαίσιο COBIT λειτουργεί σαν ένα πλαίσιο - ομπρέλλα, που μπορεί να ευθυγραμμίζεται με μια σειρά σχετικών κανονισμών, πλαισίων και προτύπων, ώστε να είναι δυνατή η συνδυαστική εφαρμογή του με αυτά. Συγκεκριμένα εναρμονίζεται με τα κυριότερα Πρότυπα της σειράς ISO 27000, όπως το 27001, καθώς και με τα πλαίσια NIST για τη διαχείριση επικινδυνότητας, την ασφάλεια πληροφοριακών συστημάτων και την κυβερνοασφάλεια των κρίσιμων υποδομών (Πλαίσια 800-37,800-53, Critical Infrastructure Cybersecurity). Η τάση των Προτύπων, όπως το ISO 27001, να εστιάζουν πλέον σε τομείς διεργασιών, διαδικασιών και ελέγχων, μπορεί να διευκολύνει τη συνύπαρξή τους με Πλαίσια όπως το COBIT, ώστε να μην αντιμετωπίζεται το ζήτημα της ασφάλειας πληροφοριών σε ένα αυστηρά τεχνικό πλαίσιο , αλλά να εντάσσεται σε μια ολιστική προσέγγιση αποτελεσματικής διακυβέρνησης και διοίκησης.[10]

1.2. Διαχείριση επικινδυνότητας

1.2.1. Σημασία και στόχοι

Η ιδέα της συστηματικής αντιμετώπισης της επικινδυνότητας και η διαμόρφωση τεχνικών αποφυγής και διαχείρισης του κινδύνου, αποτελεί γνώρισμα της μεταβιομηχανικής κοινωνίας της διακινδύνευσης (risk society) και είναι αποτέλεσμα των κινδύνων που δημιουργεί η ραγδαία τεχνολογική ανάπτυξη. Η διασφάλιση της πληροφορίας ως επιχειρηματικού αγαθού με την εγκατάσταση ενός ΣΔΑΠ, είναι αντικείμενο του γενικότερου τομέα της διαχείρισης της διακινδύνευσης (risk management), που έχει ενσωματωθεί στην επιστήμη της διοίκησης οργανισμών και επιχειρήσεων. Κύριος άξονας επομένως του ΣΔΑΠ, είναι η διαχείριση επικινδυνότητας. Παράλληλα εξυπηρετούνται σκοποί όπως η συμμόρφωση με νομικές απαιτήσεις, η επιχειρησιακή συνέχεια, καθώς και η συμμόρφωση με απαιτήσεις προτύπων, ώστε να επιτύχει ο οργανισμός την πιστοποίησή του.

Η διαχείριση επικινδυνότητας πρέπει να ενσωματωθεί στον κύκλο ζωής των συστημάτων, ως επιστημονική μεθοδολογία. Προκειμένου να γίνει δυνατή η αντιμετώπιση του κινδύνου, είναι αναγκαίο να καθοριστεί η επικινδυνότητα ως μέγεθος. Η μεθοδολογία που έχει επικρατήσει είναι η αξιοποίηση της στατιστικής και των πιθανοτήτων (μέθοδος Bayes), ώστε να εκτιμηθεί η πιθανότητα ενός περιστατικού ασφαλείας. Τα πληροφοριακά συστήματα δέχονται επιθέσεις

[9] ISACA COBIT Focus Area: Information Security Using COBIT 2019, ISACA 2020 https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ku2gEAC
[10] ISACA Implementation Guide ISO/IEC 27001:2022 Practical guide σελ.43 επ

(attacks) από διαφορετικές πηγές, οι οποίες προξενούν ζημιές στον οργανισμό που τα χρησιμοποιεί. Η διακινδύνευση, προσδιορίζεται από τη πιθανότητα εμφάνισης ενός κινδύνου, σε συνάρτηση με το συνολικό κόστος των επιπτώσεων που συνεπάγεται η επέλευση του κινδύνου στον οργανισμό. Κάθε αγαθό, πρέπει συνακόλουθα να εκτιμηθεί από την οπτική της έκθεσής του στον κίνδυνο και να εντοπιστεί ο βαθμός ευπάθειάς του (vulnerability), σε κάθε δεδομένη απειλή (threat), προς την οποία είναι αυτό ευάλωτο. Η έκφραση των παραπάνω εννοιών σε μετρήσιμα μεγέθη, δεν αποτελεί μια απλή διαδικασία, καθώς απαιτεί τη συντονισμένη κινητοποίηση όλων των οργανωσιακών δομών του οργανισμού. Ειδικότερα η εμπλοκή του ανθρώπινου παράγοντα και η δυνατότητα αποτύπωσης της ανθρώπινης συμπεριφοράς με μετρήσιμους όρους, συναντά σημαντικές δυσχέρειες. Ωστόσο ο προσδιορισμός της διακινδύνευσης είναι σημαντικός, καθώς σε αυτόν βασίζεται η λήψη αποφάσεων για μείωση του κινδύνου σε αποδεκτό επίπεδο. Στις ευπάθειες των συστημάτων, αντιπαρατίθενται έλεγχοι (controls), αντίμετρα (countermeasures) και μέτρα ασφαλείας (safeguards), που λειτουργούν ως δικλείδες ασφαλείας για αποφυγή των απειλών.

Αφετηρία για τη διαχείριση της διακινδύνευσης αποτελεί η διεργασία της αποτίμησης της διακινδύνευσης (risk assessment), η οποία εξελίσσεται σε στάδια. Αρχικά απαιτείται η αναγνώριση των αγαθών, των απειλών, των ευπαθειών και των επιπτώσεών τους, ώστε να περιγραφούν οι συνθήκες εκδήλωσης ενός πιθανού κινδύνου (risk identification). Ακολουθεί η ανάλυση της επικινδυνότητας (risk analysis), ώστε να προσδιοριστεί η αιτία του κινδύνου και η πιθανότητα να συμβεί σε συνάρτηση με τη σοβαρότητα των συνεπειών που θα προκαλέσει. Η τελική αξιολόγηση της επικινδυνότητας (risk evaluation), δείχνει αν ο κίνδυνος είναι αποδεκτός ή πρέπει να αντιμετωπιστεί. Η συγκρότηση πολιτικών αντιμετώπισης και η λήψη μέτρων ,συνιστά το στάδιο της αντιμετώπισης της επικινδυνότητας (risk treatment), που σκοπεύει στη διατήρηση του κινδύνου στο όριο που έχει τεθεί σαν αποδεκτό (risk threshold), ώστε να απομείνει μόνο η επικινδυνότητα που μπορεί να αντιμετωπιστεί (residual risk). Το όριο αυτό, καθορίζει την διάθεση για ανάληψη του κινδύνου από την επιχείρηση (risk appetite). Πέρα από αυτό, δεν υπάρχει ανοχή του κινδύνου και είναι αναγκαία η διαχείριση της επικινδυνότητας, είτε με μέτρα αποφυγής και μείωσής του κινδύνου, είτε με τον διαμοιρασμό ή τη μεταβίβασή του σε τρίτους.

Παράλληλα με τις παραπάνω διαδικασίες, είναι σημαντικό να αναπτυχθούν μηχανισμοί διαβούλευσης μεταξύ των δικαιούχων του οργανισμού (communication of risk and consultation), αλλά και συνεχούς παρακολούθησης (monitoring). Έτσι το σύστημα ασφαλείας ελέγχεται σταθερά για την αποδοτικότητα του στη διαχείριση της διακινδύνευσης, ώστε σε περίπτωση αστοχιών του, να εκδηλώνονται ενέργειες αναθεώρησής του (review of risk).[11]

[11] David Sutton INFORMATION RISK MANAGEMENT A practitioner's guide, BCS Learning and Development Ltd 2021,σελ.29 επ.

1.2.2. Μεθοδολογίες, πλαίσια και πρότυπα διαχείρισης επικινδυνότητας

Η διαχείριση επικινδυνότητας στον τομέα της ασφάλειας πληροφοριών, συνιστά μια σύνθετη διεργασία που εμπλέκει την ανάπτυξη μεθοδολογιών, μεθόδων και εργαλείων, καθώς και εξειδικευμένο επιστημονικό προσωπικό, που θα τις εφαρμόσει με επιτυχία. Τα πλαίσια (frameworks) ορίζουν τις προδιαγραφές μιας δομής, που λειτουργεί ως υπόβαθρο για την ανάπτυξη του συνόλου των διαδικασιών που σχετίζονται με τη διαχείριση των κινδύνων ασφάλειας πληροφοριών. Από την άλλη, οι μεθοδολογίες παρέχουν συστηματική καθοδήγηση για τον τρόπο εκτέλεσης των παραπάνω διεργασιών αναγνώρισης, ανάλυσης και αποτίμησης της διακινδύνευσης. Τα πλαίσια παρέχουν μια γενικότερη προσέγγιση σε σχέση με τις μεθοδολογίες, καθώς λειτουργούν σαν υποδομή στην οποία μπορούν να ενταχθούν διαφορετικών ειδών διεργασίες, που εφαρμόζονται είτε αποκλειστικά, είτε συνδυαστικά. Ενώ στα πλαίσια δίνονται περισσότερες εναλλακτικές αντιμετώπισης της διακινδύνευσης, με την τροποποίηση, αποφυγή, διατήρηση ή διαμοιρασμό του κινδύνου, οι μεθοδολογίες στοχεύουν στην εξειδίκευση των δράσεων και κατά συνέπεια είναι λιγότερο ευέλικτες.[12]

Ανάλογα με το πλαίσιο και τη μεθοδολογία που θα υιοθετήσει ένας οργανισμός, επιλέγεται στη συνέχεια η μέθοδος που θα εφαρμοστεί για την ολοκλήρωση της διαδικασίας της διαχείρισης της διακινδύνευσης. Η επιλογή της κατάλληλης μεθόδου είναι δύσκολο εγχείρημα, για τον λόγο ότι κάθε μέθοδος εστιάζει σε διαφορετικές διεργασίες και χρησιμοποιεί διαφορετικές αναλύσεις. Σημαντικό κριτήριο επιλογής, είναι και η ελεύθερη διαθεσιμότητα της μεθόδου. Διαδεδομένες μέθοδοι είναι οι MAGERIT της Ισπανικής Κυβέρνησης, η σειρά μεθόδων OCTAVE του Software Engineering Institute USA , η EU ITSRM της Ε.Ε., η ETSI TS 102 165-1 (threat, vulnerability and risk analysis TVRA) του Technical Committee Cybersecurity, η γαλλική EBIOS.[13]

Τα πλαίσια και οι μεθοδολογίες περιλαμβάνουν προσεγγίσεις είτε με βάση είτε το αγαθό (asset based), είτε μια υποθετική εξέλιξη (event based- risk scenario). Η ανάλυση της επικινδυνότητας μπορεί να προσανατολίζεται στην απειλή, στην επίπτωση επί του αγαθού ή στην ευπάθεια (threat, asset/impact or vulnerability oriented). Αντίστοιχα, μπορεί να χρησιμοποιούν είτε ποσοτικά, είτε ποιοτικά κριτήρια, ή και ένα συνδυασμό των παραπάνω. Ο υπολογισμός του κινδύνου βασίζεται σε τύπους που χρησιμοποιούν συντελεστές όπως η πιθανότητα εμφάνισης περιστατικών ασφαλείας, η πιθανότητα απειλών, η επίπτωση για τον οργανισμό, η έκταση των ευπαθειών. Η αποτύπωση του κινδύνου μπορεί να είναι αριθμητική ή να εκφράζεται σε κατηγορίες και επίπεδα. Τα δεδομένα αυτά, αξιοποιεί η μέθοδος, μορφοποιώντας σε συγκεκριμένα βήματα και καθορισμένες δράσεις τα πλαίσια και τις μεθοδολογίες, με την υποστήριξη ενός λογισμικού που λειτουργεί ως ένα εύχρηστο εργαλείο για τους εμπλεκόμενους με την διαδικασία της ασφάλειας πληροφοριών.

[12] ENISA Compendium of Risk Management Frameworks with potential Interoperability 2022 σελ.6 επ.
[13] Σ.Κάτσικας ό.π. σελ.119

Τρωτό σημείο των πλαισίων, ως συστήματος αντιμετώπισης της διακινδύνευσης των πληροφοριών, είναι η απλουστευμένη μοντελοποίηση σύνθετων παραμέτρων και χαρακτηριστικών του περιβάλλοντος ενός οργανισμού. Η χρήση της στατιστικής και των μαθηματικών δημιουργεί την εντύπωση της αντικειμενικότητας και της τεκμηρίωσης των αποτελεσμάτων, όμως στην πραγματικότητα δεν υπάρχει ουσιαστική συνεκτίμηση των ιδιομορφιών κάθε επιχειρηματικού περιβάλλοντος. Παρόλα αυτά, οι κατευθύνσεις που προσφέρονται μέσα από τα πλαίσια, αποτελούν την ασφαλέστερη λύση για τη διακυβέρνηση της διακινδύνευσης, καθώς λαμβάνουν υπόψη κανονιστικά πλαίσια και νομοθετικές ρυθμίσεις, όπως ο Γενικός Κανονισμός Προσωπικών Δεδομένων στον ευρωπαϊκό χώρο, ενώ παράλληλα δεν έχουν δεσμευτικό χαρακτήρα. Αντίθετα, διαμορφώνουν μια βάση για την εκδήλωση ενεργειών στο ζήτημα της ασφάλειας, που γίνεται κατανοητή σε όλα τα επίπεδα της επιχειρησιακής δομής. Εναπόκειται στον κάθε οργανισμό να επιλέξει τη μεθοδολογία που τον εξυπηρετεί για την επίτευξη των στόχων του, αλλά και να συνδυάσει προβλέψεις διαφορετικών πλαισίων, με τον τρόπο που παράγει τα επιθυμητά για αυτόν αποτελέσματα. Η δημιουργία ευέλικτων εργαλείων για την εφαρμογή των μεθοδολογιών και η ανάπτυξη της διαλειτουργικότητας των πλαισίων, αποτελεί μία εναλλακτική πρόταση για τη σύγχρονη επιχειρηματικότητα.[14]

Τα πλαίσια και οι μεθοδολογίες έχουν εκδοθεί από διαφορετικούς φορείς, όπως ανεξάρτητοι ή κυβερνητικοί οργανισμοί, ιδιωτικές επιχειρήσεις και ακαδημαϊκοί παράγοντες. Τα κείμενα με την μεγαλύτερη επιδραστικότητα στον τομέα της ασφάλειας πληροφοριών, είναι τα πρότυπα και οι κατευθυντήριες γραμμές (standards and guidelines) που έχουν συνταχθεί από Οργανισμούς προτύπων, όπως τον Διεθνή Οργανισμό Τυποποίησης (ISO) και το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας του Υπουργείου Εμπορίου των Η.Π.Α. (NIST). Τα πλαίσια ISO/IEC 27005:2022 και NIST SP800-30, θεωρούνται τα κυρίαρχα στον τομέα της διακυβέρνησης και διοίκησης επικινδυνότητας πληροφοριών. Διαδεδομένο Πλαίσιο είναι επίσης το Risk IT του Οργανισμού ISACA, το οποίο λειτουργεί συμπληρωματικά στο Πλαίσιο για τη διοίκηση των πληροφοριακών συστημάτων COBIT. Για την εφαρμογή των πλαισίων αυτών, προσφέρεται πλήθος μεθόδων και εργαλείων, που αξιοποιούν τις προτεινόμενες από αυτά μεθοδολογίες, παρέχοντας στις σύγχρονες επιχειρήσεις και οργανισμούς ολοκληρωμένους τρόπους αντιμετώπισης της διακινδύνευσης στο χώρο των πληροφοριών και των πληροφοριακών συστημάτων.

[14] ENISA Interoperable EU Risk Management Framework 2022

1.2.3.Το Πρότυπο ISO/IEC 27005:2022

Το Πρότυπο ISO/IEC 27005[15], εξειδικεύει το γενικό πρότυπο καθοδήγησης στη διοίκηση επικινδυνότητας ISO/IEC 31000, για τον τομέα της ασφάλειας πληροφοριών. Σκοπός του είναι η παροχή καθοδήγησης στις απαιτήσεις που θέτει το πρότυπο της ίδιας σειράς 27001, σχέση που ενισχύθηκε στη νέα εκδοχή του 2022. Απευθύνεται σε οποιονδήποτε οργανισμό επιθυμεί να εγκαταστήσει ένα ΣΔΑΠ σύμφωνα με το ISO27001 ή γενικότερα να εφαρμόσει τις διαδικασίες της διοίκησης επικινδυνότητας στον τομέα της ασφάλειας πληροφοριών. Αναλύει τις διεργασίες της αποτίμησης και αντιμετώπισης της επικινδυνότητας, μέσα από μια επαναληπτική διαδικασία, προσδιορίζοντας δύο διακριτούς κύκλους, στο πλαίσιο των οποίων πραγματοποιούνται οι παραπάνω διεργασίες. Ο στρατηγικός κύκλος, αφορά μακροσκοπικές αλλαγές στο γενικότερο πλαίσιο του οργανισμού και γίνεται σε μεγαλύτερα χρονικά διαστήματα, ενώ ο λειτουργικός αφορά λεπτομερείς κινδύνους συγκεκριμένης αποτίμησης ή αντιμετώπισης επικινδυνότητας.

Το έναυσμα (trigger criteria), είναι ένα δομικό στοιχείο που εισάγει το Πρότυπο στη νέα του έκδοση, το οποίο οδηγεί στην έναρξη μιας δραστηριότητας, λόγω μιας αλλαγής ή αναθεώρησης κάποιου βήματος. Με επίκεντρο το έναυσμα, η αποτίμηση επικινδυνότητας γίνεται δυναμική και επίκαιρη. Τον ίδιο σκοπό εξυπηρετεί και η υιοθέτηση μιας προσέγγισης, βασισμένης σε σενάρια κινδύνου (risk scenarios), που ορίζονται σαν μια ακολουθία συμβάντων, τα οποία οδηγούν σε μία ανεπιθύμητη συνέπεια.

Η ροή των εργασιών ξεκινά από τον καθορισμό του γενικού πλαισίου, εσωτερικού και εξωτερικού. Η αποτίμηση της επικινδυνότητας στη συνέχεια, περιλαμβάνει τις δραστηριότητες της αναγνώρισης, της ανάλυσης και της αξιολόγησης της επικινδυνότητας και πραγματοποιείται μέσω δύο βασικών προσεγγίσεων αναγνώρισης κινδύνων. Η προσέγγιση που βασίζεται σε συμβάντα (event based approach) αναφέρεται σε στρατηγικά σενάρια, που λαμβάνουν υπόψη πηγές κινδύνου και τον τρόπο που επηρεάζουν τα ενδιαφερόμενα μέρη, εστιάζοντας στο συνολικό τοπίο των απειλών. Η προσέγγιση που βασίζεται στα αγαθά (asset based), αναφέρεται στη δημιουργία λειτουργικών σεναρίων για την αναγνώριση απειλών και ευπαθειών που σχετίζονται με συγκεκριμένα αγαθά.

Ακολουθούν οι δραστηριότητες αντιμετώπισης επικινδυνότητας, σύμφωνα με τα αποτελέσματα της αποτίμησης, με τη λήψη αντιμέτρων, ώστε να ικανοποιούνται τα κριτήρια αποδοχής επικινδυνότητας που έχουν τεθεί. Σημαντικές διαδικασίες που αφορούν σε όλα τα στάδια του Προτύπου, είναι η διαδικασία επικοινωνίας και διαβούλευσης μεταξύ των ενδιαφερομένων μερών και των ιδιοκτητών επικινδυνότητας (risk owners), καθώς και η διαδικασία

[15] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks

παρακολούθησης και αναθεώρησης, ώστε να εξασφαλίζεται η προσαρμογή στις αλλαγές και η αποτελεσματικότητα του ΣΔΑΠ.

1.2.4. Το Πρότυπο NIST SP 800-30

Το ευρύτερο Πλαίσιο της σειράς NIST SP 800 περιλαμβάνει Πρότυπα της Ομοσπονδιακής Κυβέρνησης των ΗΠΑ, με αντικείμενο τις πολιτικές, τις διαδικασίες και τις κατευθυντήριες γραμμές σχετικά με την ασφάλεια πληροφοριακών συστημάτων. Το Πρότυπο 800-30 παρέχει καθοδήγηση για διεξαγωγή της αποτίμησης επικινδυνότητας, σαν μέρος μιας ευρύτερης διαδικασίας διαχείρισης επικινδυνότητας (risk management) που αφορά όλες τις δραστηριότητες του οργανισμού. Λογω της ευελιξίας του, έχει εφαρμογή σε κάθε είδους οργανισμό, που μπορεί να το προσαρμόσει στις ιδιαίτερες ανάγκες του. Περιλαμβάνει τέσσερις κεντρικές διεργασίες:

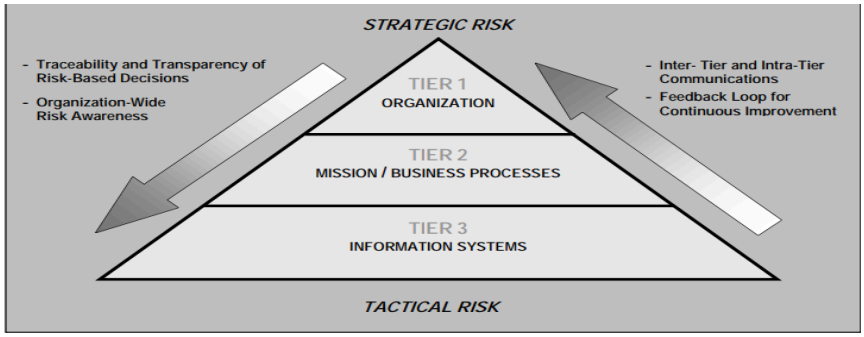
- Καθορισμός της επικινδυνότητας (framing risk)→ Αναφέρεται στη περιγραφή του γενικού πλαισίου και του περιβάλλοντος στο οποίο θα εξεταστεί η διακινδύνευση και θα σχεδιαστεί η στρατηγική διαχείρισής της.
- Αποτίμηση επικινδυνότητας (assessing risk)→ Περιλαμβάνει την αναγνώριση των απειλών και των ευπαθειών, της βλάβης για τον οργανισμό και της πιθανότητας να επέλθει, ώστε να προσδιοριστεί η επικινδυνότητα.
- Απόκριση στην επικινδυνότητα (responding to risk)→ Στοχεύει στην ανάπτυξη και εφαρμογή τρόπων δράσης σύμφωνα με τα αποτελέσματα της αποτίμησης επικινδυνότητας, οι οποίοι να συμπλέουν με το συνολικό οργανωσιακό πλαίσιο επικινδυνότητας του οργανισμού.
- Παρακολούθηση επικινδυνότητας (monitoring risk)→ Περιέχει τον έλεγχο της αποτελεσματικότητας των τρόπων απόκρισης, τον εντοπισμό αλλαγών στο λειτουργικό περιβάλλον των πληροφοριακών συστημάτων και την επίβλεψη της τήρησης του σχεδιασμού απόκρισης σε συνδυασμό με την συμμόρφωση στις απαιτήσεις.

  Το Πρότυπο δίνει βαρύτητα στην διεργασία της αποτίμησης επικινδυνότητας, προβλέποντας μία διαδικασία τεσσάρων βημάτων:

  - ➢ Βήμα 1: Προετοιμασία για την αποτίμηση σύμφωνα με το οργανωσιακό πλαίσιο επικινδυνότητας (prepare for risk assessment)
  - ➢ Βήμα 2: Διενέργεια αποτίμησης (conduct)
  - ➢ Βήμα 3:Επικοινωνία σχετικά με τα αποτελέσματα της αποτίμησης (communicate)
  - ➢ Βήμα 4:Επικαιροποίηση σε σταθερή βάση της διαδικασίας αποτίμησης (maintain)

Το NIST SP 800-30 περιγράφει τη μεθοδολογία και λειτουργεί υποστηρικτικά στη γενική καθοδήγηση που παρέχει το πρότυπο της ίδιας σειράς 800-39, για τη διαχείριση της επικινδυνότητας στην ασφάλεια πληροφοριών. Το τελευταίο πρότυπο, αποτελεί μια ευέλικτη σφαιρική προσέγγιση για τη διαχείριση της επικινδυνότητας από τη χρήση πληροφοριακών συστημάτων, που εκτείνεται σε όλο το το φάσμα των επιχειρησιακών διεργασιών του οργανισμού. Αναφέρεται στην αποτίμηση επικινδυνότητας και στα τρία επίπεδα (tiers) της

διαχείρισης επικινδυνότητας. Στο οργανωσιακό επίπεδο, κατά το οποίο τίθενται οι στρατηγικοί στόχοι και οι πολιτικές διαχείρισης επικινδυνότητας, στο επίπεδο των επιχειρησιακών διαδικασιών του οργανισμού και στο επίπεδο των πληροφοριακών συστημάτων και της ασφάλειάς τους. [16]



Σχήμα 1: Επίπεδα διαχείρισης επικινδυνότητας σε όλο το φάσμα του οργανισμού

Αν και σχεδιάστηκε αρχικά για οργανισμούς κρίσιμων υποδομών των ΗΠΑ, χρησιμοποιείται σε ευρεία κλίμακα από δημόσιους και ιδιωτικούς φορείς για την διαχείριση επικινδυνότητας πληροφοριών, αλλά και σαν ένα γενικής φύσης επιχειρησιακό πρόγραμμα διαχείρισης επικινδυνότητας (Enterprise Risk Management Programme ERM).[17]

Ένα άλλο Πρότυπο NIST, το 800-53, λειτουργεί συμπληρωματικά με τα παραπάνω αναφορικά με την συμμόρφωση στις απαιτήσεις ασφαλείας και τη προστασία προσωπικών δεδομένων, εστιάζοντας στους ελέγχους ασφάλειας που μπορούν να υλοποιηθούν για την προστασία των συστημάτων πληροφοριών. Περιλαμβάνει ελέγχους οργανωμένους σε 20 κατηγορίες (control families), καλύπτοντας ευρύ φάσμα απειλών και κινδύνων. Διαθέτει ευελιξία καθώς διαχωρίζει τους ελέγχους σε βασικούς (basic) και ενισχυμένους (enhanced), που ο οργανισμός επιλέγει επιπρόσθετα από τον αντίστοιχο βασικό, εάν κρίνει ότι ανταποκρίνονται στις ανάγκες του.[18]

1.2.4. Το Πλαίσιο ISACA The Risk IT Framework

Το Risk IT[19] αναπτύχθηκε για να εξειδικεύσει την γενική έννοια της διακινδύνευσης στον τομέα της Τεχνολογίας των πληροφοριών ενός οργανισμού. Αποτελεί μια συνέχεια της αντίληψης διακυβέρνησης που εκφράζει το Πρότυπο COBIT για μια ολιστική διαχείριση του κινδύνου σε όλα τα επίπεδα. Καλύπτει το κενό μεταξύ των παραδοσιακών γενικών πλαισίων διαχείρισης

[16] NIST SP 800-39 "Managing Information Security Risk: Organization, Mission, and Information System View" Date Published: March 2011 https://csrc.nist.gov/pubs/sp/800/39/final

[17] ENISA Compendium of Risk Management Frameworks with potential Interoperability 2022 ό.π. σελ.10

[18] NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[19] ISACA The Risk IT Framework 2nd edition 2020 https://www.isaca.org/resources/it-risk

επικινδυνότητας και ειδικών πλαισίων, όπως το ISO 27005 για την ασφάλεια πληροφοριών και το NIST Cybersecurity Framework για τις Κρίσιμες Υποδομές. Απευθύνεται σε κάθε είδους οργανισμό που στοχεύει στη διαχείριση της επικινδυνότητας στον τομέα της ηλεκτρονικής και ψηφιακής τεχνολογίας επικοινωνιών και πληροφορίας, εστιάζοντας στις ιδιομορφίες των κινδύνων που σχετίζονται με τον τομέα του IT και προκύπτουν από την ενσωμάτωση πληροφοριακών συστημάτων στην επιχειρησιακή πρακτική. Το Πρότυπο, στη νέα του έκδοση, θέτει τη διαχείριση της επικινδυνότητας του IT, σαν βασικό παράγοντα αντιμετώπισης των κινδύνων που σχετίζονται με τον κυβερνοχώρο (cyberrisk). Το πλαίσιο στη νέα του έκδοση του 2020, αφού ορίσει τις αρχές διαχείρισης επικινδυνότητας που αντιστοιχούν σε ανάλογες του COBIT, περιλαμβάνει τέσσερις τομείς με αντίστοιχες διεργασίες:

- Διακυβέρνηση επικινδυνότητας (Risk Governance)
- Διοίκηση επικινδυνότητας (Risk management)
- Αποτίμηση επικινδυνότητας (Risk assessment)
- Επίγνωση επικινδυνότητας, Αναφορά και Επικοινωνία (Risk Awareness, Reporting and Communication)

Οι κυριότερες υποδιεργασίες είναι ο καθορισμός περιεχομένου (Setting Context), η αναγνώριση κινδύνων και η αποτίμηση (Risk Identification and Assessment), Αναφορά και επικοινωνία (Risk Reporting and Communication), Ανάλυση επικινδυνότητας και εκτίμηση επιπτώσεων στην επιχείρηση (Risk Analysis and Business Impact Evaluation) Απόκριση (Risk Response). Το Risk IT είναι ένα ευέλικτο Πρότυπο, καθώς δεν είναι υποχρεωτική η τήρηση της προτεινόμενης σειράς εργασιών. Κάθε οργανισμός μπορεί να προσαρμόσει τη σειρά ανάλογα με τις ανάγκες του, ενώ παράλληλα δεν αποκλείει την ταυτόχρονη εφαρμογή άλλων πλαισίων όσον αφορά τα μέτρα ασφαλείας.[20]

1.2.5. Η διαλειτουργικότητα των πλαισίων κατά τον ENISA

Η χρήση από τους οργανισμούς σε διεθνές και εθνικό επίπεδο, διαφορετικών πλαισίων και μεθοδολογιών για τη διαχείριση της επικινδυνότητας στον τομέα της ασφάλειας πληροφοριών, δημιουργεί προβλήματα, όταν απαιτείται να ανταλλαγούν πληροφορίες, να μεταφερθούν δεδομένα και να συγκριθούν τα αποτελέσματά τους. Πρόκειται για το ζήτημα της διαλειτουργικότητας (interoperability) των Πλαισίων, το οποίο απασχόλησε τον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια ENISA σε τρεις σχετικές έρευνες που εξέδωσε από τον Ιανουάριο του 2022.

Στην πρώτη (Compendium of risk management frameworks with potential interoperability) αναλύονται τα κυριότερα πλαίσια και μεθοδολογίες που εμφανίζουν στοιχεία

[20] ENISA Compendium of Risk Management Frameworks with potential Interoperability 2022 σελ.15

διαλειτουργικότητας, στη δεύτερη (Interoperable eu risk management framework) προτείνεται μια μεθοδολογία αποτίμησης της δυνατότητας των Πλαισίων για διαλειτουργικότητα, μέσω των κοινών χαρακτηριστικών που εμφανίζουν, ενώ στη τρίτη (Interoperable EU Risk Management Toolbox) προτείνεται μια λύση για την ένταξη διαφορετικών μεθόδων στο περιβάλλον ενός οργανισμού και τη δημιουργία μιας κοινής βάσης κατανόησης της επικινδυνότητας.

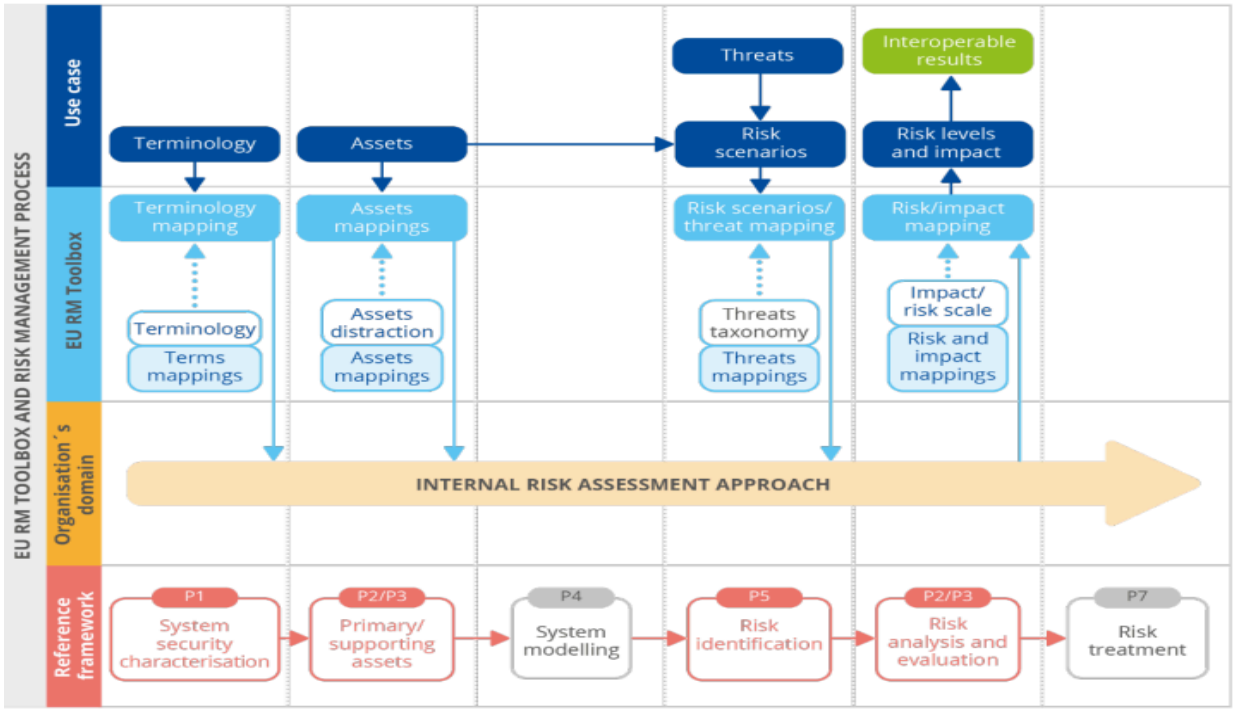
Η έρευνα του ENISA, θεωρώντας σαν στοιχειώδη συστατικά κάθε Πλαισίου διαχείρισης επικινδυνότητας, τις φάσεις της αναγνώρισης, αποτίμησης, αντιμετώπισης και παρακολούθησης της επικινδυνότητας, εστιάζει στις τρεις πρώτες, επιχειρώντας μέσα από την ανάλυση των λειτουργικών και μη λειτουργικών χαρακτηριστικών των Πλαισίων που εξετάζει, να τα κατατάξει σε μία κλίμακα διαλειτουργικότητας (υψηλή, μέση και χαμηλή).

Στα λειτουργικά χαρακτηριστικά που συμβάλλουν στην διαλειτουργικότητα, περιλαμβάνονται χαρακτηριστικά γενικής φύσης, όπως οι κοινές προσεγγίσεις των Πλαισίων με βάση τα αγαθά ή τα σενάρια και η υιοθέτηση της ίδιας ποσοτικής ή ποιοτικής μεθόδου. Ακολουθεί η χρήση κοινών μεθόδων αναγνώρισης επικινδυνότητας (ταξινόμηση και εκτίμηση αγαθών, κατάλογοι απειλών και ευπαθειών), αποτίμησης και υπολογισμού της επικινδυνότητας και τέλος η χρήση κοινών αντίμετρων για μείωση του επιπέδου επικινδυνότητας (κοινός κατάλογος αντίμετρων και κοινός τρόπος υπολογισμού της απομείνουσας επικινδυνότητας). Στα μη λειτουργικά κατατάσσονται η γλώσσα του Προτύπου, η συμμόρφωση με άλλα πρότυπα, το κόστος άδειας χρήσης.

Στη τελευταία έρευνα του ο ENISA, λαμβάνοντας υπόψη τα ευρήματα των προηγούμενων ερευνών σχετικά με τη διαλειτουργικότητα, προτείνει μια εργαλειοθήκη (toolbox), με στόχο την παροχή στα ενδιαφερόμενα μέρη ενός πλαισίου αναφοράς για τη κατανόηση των αποτελεσμάτων της διαχείρισης επικινδυνότητας, ανεξαρτήτως του πλαισίου βάσει του οποίου πραγματοποιήθηκε η αποτίμηση και της μεθόδου με την οποία αυτά προέκυψαν. [21] Η μέθοδος που χρησιμοποιείται για την εφαρμογή της εργαλειοθήκης, βασίζεται στο Πρότυπο ISO 27005 και στη μεθοδολογία ITSRM2, που επιλέχθηκαν λόγω του υψηλού βαθμού διαλειτουργικότητάς τους. Ωστόσο δεν επεμβαίνει στις επιλογές των οργανισμών για χρήση συγκεκριμένων Προτύπων και μεθόδων, αλλά επιχειρεί να τους διευκολύνει στη κατανόηση και σύγκριση των αποτελεσμάτων διαφορετικών μεθόδων που ακολουθούν άλλοι οργανισμοί, ειδικότερα στον τομέα των απειλών και των σεναρίων κινδύνου.

[21] ENISA Interoperable EU Risk Management Toolbox 2023
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox

Figure 1: The role of the EU RM toolbox and its positioning in the RM process



Σχήμα 2: Ο ρόλος της εργαλειοθήκης EU RM Toolbox στη διαδικασία διαχείρισης επικινδυνότητας

Το σχήμα αποτυπώνει τη θέση του εργαλείου EU RM Toolbox σε σχέση με τα σενάρια κινδύνου και τα αντίστοιχα εργαλεία που χρησιμοποιούν οι οργανισμοί στο περιβάλλον τους. Το εργαλείο λειτουργεί σε ένα ενδιάμεσο επίπεδο μεταξύ των σεναρίων κινδύνου που χρησιμοποιεί ένας οργανισμός για την αποτίμηση επικινδυνότητας και της μεθοδολογίας που έχει υιοθετήσει ο οργανισμός. Το εργαλείο χρησιμοποιείται σαν Πλαίσιο αναφοράς για τις διεργασίες της αποτίμησης επικινδυνότητας και διευκολύνει την εναρμόνισή τους ως προς τέσσερις βασικές λειτουργίες:

• Καθιέρωση μιας κοινής κατανόησης των δραστηριοτήτων που πραγματοποιούνται για τη διαδικασία της διαχείρισης επικινδυνότητας

• Ορισμός του πεδίου εφαρμογής του περιβάλλοντος στο οποίο θα εφαρμοστεί η διαδικασία αποτίμησης

• Αναγνώριση σεναρίων κινδύνου που σχετίζονται με μια συγκεκριμένη απειλή ή ομάδας απειλών που διερευνώνται.

• Σύνδεση των επιπέδων κινδύνου που υπολογίζονται με διάφορες μεθόδους, με αυτά που καθορίζονται από μια κοινή κλίμακα αξιολόγησης της επικινδυνότητας.

ΚΕΦΑΛΑΙΟ 2 : ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΙΣ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

2.1. ΄Εννοια και προσδιορισμός των Κρίσιμων Υποδομών

2.1.1. Κριτήρια προσδιορισμού ΚΥ και η έννοια της κρίσιμης οντότητας

Κρίσιμες υποδομές (Κ.Υ.) (Critical Infrastructures C.I.) καλούνται οι πραγματικές εγκαταστάσεις, οι τεχνολογίες πληροφοριών, τα δίκτυα και οι υπηρεσίες, που η καταστροφή τους ή η διακοπή λειτουργίας τους μπορεί να έχει σοβαρές επιπτώσεις σε ζωτικές λειτουργίες, που σχετίζονται με την υγεία, την ασφάλεια ή την οικονομική και κοινωνική ευημερία των πολιτών. Η υγεία, η ενέργεια, οι μεταφορές, το χρηματοοικονομικό σύστημα αποτελούν χαρακτηριστικά παραδείγματα κρίσιμων υποδομών. Η εξάρτηση της σύγχρονης κοινωνίας από τις κρίσιμες υποδομές συνεχώς αυξάνεται, ενώ παράλληλα οι νέες τεχνολογίες που ενσωματώνονται στα πληροφοριακά συστήματα που τις υποστηρίζουν, διαμορφώνουν ένα νέο τοπίο απειλών, στο οποίο κυριαρχούν οι κίνδυνοι του κυβερνοχώρου. Η διατήρηση επομένως του λειτουργικού επιπέδου των κρίσιμων υποδομών, συνδέεται πλέον αναπόσπαστα με την ασφάλεια των πληροφοριακών συστημάτων που ελέγχουν τις εγκαταστάσεις και το φυσικό περιβάλλον τους. Στη νέα αυτή πραγματικότητα, ο τομέας της κυβερνοασφάλειας βρίσκεται στο επίκεντρο της αντιμετώπισης των κινδύνων.

Τα υποστηρικτικά αυτά συστήματα (Critical Information Infrastructures- CIIs), συνιστούν τους πυλώνες της οικονομίας και της κοινωνικής ζωής, τυχόν δε προσβολή τους, μπορεί να επιφέρει αλυσιδωτές επιδράσεις σε μεγάλο μέρος του πληθυσμού. ΄Αλλωστε, πέρα από τη περίπτωση που τα πληροφοριακά συστήματα αποτελούν την προϋπόθεση για τη λειτουργία μιας φυσικής κρίσιμης υποδομής, μπορεί τα ίδια να συνιστούν μια κρίσιμη υποδομή που παρέχει πληροφορίες ή ηλεκτρονικές υπηρεσίες.

Η σύνθετη υπόσταση των ΚΥ, ως αλληλένδετων φυσικών και ψηφιακών πεδίων, διαμορφώνει διαφορετικούς όρους διαχείρισης για τους ιδιοκτήτες/διαχειριστές τους (owners/operators). Το βάρος μετατοπίζεται πλέον από την προστασία των στοιχείων/αγαθών των ΚΥ, στη δυνατότητα των διαχειριστών τους να αντιμετωπίσουν αποτελεσματικά τους κινδύνους και να εξασφαλίσουν τη λειτουργία τους. Το στοιχείο της κρισιμότητας χαρακτηρίζει επομένως όχι μόνο τις υποδομές, αλλά και τις οντότητες που έχουν την ευθύνη λειτουργίας τους, οιαδήποτε νομική μορφή και αν έχουν. Αποδίδεται έτσι σε αυτές η έννοια της "κρίσιμης οντότητας" (critical entity), καθώς η αξιοπιστία μιας ΚΥ, είναι συνάρτηση της αξιοπιστίας της οντότητας που τη διαχειρίζεται. Ανεξάρτητα αν η οντότητα που διαχειρίζεται μια ΚΥ ανήκει σε δημόσιο ή ιδιωτικό φορέα, η διασφάλιση της λειτουργικότητας των υποδομών ενός Κράτους, αποτελεί το αντικείμενο μιας εθνικής στρατηγικής με στόχο την αποτροπή, τον μετριασμό ή την εξουδετέρωση κινδύνων και ευπαθειών.[22]

[22] Γεώργιος Στεργιόπουλος "Ασφάλεια Κρίσιμων Υποδομών" σε "Ασφάλεια πληροφοριών και συστημάτων στον Κυβερνοχώρο" , εκδ. Νέες Τεχνολογίες 2021,κεφ.22 σελ. 634 επ.

Προαπαιτούμενο για την προστασία των ΚΥ είναι η αναγνώριση και ο προσδιορισμός τους. Για τον λόγο αυτό, έχουν αναπτυχθεί μεθοδολογίες εντοπισμού ΚΥ και κριτήρια αξιολόγησης της κρισιμότητας. Βασικό κριτήριο είναι η ένταξη της υποδομής σε κάποιο τομέα, ανάλογα με το είδος της υπηρεσίας που παρέχεται, σε συνδυασμό με χαρακτηριστικά και ιδιότητες τεχνικής ή άλλης φύσης. Σύμφωνα με τη προσέγγιση από την κορυφή προς τη βάση (top down approach), ο προσδιορισμός των ΚΥ γίνεται από κρατικά όργανα, ενώ σύμφωνα με την αντίθετη προσέγγιση (bottom up approach), γίνεται από τους ιδιοκτήτες/διαχειριστές των ΚΥ. Στη διαδικασία εμπλέκονται αρχές και φορείς που έχουν συσταθεί από το κράτος, με αρμοδιότητες εποπτείας και ελέγχου. Ειδικότερα για τον προσδιορισμό των κρίσιμων πληροφοριακών υποδομών (CIIs), οι μεθοδολογίες αναγνώρισης συνοψίζονται σε τρία βήματα:

- Αναγνώριση κρίσιμων τομέων (δημιουργία λίστας)
- Αναγνώριση κρίσιμων υπηρεσιών
- Αναγνώριση των στοιχείων (assets) του δικτύου και των υπηρεσιών των κρίσιμων πληροφοριακών συστημάτων, που υποστηρίζουν τις κρίσιμες υποδομές

Η διαδικασία της αναγνώρισης δεν είναι ωστόσο απλή, καθώς απαιτείται λεπτομερής κατάλογος των τομέων και προσδιορισμός κριτηρίων αναγνώρισης των κρίσιμων στοιχείων-αγαθών, ενώ πρέπει να υπάρχει αποτελεσματικός μηχανισμός συνεργασίας ιδιωτικού και δημόσιου τομέα.[23] Για τον προσδιορισμό των Κ.Υ., εκτός από τα τομεακά κριτήρια, μπορεί να εφαρμοστούν οριζόντια- διατομεακά κριτήρια, που βασίζονται στην εκ των προτέρων αποτίμηση των πιθανών επιπτώσεων από τη διατάραξη της λειτουργίας της υποδομής. Τέτοια κριτήρια είναι το εύρος της επηρεαζόμενης γεωγραφικής περιοχής, οι ανθρώπινες απώλειες, οι οικονομικές και δημόσιες επιπτώσεις. Στις επιπτώσεις περιλαμβάνονται η επίδραση της διατάραξης στα μακροοικονομικά μεγέθη, οι περιβαλλοντικές συνέπειες, η απώλεια της εμπιστοσύνης των πολιτών και ο αντίκτυπος της διαταραχής στη καθημερινή ζωή τους. Σημαντικές παράμετροι είναι ο αριθμός των ανθρώπων που μπορεί να επηρεαστούν, η ένταση των επιπτώσεων και η διάρκεια των συνεπειών.[24]

2.1.2. Στρατηγικές προστασίας Κ.Υ.

Για την προστασία των Κ.Υ. (CIP), έχουν υποστηριχθεί κυρίως δύο προσεγγίσεις. Η προσέγγιση μέσω της προστασίας των κρίσιμων πληροφοριακών συστημάτων (CICIP) και η ολιστική προσέγγιση "All Hazards". Η πρώτη αφορά στη προστασία των IT συνδέσεων ανάμεσα στους διαφορετικούς τομείς υποδομών, ενώ η δεύτερη, εκτός από τα πληροφοριακά συστήματα, περιλαμβάνει και τη φυσική ασφάλεια των κρίσιμων υποδομών. Στην "All Hazards"

[23] ENISA Methodologies for the identification of Critical Information Infrastructure assets and services, 2015 https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

[24] Petrakos, N., Kotzanikolaou, P. (2019). Methodologies and Strategies for Critical Infrastructure Protection, pp 17-33 In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer https://doi.org/10.1007/978-3-030-00024-0_2

προσέγγιση, κυρίαρχο ρόλο έχουν οι κυβερνητικές υπηρεσίες με συντονιστικές αρμοδιότητες. Οι πυλώνες ενός οργανωσιακού συστήματος CICIP είναι :

- Πρόληψη και Προειδοποίηση (Prevention and Early Warning): Ετοιμότητα των διαχειριστών των ΚΥ για αντιμετώπιση περιστατικών ασφάλειας.
- Ανίχνευση (Detection): Ανακάλυψη απειλών και περιστατικών ασφάλειας μη εμφανών σε συνεργασία με Ομάδες Αντιμετώπισης Περιστατικών Ασφάλειας (CERTs/CSIRTs), για την αποτελεσματική αντιμετώπισή τους.
- Αντίδραση (Reaction): Αναγνώριση πηγής προβλημάτων και διόρθωση
- Διαχείριση Κρίσεων (Crisis Management): Ελαχιστοποίηση των επιπτώσεων κρίσεων

Αποτελεί ωστόσο κοινή παραδοχή ότι δεν υπάρχει οργανωσιακό σύστημα προστασίας που να αποτρέπει πλήρως την εκδήλωση περιστατικών ασφάλειας. Η ολιστική προσέγγιση προστασίας, στοχεύει στη προσπάθεια περιορισμού των συνεπειών ενδεχόμενων περιστατικών, μέσω της διαρκούς παρακολούθησης. [25]

Ωστόσο σε όλα τα οργανωσιακά συστήματα που εκφράζουν τις στρατηγικές προστασίας των ΚΥ εντοπίζονται κοινά σημεία, που συνοψίζονται ως εξής:

- Η ύπαρξη ενός στρατηγικού οράματος προστασίας
- Ο καθορισμός μιας οργανωτικής δομής με όργανα, ρόλους και αρμοδιότητες
- Η σύμπραξη ιδιωτικού-δημόσιου τομέα (Public-Private Partnership (PPP)
- Η ανταλλαγή πληροφοριών (διαμοιρασμός/επίγνωση απειλών/κινδύνων)
- Δημιουργία θεσμικού πλαισίου
- Αναγνώριση των εθνικών ΚΥ
- Αποτίμηση επικινδυνότητας
- Διαχείριση επικινδυνότητας και κρίσεων/ υιοθέτηση μέτρων απόκρισης

2.1.3. Το θεσμικό πλαίσιο της ΕΕ

2.1.3.1. Η Οδηγία NIS

Από το 2004, η Ευρωπαϊκή Επιτροπή ασχολήθηκε με τη ρύθμιση του ζητήματος των κρίσιμων υποδομών, εκδίδοντας το 2005 την "Πράσινη βίβλο" και στη συνέχεια το Ευρωπαϊκό Πρόγραμμα Προστασίας Κρίσιμων Υποδομών, που αποτέλεσε τη βάση για την πρώτη Οδηγία 2008/114/ΕΚ με θέμα τον προσδιορισμό και την προστασία των ΚΥ. Η ραγδαία κλιμάκωση των κινδύνων και η έξαρση των περιστατικών ασφαλείας σε ΚΥ, είχε σαν αποτέλεσμα την έκδοση το 2016 της Οδηγίας (ΕΕ) 2016/1148 σχετικά με τα "Μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση" (Οδηγία NIS), με την οποία προσεγγίστηκε το ζήτημα των ΚΥ, μέσα από την επιβολή στα κράτη-μέλη της υποχρέωσης να

[25] Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης: Στρατηγικός Σχεδιασμός , Επιστημονική Επιμέλεια: Δ. Γκρίτζαλης, Ν.Μήτρου, Β. Σκουλαρίδου, eGov Forum-CICIP-D1-v2.3/29.09.2008 https://www.infosec.aueb.gr/CIS_Reviews/reviews/1580eGovFor_CICIP.pdf

θεσπίσουν μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.[26] Παράλληλα, η Οδηγία προέβλεψε τη δημιουργία εθνικών αρχών για την ασφάλεια των δικτύων και πληροφοριών, καθώς και ομάδων συνεργασίας και απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (GSIRT) μεταξύ των κρατών μελών. Σαν φορέα παροχής καθοδήγησης και εμπειρογνωμοσύνης όρισε τον ENISA. Η Οδηγία NIS υπήρξε το πρώτο κείμενο οριζόντιου χαρακτήρα, που εκφράζει τη στρατηγική της ΕΕ για τη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος, όμως σαν Οδηγία ελάχιστης εναρμόνισης, άφηνε περιθώρια ευελιξίας για την οργάνωση των δομών και διαδικασιών στα κράτη-μέλη. Χωρίς να χρησιμοποιεί τον όρο της Κυβερνοασφάλειας, τα μέτρα που περιλαμβάνει, αναφέρονται στην αντιμετώπιση των κινδύνων του Κυβερνοχώρου. [27]

Στο πεδίο των ΚΥ, η οδηγία NIS έθεσε απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών για τους φορείς εκμετάλλευσης βασικών υπηρεσιών (ΦΕΒΥ) και τους παρόχους ψηφιακών υπηρεσιών (Operators of Essential Services OES/ Digital services providers DSP). Σαν κριτήρια προσδιορισμού των ΦΕΒΥ όρισε τα εξής:

- Παροχή υπηρεσίας ουσιώδους για τη διατήρηση κρίσιμων κοινωνικών και/ή οικονομικών δραστηριοτήτων
- Η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφοριών
- Πρόκληση σοβαρής διατάραξης της παροχής της υπηρεσίας από τυχόν συμβάν

Ο ENISA στη συνέχεια παρείχε κατευθυντήριες οδηγίες συμμόρφωσης των ΦΕΒΥ στις απαιτήσεις της Οδηγίας NIS, με στόχο την επίτευξη ενός κοινού πεδίου για την ασφάλεια πληροφοριών και πληροφοριακών συστημάτων στην ΕΕ. [28] Ως κύριος άξονας της πολιτικής για τους ΦΕΒΥ ορίζεται η ανάπτυξη της συνεργασίας μεταξύ των διαχειριστών των ΚΥ, στο πεδίο της διαχείρισης επικινδυνότητας της Τεχνολογίας πληροφοριών (IT). Σημαντικό στοιχείο της συνεργασίας είναι η αναφορά των περιστατικών ασφαλείας, μέσω μιας θεσμοθετημένης διαδικασίας, στην οποία εμπλέκονται ιδιωτικοί και δημόσιοι φορείς.

Η διαδικασία διαχείρισης επικινδυνότητας που προτείνεται από τον ENISA, ακολουθεί τη δομή των διεργασιών που προβλέπει το ISO 27005. Στα Παραρτήματα, αναλύονται ειδικότερα τα Πρότυπα ISO 27001 για την ασφάλεια πληροφοριών και COBIT 5 για την ολιστική διακυβέρνηση του τομέα του IT σε όλο το φάσμα της επιχείρησης. Παράλληλα αξιολογούνται τα κυριότερα διεθνή και εθνικά Πλαίσια, Πρότυπα και μεθοδολογίες διαχείρισης/αποτίμησης

---

[26] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (NIS) 32016L1148 - EN - EUR-Lex

[27] Μήτρου Λ.“Το κανονιστικό πλαίσιο της (Κυβερνο) Ασφάλειας” κεφ.3 σε Κάτσικας Σ., Γκρίτζαλης Σ., Λαμπρινουδάκης Κ (επιμ.) “Ασφάλεια πληροφοριών και συστημάτων στον Κυβερνοχώρο” , εκδ. Νέες Τεχνολογίες 2021 σελ.78 επ.

[28] ENISA Guidelines on assessing DSP and OES compliance to the NISD security requirements Information Security Audit and Self – Assessment/ Management Frameworks Nov.2018 https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

επικινδυνότητας, όσον αφορά τα ιδιαίτερα χαρακτηριστικά τους κατά την εφαρμογή τους στους ΦΕΒΥ (ISO 27005, Risk IT, NIST 800-30 και 800-39,Octave, Magerit,Mehari, Monarc). Ο ENISA,διαμορφώνοντας ένα πρόγραμμα τακτικών ελέγχων στους ΦΕΒΥ, ώστε να ανταποκρίνονται στις απαιτήσεις της Οδηγίας NIS, κατατάσσει τα μέτρα ασφαλείας για τους ΦΕΒΥ σε τέσσερις τομείς (Διακυβέρνηση και Οικοσύστημα, Προστασία, ΄Αμυνα, Ανθεκτικότητα) με αντίστοιχους υποτομείς, διατυπώνοντας ανά μέτρο ασφαλείας κατάλληλες ερωτήσεις για τον έλεγχο και την τεκμηρίωση εφαρμογής τους.

2.1.3.2. Η Οδηγία NIS 2

Η Οδηγία NIS , ενόψει της πολυπλοκότητας των περιστατικών ασφαλείας και ιδιαίτερα των προκλήσεων στον τομέα της κυβερνοασφάλειας, παρουσίασε ανεπάρκειες ως προς την ενιαία αντιμετώπιση του ζητήματος της ασφάλειας των πληροφοριακών συστημάτων στο χώρο της ΕΕ. Με δεδομένο ότι η Οδηγία άφηνε τη ρύθμιση σημαντικών υποχρεώσεων και απαιτήσεων στη διακριτική ευχέρεια των κρατών -μελών, εμφανίστηκαν αποκλίσεις κατά την εφαρμογή της, που θα μπορούσαν να οδηγήσουν στη δημιουργία ευπαθειών, με συνολικά αρνητικά αποτελέσματα για τη λειτουργία της εσωτερικής αγοράς.

΄Οπως προέκυψε από έρευνα του ENISA σχετικά με τις επενδύσεις των επιχειρήσεων Κ.Υ. (OES/DPS) της ΕΕ για την εφαρμογή της Οδηγίας NIS στον τομέα της Τεχνολογίας Πληροφοριών (IT), η ΕΕ υπολείπεται έναντι των χωρών της Β.Αμερικής και της Ασίας (APAC) στις επενδύσεις στις νέες τεχνολογίες. Ειδικότερα στο πεδίο των επενδύσεων για την Κυβερνοασφάλεια, οι παραπάνω χώρες έχουν το προβάδισμα, με την ΕΕ να προσπαθεί να τις ακολουθήσει. [29] Οι λόγοι αυτοί επέβαλαν την έκδοση μιας επικαιροποιημένης Οδηγίας, που θα ενοποιούσε διαδικασίες και πρακτικές και θα έθετε νέες υποχρεώσεις στις οντότητες των ΚΥ, σύμφωνα με τα δεδομένα της τεχνολογίας, ιδιαίτερα στον τομέα της Κυβερνοασφάλειας.

Τον Δεκέμβριο του 2022, εκδόθηκε η νέα Οδηγία NIS 2, η οποία θέτει ως χρονικό όριο συμμόρφωσης των κρατών μελών με τις ρυθμίσεις της την 17-10-2024 (άρθρο 44), μετά την οποία η Οδηγία NIS θα παύσει να ισχύει.[30] Κύριο σημείο στο οποίο διαφοροποιείται η NIS 2, είναι ο σαφής προσδιορισμός των οντοτήτων που αναγνωρίζονται σαν κρίσιμες και η επιβολή σε αυτές ενός αυστηρότερου πλαισίου υποχρεώσεων. Καταργεί τη διάκριση μεταξύ ΦΕΒΥ και παρόχων ψηφιακών υπηρεσιών και εισάγει τις έννοιες των βασικών και σημαντικών οντοτήτων (essential /important entities). Η διάκριση μεταξύ βασικών και σημαντικών δεν είναι ουσιώδης, αφού διαφοροποιούνται σε επιμέρους ζητήματα ελέγχων, επιθεώρησης και ύψους προστίμων για

[29] ENISA NIS Investments Report 2023, Nov.16,2023
https://www.enisa.europa.eu/publications/nis-investments-2023

[30] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (NIS 2) 32022L2555 - EN - EUR-Lex

πιθανές παραβάσεις. Για την κατάταξη των οντοτήτων στον κατάλογο των βασικών και σημαντικών, ορίζονται ενιαία κριτήρια ταξινόμησης, σε συγκεκριμένους τομείς και υποτομείς που παρατίθενται στα παραρτήματα της Οδηγίας και ισχύουν για το σύνολο του χώρου της ΕΕ. Παράλληλα, θέτει υποχρεώσεις στα κράτη μέλη για δημιουργία μηχανισμών καταχώρισης σε ειδικά μητρώα βασικών και σημαντικών οντοτήτων. Έως τις 17 Απριλίου 2025, τα κράτη μέλη οφείλουν να καταρτίσουν σχετικό κατάλογο βασικών και σημαντικών οντοτήτων, τον οποίο θα κοινοποιήσουν στην Επιτροπή.

Οι παραπάνω οντότητες, σε περίπτωση που δεν συμμορφωθούν με τις απαιτήσεις και τα μέτρα που προβλέπει η Οδηγία, υπόκεινται σε διοικητικά πρόστιμα και κυρώσεις. Κυριότεροι τομείς απαιτήσεων είναι η διακυβέρνηση και η κατάρτιση ενός ΣΔΑΠ για διαχείριση επικινδυνότητας, η εγγραφή στα μητρώα βασικών/ σημαντικών οντοτήτων, η αναφορά περιστατικών ασφαλείας, η ανθεκτικότητα της τεχνολογίας πληροφοριών, η λήψη τεχνολογικά προηγμένων μέτρων ασφαλείας και ιδιαίτερα κυβερνοασφάλειας, η διενέργεια ελέγχων και δοκιμών.

Στη νέα Οδηγία, γίνεται ευθεία αναφορά στη Κυβερνοασφάλεια, στην οποία εστιάζει σαν προϋπόθεση για την αντιμετώπιση των νέων απειλών και επιθέσεων, αλλά και για την αξιοποίηση του ψηφιακού μετασχηματισμού. Ως κεντρικός στόχος της Οδηγίας, καθορίζεται η επίτευξη υψηλού ενιαίου επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση. Επιβάλλεται έτσι στα κράτη μέλη, η ανάπτυξη εθνικής στρατηγικής για την Κυβερνοασφάλεια, που να περιλαμβάνει την ενεργητική κυβερνοπροστασία. Για τον λόγο αυτό, οι απαιτήσεις κυβερνοασφάλειας θα πρέπει να εφαρμόζονται ενιαία από όλα τα κράτη μέλη, αντικείμενο που εποπτεύεται από τις Εθνικές Αρχές Κυβερνοασφάλειας, που οφείλουν αυτά να συστήσουν. Η Οδηγία NIS 2, σαν βάση αναφοράς για τα μέτρα διαχείρισης κινδύνων στον τομέα της Κυβερνοασφάλειας, προβλέπει υποχρεώσεις ανταλλαγής πληροφοριών μέσω του δικτύου CSIRT για γνωστοποίηση ευπαθειών των συστημάτων και αντιμετώπιση σημαντικών κυβερνοαπειλών. Στο δίκτυο CSIRT παρέχονται αρμοδιότητες συνεργασίας με τις εθνικές ομάδες αντιμετώπισης περιστατικών ασφαλείας και τα αντίστοιχα διεθνή δίκτυα, μέσω ενοποιημένων διαδικασιών κοινοποίησης συμβάντων και εποπτείας, ενώ συνεργάζεται παράλληλα με το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe). Μεγάλη βαρύτητα αποδίδεται στην αναφορά περιστατικών κυβερνοασφάλειας (άρθρο 23), βάσει ενός συστήματος τριών χρονικών σταδίων, που ξεκινά από τη στιγμή που έγινε αντιληπτό ένα σημαντικό περιστατικό ασφαλείας. Προβλέπεται αναφορά εντός 24ώρου, μετά από 72 ώρες και τέλος υποβολή λεπτομερούς αναφοράς εντός μηνός προς την GSIRT και άλλες αρμόδιες αρχές, που αντίστοιχα παρέχουν καθοδήγηση για αντιμετώπιση του περιστατικού.

Η NIS 2, ακολουθεί ολιστική προσέγγιση διαχείρισης "έναντι όλων των κινδύνων" (All Hazards) στον τομέα της κυβερνοασφάλειας, η οποία συμπεριλαμβάνει την ανθεκτικότητα των συστημάτων δικτύου και πληροφοριών από απειλές που στρέφονται κατά των υλικών

συστατικών στοιχείων και του περιβάλλοντός τους, όπως φυσικά φαινόμενα, κακόβουλες πράξεις ή ανθρώπινα σφάλματα. Για τη διαχείριση της επικινδυνότητας, προβλέπει την εφαρμογή διεθνών Προτύπων, παραπέμποντας ενδεικτικά σε αυτά που περιλαμβάνονται στη σειρά ISO 27000. Στη νέα Οδηγία, σημαντικές αρμοδιότητες δίνονται στην Ομάδα Συνεργασίας (Cooperation Group), ένα όργανο που αποτελείται από εκπροσώπους των κρατών-μελών, της Επιτροπής και του ENISA, του οποίου ο ρόλος αναβαθμίζεται με την ενεργή συμμετοχή του στις προβλεπόμενες διαδικασίες, σαν συμβουλευτικού και γνωμοδοτικού οργανισμού.

2.1.3.4. Η Οδηγία CER

Γεγονότα όπως η δολιοφθορά στον αγωγό αερίου Nord Stream και ο πόλεμος μεταξύ Ρωσίας και Ουκρανίας, έδειξαν ότι η γεωγραφική περιοχή της Ευρώπης, είναι ευάλωτη σε πολυδιάστατες απειλές υβριδικού τύπου, που συνδυάζουν κυβερνοεπιθέσεις, με επιθέσεις στο φυσικό περιβάλλον των κρίσιμων υποδομών. Οι νέοι κίνδυνοι που θα μπορούσαν να υπονομεύσουν τη λειτουργία των ΚΥ της ΕΕ, έθεσαν επιτακτικά το ζήτημα της ενίσχυσης της ετοιμότητας των ΚΥ για αντιμετώπιση περιστατικών και κρίσεων, καθώς και της ανάγκης για εναρμόνιση των κανόνων και συνεργασία σε διεθνές επίπεδο. Έτσι παράλληλα με την Οδηγία NIS 2, η ΕΕ τον Δεκέμβριο του 2022 προχώρησε στην έκδοση της Οδηγίας 2022/2557 για την ανθεκτικότητα των Κρίσιμων Οντοτήτων (Οδηγία CER), με τις δύο Οδηγίες να χαρακτηρίζονται σαν "όψεις του ίδιου νομίσματος".[31] Η οδηγία CER αντικαθιστά την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας του 2008, καθώς προβλέπει ως καταληκτική προθεσμία θέσπισης μέτρων υλοποίησής της για τα κράτη μέλη, την 17-10-2024, θέτοντας ένα χρονοδιάγραμμα πλήρους συμμόρφωσης προς τις απαιτήσεις της έως το 2027.

Στόχος της Οδηγίας CER [32] είναι οι κρίσιμες οντότητες να είναι σε θέση να προλαμβάνουν περιστατικά που ενδέχεται να διαταράξουν την παροχή βασικών υπηρεσιών, να αντιδρούν και να αντιστέκονται σε απειλές, να μετριάζουν και να απορροφούν τις επιπτώσεις, αλλά επίσης να προσαρμόζονται και να ανακάμπτουν από περιστατικά ασφαλείας. Το σημείο που τη διακρίνει από την Οδηγία NIS 2, είναι ότι εστιάζει στην αντιμετώπιση των ευπαθειών και στη διαχείριση επικινδυνότητας, ώστε να ενισχυθεί η ανθεκτικότητα των κρίσιμων οντοτήτων. Δεν κάνει διαχωρισμό μεταξύ βασικών και σημαντικών οντοτήτων, αλλά χρησιμοποιεί τον όρο "κρίσιμες οντότητες" για τους φορείς υποδομών ζωτικής σημασίας, που έχουν αναγνωριστεί από τα κράτη μέλη ως κρίσιμοι, βάσει της διαδικασίας αποτίμησης κινδύνου και σύμφωνα με ενιαία στον ευρωπαϊκό χώρο κριτήρια. Όσες οντότητες αναγνωριστούν ως κρίσιμες, πρέπει αντίστοιχα να θεωρηθούν σαν βασικές οντότητες στο πεδίο της NIS 2. Η Οδηγία CER καθορίζει συγκεκριμένα κριτήρια βάσει των οποίων κρίνεται η κρισιμότητα μιας οντότητας και ειδικότερα:

---

[31] European Commission, Press Release 18-10-22 "Critical Infrastructure : Commission accelerates work to build up European resilience"https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

[32] Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 14ης Δεκεμβρίου 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (οδηγία CER) 32022L2557 - EN - EUR-Lex

- Τον αριθμό των χρηστών που εξαρτώνται από τη βασική υπηρεσία που παρέχεται
- Τον βαθμό εξάρτησης άλλων κρίσιμων οντοτήτων από τη βασική υπηρεσία
- Τον αντίκτυπο που θα μπορούσαν να έχουν τα περιστατικά σε οικονομικές και κοινωνικές δραστηριότητες, στο περιβάλλον, στη δημόσια ασφάλεια και στην υγεία του πληθυσμού
- Το μερίδιο αγοράς της οντότητας στην αγορά παροχής της βασικής υπηρεσίας
- Τη γεωγραφική περιοχή που θα μπορούσε να επηρεαστεί από ένα περιστατικό
- Τη σημασία της οντότητας για τη διατήρηση επαρκούς επιπέδου της βασικής υπηρεσίας

Η Οδηγία μετατοπίζει έτσι το βάρος αφενός από την έννοια της προστασίας, στην έννοια της ανθεκτικότητας έναντι φυσικών και ανθρωπογενών κινδύνων, και αφετέρου από τις κρίσιμες υποδομές, στις κρίσιμες οντότητες, για τις οποίες προβλέπονται αυξημένες υποχρεώσεις. Οι κύριες απαιτήσεις για τις κρίσιμες οντότητες είναι:

- Αποτίμηση επικινδυνότητας βάσει της προσέγγισης “all hazards” (ασφάλεια συστημάτων δικτύου/πληροφοριών και υλικού/φυσικού τους περιβάλλοντος)
- Ύπαρξη σχεδίου για την ανθεκτικότητα και την επιχειρησιακή συνέχεια
- Λήψη μέτρων για την ανθεκτικότητα (τεχνικών, ασφαλείας, οργανωσιακών)
- Αναφορά περιστατικών που διαταράσσουν ή μπορεί να διαταράξουν τη λειτουργία τους
- Αναθεώρηση της αποτίμησης επικινδυνότητας τουλάχιστον ανά τετραετία
- Πρόγραμμα τακτικής εκπαίδευσης προσωπικού
- Ορισμός εκπροσώπου ως συνδέσμου για επαφή με τις αρμόδιες αρχές

Αντίστοιχα, οι απαιτήσεις για τα κράτη μέλη είναι η αναγνώριση των κρίσιμων οντοτήτων και η γνωστοποίησή τους στην ΕΕ, η εποπτεία τους, η θέσπιση μηχανισμού κοινοποίησης περιστατικών και η συνεργασία με τους αρμόδιους φορείς, σε συνδυασμό με την χάραξη μιας ολιστικής στρατηγικής ανθεκτικότητας των εθνικών κρίσιμων οντοτήτων. Παράλληλα τα κράτη μέλη πρέπει να ενθαρρύνουν την εφαρμογή από τις κρίσιμες οντότητες ευρωπαϊκών και διεθνών Προτύπων για την εναρμόνιση των πρακτικών και των τεχνικών προδιαγραφών. Τα κράτη μέλη οφείλουν να εγκρίνουν ένα ολοκληρωμένο πλαίσιο διακυβέρνησης των κρίσιμων οντοτήτων τους μέχρι την 17-1-2026. Ο συντονισμός της εφαρμογής της Οδηγίας, πραγματοποιείται από την Ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων, που υποστηρίζει την Επιτροπή στη παροχή συνδρομής στα κράτη μέλη.

2.2. Τομείς και κατηγορίες Κρίσιμων Υποδομών/ Οντοτήτων /Λειτουργιών

2.2.1. Ευρωπαϊκή Ένωση

Αν και στη Πράσινη Βίβλο γινόταν αναφορά ενδεικτικά σε 11 τομείς ΚΥ (Ενέργεια, Προμήθεια νερού, Τεχνολογίες πληροφοριών και επικοινωνίας, προμήθεια τροφής, υγεία, χρηματοπιστωτικές αγορές, Δημόσια τάξη και ασφάλεια, Δημόσια διοίκηση, Μεταφορές, Χημική και Ατομική βιομηχανία, Διάστημα και έρευνα), [33] η Οδηγία NIS, δεν κατηγοριοποίησε στη συνέχεια τους ΦΕΒΥ, προκρίνοντας τη λύση του προσδιορισμού τους μέσω μιας σύνθετης διαδικασίας με τεχνικές και πολιτικές παραμέτρους, που εστιάζει στον αντίκτυπο που θα προκαλούσε η διατάραξη της λειτουργίας τους. Ο ENISA ωστόσο σε χρονικά προγενέστερες οδηγίες του για τις μεθοδολογίες προσδιορισμού των ΚΥ, προκειμένου να διευκολύνει τα κράτη-μέλη στον προσδιορισμό, είχε καταρτίσει ένα κατάλογο 13 τομέων με υποτομείς και αντίστοιχες κρίσιμες υπηρεσίες, προσθέτοντας στους τομείς της Πράσινης Βίβλου το περιβάλλον, την πολιτική προστασία και την Εθνική Άμυνα.[34]

Η παραπάνω πολιτική προσδιορισμού των ΚΥ, προκάλεσε τον κατακερματισμό της έννοιας της κρίσιμης υποδομής στο χώρο της ΕΕ, με αποτέλεσμα την ασυνέπεια στην αναγνώρισή τους. Κρίθηκε επομένως επιβεβλημένο να ρυθμιστεί με ενιαίο και αξιόπιστο τρόπο το ζήτημα του προσδιορισμού των κρίσιμων οντοτήτων, ως παρόχων των βασικών και σημαντικών υπηρεσιών. Ετσι στην Οδηγία NIS 2 (παράρτημα 1), ορίζονται ρητά οι 11 τομείς και οι υποτομείς των βασικών οντοτήτων υψηλής κρισιμότητας:

1. Ενέργεια → Ηλεκτρική ενέργεια,τηλεθέρμανση/ τηλεψύξη, πετρέλαιο, αέριο υδρογόνο	7. Λύματα
2. Μεταφορές → Εναέριες,Σιδηροδρομικές, Πλωτές, Οδικές	8. Ψηφιακές υποδομές
3. Τραπεζικός τομέας	9. Διαχείριση υπηρεσιών ΤΠΕ
4. Υποδομές χρηματοπιστωτικών αγορών	10. Οντότητες δημόσιας διοίκησης
5. Υγεία	11. Διάστημα (παροχή υπηρεσιών από επίγειες υποδομές που ανήκουν σε κράτη μέλη ή ιδιώτες)
6. Υδροδότηση	

[33] Commission of the European Communities (2005), "Green Paper on a European Programme for Critical Infrastructure Protection" Annex 2
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=pl
[34] ENISA Methodologies for the identification of C. I.I. assets and services, 2015 ό.π. σελ. 22

Στο παράρτημα 2 παράλληλα, αναφέρονται οι επτά σημαντικοί τομείς και συγκεκριμένα ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, διαχείριση αποβλήτων, παρασκευή/ διανομή χημικών προϊόντων, παραγωγή/μεταποίηση/διανομή τροφίμων, κατασκευαστικός τομέας, ψηφιακοί πάροχοι και έρευνα. Στην Οδηγία CER ακολουθείται επίσης η ίδια πολιτική ρητού προσδιορισμού των κρίσιμων οντοτήτων. Στο παράρτημα της παρατίθεται λεπτομερής κατάλογος τομέων, υποτομέων και κατηγοριών οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της, οι οποίοι ταυτίζονται με τους τομείς της Οδηγίας NIS 2, με τη προσθήκη του τομέα της παραγωγής, μεταποίησης και διανομής τροφίμων.

2.2.2. Η.Π.Α

Αντίθετα με την ΕΕ, οι ΗΠΑ εξαρχής ακολούθησαν πολιτική καθορισμού συγκεκριμένων τομέων των ΚΥ, που, αν προσβληθούν, μπορεί να προκαλέσουν σοβαρές επιπτώσεις στην υγεία, την ασφάλεια, την οικονομία και το κοινωνικό σύστημα. [35] Σύμφωνα με την Προεδρική Οδηγία του 2013 και το Εθνικό Σχέδιο Προστασίας Υποδομών (National Infrastructure Protection Plan - NIPP), που εκδόθηκε στη συνέχεια, οι 16 τομείς ΚΥ είναι : [36]

1. Χημικές ουσίες	9. Χρηματοπιστωτικές υπηρεσίες
2. Εμπορικές εγκαταστάσεις	10. Τομέας τροφίμων και γεωργίας
3. Επικοινωνίες	11.Κυβερνητικές εγκαταστάσεις
4. Κρίσιμος κατασκευαστικός τομέας	12.Υγειονομική φροντίδα και Δημόσια Υγεία
5. Φράγματα (Dams)	13.Τεχνολογία της πληροφορίας
6. Βιομηχανική βάση Εθνικής Άμυνας	14.Πυρηνικοί αντιδραστήρες/ Υλικά/ Απόβλητα
7. Υπηρεσίες έκτακτης ανάγκης	15.Μεταφορές
8. Ενέργεια	16.Υδροδότηση και αποχέτευση

[35] CISA Critical Infrastructure Sectors |https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[36] Presidential Policy Directive (PPD)21: Critical Infrastructure Security and Resilience https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

Η προστασία των αγαθών, των συστημάτων και των δικτύων που ανήκουν στους παραπάνω τομείς, είτε έχουν φυσική υπόσταση, είτε είναι άυλα, αποτελεί προτεραιότητα για την εθνική ασφάλεια και προϋποθέτει συνεργασία δημόσιου και ιδιωτικού τομέα, ενώ η εποπτεία των ΚΥ έχει ανατεθεί στο Υπουργείο Εσωτερικών (Secretary of Homeland Security) σε συνδυασμό με την άσκηση αρμοδιοτήτων από τομεακές αρχές (specific sector agencies). Η Αρχή για την Κυβερνοασφάλεια και την ασφάλεια των υποδομών (CISA) κατάρτισε το 2019 ένα κατάλογο 55 κρίσιμων λειτουργιών δημόσιου και ιδιωτικού τομέα, τις οποίες κατέταξε σε 4 ευρύτερες κατηγορίες που αφορούν:

- Σύνδεση (Λειτουργία διαδικτύου και παροχή σχετικών υπηρεσιών)
- Διανομή (Ηλεκτρική ενέργεια/ μεταφορές επιβατών και εμπορευμάτων/ μεταφορές με αγωγούς)
- Διαχείριση (τομείς δημόσιου και ιδιωτικού τομέα για διακυβέρνηση/εκπαίδευση/χρηματοπιστωτικές υπηρεσίες/υγεία κλπ)
- Προμήθεια (παραγωγή/ παροχή τροφίμων, νερού, καυσίμων, προϊόντων και υπηρεσιών τεχνολογίας της πληροφορίας κλπ)[37]

2.2.3. Εξαρτήσεις και αλληλεξαρτήσεις ΚΥ

Οι παραπάνω τομείς ωστόσο, δεν αποτελούν στεγανά, καθώς κύριο χαρακτηριστικό των ΚΥ είναι η εξάρτησή τους από άλλες υποδομές, αλλά και η αλληλεξάρτησή τους. Ένα περιστατικό που έχει επιπτώσεις σε μια ΚΥ, επηρεάζει ή σχετίζεται με τη λειτουργία μιας άλλης υποδομής ή πολλών ταυτόχρονα υποδομών σε εθνικό ή διεθνές επίπεδο. Εξάλλου, μεταξύ των κρίσιμων οντοτήτων, υπάρχουν σταθερές σχέσεις αλληλεξάρτησης, καθώς προκειμένου να παρέχουν μια βασική υπηρεσία, ανταλλάσσουν αγαθά και υπηρεσίες. Στη σύγχρονη μορφή τους, οι ΚΥ εξαρτώνται όλο και περισσότερο από τη λειτουργία δικτύων πληροφοριών και πληροφοριακών συστημάτων, με τα οποία είναι διασυνδεδεμένες. Η αύξηση του βαθμού αλληλεξάρτησης, διαμορφώνει νέους όρους κινδύνου, με αιχμή τις απειλές του κυβερνοχώρου. Η εκδήλωση αστοχίας σε μια ΚΥ μπορεί να έχει αντίκτυπο στις διασυνδεδεμένες ΚΥ και λόγω αλυσιδωτών επιδράσεων, να οδηγήσει σε αθροιστικές συνέπειες μεγάλης κλίμακας για ΚΥ διαφορετικών τομέων. Η κατανόηση των πολύπλοκων αλληλεπιδράσεων μεταξύ των ΚΥ, είναι προϋπόθεση για την προετοιμασία, την απόκριση και την ανάκαμψη από ένα περιστατικό ασφαλείας.

Η αλληλεπίδραση μεταξύ μιας ΚΥ και του περιβάλλοντός της, κατατάσσεται σε τρεις κατηγορίες εξαρτήσεων. Τις εξαρτήσεις από άλλες υποδομές για παροχή προϊόντων ή υπηρεσιών που είναι απαραίτητα για τη λειτουργία της υποδομής (upstream dependencies), τις εσωτερικές εξαρτήσεις που αφορούν στην αλληλεξάρτηση μεταξύ αγαθών της ίδιας υποδομής (internal dependencies) και τις εξαρτήσεις από τις επιπτώσεις της υποβάθμισης λειτουργίας της

[37] CISA National Critical Functions Set, April 2019
https://www.cisa.gov/sites/default/files/publications/national-critical-functions-set-508.pdf

ΚΥ προς τους τελικούς χρήστες της υπηρεσίας (downstream dependencies). ΄Οταν η ΚΥ παρέχει άμεσα μια υπηρεσία ή ένα αγαθό στους χρήστες, η σχέση τους χαρακτηρίζεται σαν εξάρτηση πρώτης τάξεως, ενώ δεύτερης τάξης χαρακτηρίζεται όταν έμμεσα μέσω άλλων υποδομών υποστηρίζει τους χρήστες (first/second order dependency). Κάθε κατηγορία περιλαμβάνει ένα ή περισσότερα από τα εξής είδη αλληλεξαρτήσεων:

- Φυσικές, που αναφέρονται στην παροχή υλικών αγαθών
- Κυβερνοχώρου, που αφορούν στην εξάρτηση από δεδομένα και πληροφορίες που μεταδίδονται μέσω πληροφοριακής υποδομής
- Γεωγραφικές, που αναφέρονται σε ταυτόχρονες περιβαλλοντικές επιπτώσεις σε ΚΥ μιας κοινής γεωγραφικής περιοχής
- Λογικές, που προκύπτουν από λογικές ανθρώπινες αποφάσεις και ενέργειες και όχι σαν αποτέλεσμα διαδικασιών του φυσικού κόσμου ή του κυβερνοχώρου.

Οι εξαρτήσεις και αλληλεξαρτήσεις μιας ΚΥ είναι πολυδιάστατες και επηρεάζονται από το περιβάλλον λειτουργίας της, τον τρόπο και χρόνο απόκρισης σε περιστατικά, τα οργανωσιακά και λειτουργικά χαρακτηριστικά της, καθώς και το είδος της αστοχίας που προκαλεί την υποβάθμιση, λόγω των αλληλεξαρτήσεων με άλλες ΚΥ. Οι αστοχίες (failures) μπορεί να είναι:

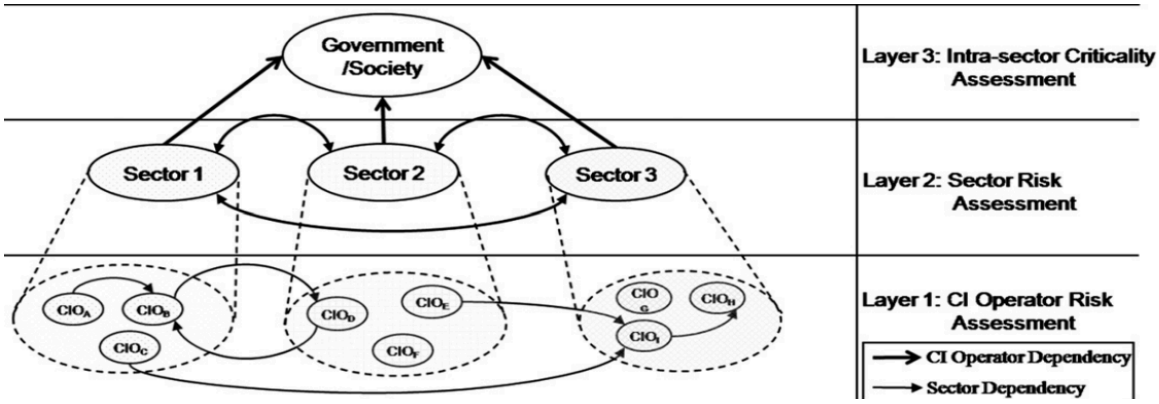
- Κοινής αιτίας, όταν έχουμε διατάραξη μιας ή περισσότερων ΚΥ ταυτοχρόνως (common cause)
- Διαδοχικές, όταν η διατάραξη μιας ΚΥ επιφέρει τη διατάραξη μιας άλλης (cascading/domino effect)
- Κλιμακούμενες όταν η διατάραξη μιας ΚΥ προκαλεί επιδείνωση της ανεξάρτητης διατάραξης μιας άλλης ΚΥ (escalating/snowball effect)[38]
-

Μια προτεινόμενη μεθοδολογία αποτίμησης κρισιμότητας μέσω της μοντελοποίησης των αλληλεξαρτήσεων, βασίζεται στο καθορισμό τριών επιπέδων, με διαφορετικές απαιτήσεις και στόχους. Η έξοδος του χαμηλότερου επιπέδου, είναι είσοδος στο ανώτερο και η μοντελοποίηση των αλληλεξαρτήσεων μεταξύ υποδομών πραγματοποιείται μέσω δένδρων εξάρτησης (dependency trees). Τα επίπεδα (layers) είναι τα εξής:

- ➢ Επίπεδο Οργανισμού : Οι αλληλεξαρτήσεις λαμβάνονται υπόψη στο πλαίσιο της προστασίας του συγκεκριμένου οργανισμού από εσωτερικές /εξωτερικές απειλές. Η μοντελοποίηση γίνεται μέσω δένδρων εξάρτησης
- ➢ Επίπεδο τομέα : Η ανάλυση κρισιμότητας αφορά όλους τους οργανισμούς του ίδιου τομέα, εξετάζονται οι αλληλεξαρτήσεις με άλλους τομείς καθώς και οι κοινωνικές επιπτώσεις. Η μοντελοποίηση περιλαμβάνει δένδρα εξάρτησης κοινωνικού αντικτύπου.

[38] Petit Frederic, "Analysis of Critical Infrastructure Dependencies and Interdependencies" Argonne June 2015 https://www.researchgate.net/publication/299525808_Analysis_of_Critical_Infrastructure_Dependencies_and_Interdependencies

➢ Διατομεακό/εθνικό επίπεδο: Εξετάζονται οι αλληλεξαρτήσεις μεταξύ όλων των τομέων σε εθνικό επίπεδο και ο αντίκτυπος στο σύνολο της κοινωνίας. Επανεξετάζονται τα αποτελέσματα των προηγούμενων επιπέδων, για μια συνολική εκτίμηση των αλληλεξαρτήσεων.[39]



Σχήμα 3: Ανάλυση κρισιμότητας μέσω της προσέγγισης τριών επιπέδων αλληλεξαρτήσεων

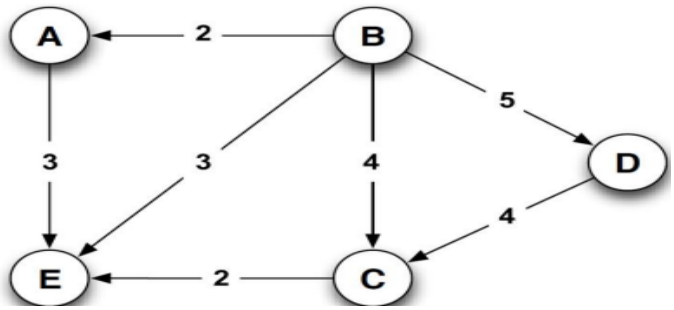
Οι εξαρτήσεις και αλληλεξαρτήσεις μεταξύ των ΚΥ είναι πολύπλοκες και εξελίσσονται δυναμικά. Για τη διαχείρισή τους στο πλαίσιο της ανθεκτικότητας και της αποτίμησης της επικινδυνότητας των ΚΥ, τα παραπάνω στοιχεία πρέπει να αναγνωριστούν, να αναλυθούν και να ενσωματωθούν σε πλαίσια και μεθοδολογίες. Οι αλληλεξαρτήσεις είτε λειτουργούν σαν πολλαπλασιαστές επικινδυνότητας, είτε αποτελούν αυτές οι ίδιες ευαλωτότητες ή απειλές για μια ΚΥ. Μία προσέγγιση αποτίμησης της επικινδυνότητας, είναι η προσέγγιση "system of systems" (SoS), σύμφωνα με την οποία μία κρίσιμη υποδομή εκλαμβάνεται σαν ένα μέρος ενός ευρύτερου συστήματος ή υποδομής. Μέσω της προσέγγισης αυτής μπορεί να καθοριστούν τα αγαθά και τα υποσυστήματα για τα οποία θα αντληθούν δεδομένα, ώστε να πραγματοποιηθεί ανάλυση και αποτίμηση των αλληλεξαρτήσεων μιας ΚΥ, αφού ληφθούν υπόψη όλα τα διασυνδεδεμένα συστήματα. Η συλλογή και ανάλυση δεδομένων, εκτός των φυσικών αλληλεξαρτήσεων, εκτείνεται στις εξαρτήσεις που αφορούν τον κυβερνοχώρο και τις γεωγραφικές εξαρτήσεις, ενώ περιλαμβάνει την απεικόνιση των εξαρτήσεων πρώτης και δεύτερης τάξης στη περίπτωση των διαδοχικών αστοχιών.

Ωστόσο η προσέγγιση αυτή, παρουσιάζει δυσκολίες εφαρμογής, καθώς κάθε οντότητα που διαχειρίζεται ΚΥ, πρέπει να λάβει υπόψη ευπάθειες και απειλές που αφορούν άλλες ΚΥ του ευρύτερου συστήματος, τις οποίες διαχειρίζονται άλλες οντότητες. Υπάρχει άλλωστε η πιθανότητα να προκύψει αιφνιδιαστικά μια αλληλεξάρτηση, η οποία δεν είχε ληφθεί υπόψη. Η οδηγία CER, επανειλημμένα αναφέρεται στις αλληλεξαρτήσεις των ΚΥ, τόσο διατομεακής και διασυνοριακής φύσης, όσο και μεταξύ των ψηφιακών και φυσικών διεπαφών, σαν παράγοντα

[39] M. Theoharidou, Kotzanikolaou P., Gritzalis D., A multi-layer Criticality Assessment methodology based on interdependencies, 2010 https://www.sciencedirect.com/science/article/abs/pii/S0167404810000210

που είναι καθοριστικός για τη διαχείριση επικινδυνότητας, δείχνοντας ότι υιοθετεί την προσέγγιση "System of Systems", χωρίς να προσδιορίζει ωστόσο τον τρόπο εφαρμογής της. [40]

Η αλληλεξάρτηση των ΚΥ, μπορεί συστηματικά να μοντελοποιηθεί μόνο μέσα από μια ολιστική προσέγγιση ασφάλειας, ώστε να αναδειχθούν πιθανοί κίνδυνοι στους οποίους δεν είχε εστιάσει η επιμέρους αποτίμηση επικινδυνότητας. Πρόκειται για μια πολύπλοκη και απαιτητική διαδικασία, που εντάσσεται συνήθως στο πλαίσιο μιας εθνικής στρατηγικής για τις ΚΥ. Μία μέθοδος ανάλυσης είναι να χρησιμοποιηθούν γράφοι επικινδυνότητας, των οποίων οι κόμβοι αποτελούν μία ΚΥ ή ένα σύστημά της,ώστε να περιγραφούν οι αλληλεξαρτήσεις πρώτης τάξεως.



Σχήμα 4 : Παράδειγμα γράφου για την επικινδυνότητα των αλληλεξαρτήσεων μεταξύ κρίσιμων υποδομών

Η μέθοδος αυτή μπορεί να επεκταθεί και πέραν των αλληλεξαρτήσεων πρώτης τάξεως. Ο προσδιορισμός του τύπου της αλληλεξάρτησης μεταξύ κρίσιμων υποδομών, μπορεί να γίνει μέσω της τάξης σύνδεσης (coupling order), όρος που υποδηλώνει την αμεσότητα της σύνδεσης ή την σύνδεση μέσω μιας ή περισσότερων ενδιάμεσων υποδομών κατά έμμεσο τρόπο. Στη τελευταία περίπτωση η τάξη σύνδεσης καλείται νιοστού βαθμού, με το (ν) να σημαίνει τον αριθμό των ενδιάμεσων συνδέσεων.[41] Ξεκινώντας έτσι από την ανάλυση εξαρτήσεων πρώτης τάξης, μοντελοποιούνται στη συνέχεια οι πολλαπλές εξαρτήσεις, που προκαλούν τη μεταφορά μιας διαδοχικής αστοχίας από τη μία ΚΥ στην άλλη, ώστε να αποτιμηθεί η επικινδυνότητα των αλυσίδων εξάρτησης ΚΥ, βάσει της οποίας θα διαμορφωθεί η πολιτική ανθεκτικότητας. Άλλη προσέγγιση συνιστά η μετρική κεντρικότητας γράφων (centrality metrics), που ποσοτικοποιεί τη κρισιμότητα μιας ΚΥ σε σχέση με τις αλληλεξαρτήσεις της από άλλες ΚΥ σε ένα "σύστημα συστημάτων", μετρώντας τη σημασία κάθε κόμβου του γράφου σε σχέση με τους υπόλοιπους.[42]

[40] Pursiainen C.& Kytömaa E. (2023) From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and Resilient Infrastructure, 8:sup1, 85-101 https://doi.org/10.1080/23789689.2022.2128562

[41] Kotzanikolaou P., Theoharidou M.& Gritzalis D. "Assessing n-order dependencies between critical infrastructures" Int. J. of Critical Infrastructures, 2013 https://www.researchgate.net/publication/264815932_Assessing_n-order_dependencies_betweencritical_infrastructures/link/5407089e0cf2bba34c1e8415/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

[42] Γ.Στεργιόπουλος ό.π. Σελ. 650

2.2.4. Τα Βιομηχανικά Συστήματα Ελέγχου (ICS) και οι ευπάθειές τους

Μια περίπτωση εξαρτήσεων και αλληλεξαρτήσεων στο πεδίο των ΚΥ, αποτελούν τα Βιομηχανικά συστήματα ελέγχου (ICS). Πρόκειται για συστήματα λογισμικού και υλικού, που έχουν σχεδιαστεί για να υποστηρίζουν ευρύ φάσμα λειτουργιών ελέγχου και παρακολούθησης των βιομηχανικών διεργασιών. Ενδεικτικά χρησιμοποιούνται σε δίκτυα ηλεκτρικής ενέργειας, εργοστάσια, δίκτυα ύδρευσης και μεταφορές**.** Η μεγαλύτερη υποκατηγορία των ΒΣΕ είναι τα συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA) τα οποία χρησιμοποιούνται για τη συλλογή δεδομένων και τον απομακρυσμένο έλεγχο των διεργασιών των ΒΣΕ.

Τα συστήματα SCADA ενσωματώνουν συστήματα απόκτησης και μετάδοσης δεδομένων καθώς και λογισμικό, ώστε να ελέγξουν κεντρικά πληθώρα εισόδων και εξόδων διαδικασιών. Συλλέγουν πληροφορίες από το πεδίο μέσω αισθητήρων, τις μεταφέρουν σε ένα κέντρο ελέγχου και τις εμφανίζουν στον χειριστή, επιτρέποντάς του έτσι, σε πραγματικό χρόνο, να παρακολουθεί ολόκληρο το σύστημα από μια κεντρική τοποθεσία. Η συλλογή των δεδομένων των αισθητήρων, γίνεται από έξυπνες ηλεκτρονικές συσκευές πεδίου, όπως ο Προγραμματιζόμενος Λογικός Ελεγκτής (PLC).

Τα συστήματα αυτά, αποτελούν δομικό στοιχείο των Κρίσιμων Υποδομών, που στηρίζονται στη λειτουργία τους για την επιχειρησιακή τους ετοιμότητα. Για το λόγο αυτό, η ασφάλειά τους είναι ουσιώδης για τη διασφάλιση της παροχής των κρίσιμων υπηρεσιών και αγαθών των ΚΥ. Η ασφάλεια των ΒΣΕ, ενόψει της αλληλεξάρτησης των ΚΥ και της ενδεχόμενης εκδήλωσης του φαινομένου των διαδοχικών αστοχιών, αποτελεί μέρος της στρατηγικής για την προστασία και την ανθεκτικότητα των ΚΥ. Οι ευπάθειες των συστημάτων αυτών αφορούν :

- Το υλικό (μηχανήματα και συσκευές πεδίου)
- Το Υλικολογισμικό (firmware)
- Το Λογισμικό (έλεγχος του υλικού και εφαρμογές)
- Το Δίκτυο (πληροφοριακό και βιομηχανικό)
- Τις Διεργασίες (λογικές επιθέσεις)

Ο ψηφιακός μετασχηματισμός και η ανάπτυξη των νέων τεχνολογιών του Διαδικτύου των πραγμάτων και των υπηρεσιών, είχε σαν αποτέλεσμα τη μετατροπή των ΒΣΕ από απομονωμένα συστήματα, σε συστήματα διασυνδεδεμένα με το Διαδίκτυο, με μεγαλύτερες δυνατότητες και αυξημένη απόδοση. Ωστόσο η εξέλιξη αυτή των ΒΣΕ, είχε σαν συνέπεια την αύξηση των αλληλεξαρτήσεων με τα δίκτυα επικοινωνίας και την έκθεσή τους σε νέους κινδύνους και απειλές, που έχουν σαν τελικό στόχο την απόκτηση του ελέγχου των ΚΥ που υποστηρίζουν.[43] Με τα νέα τεχνολογικά δεδομένα, τα ΒΣΕ εντάσσονται στο ευρύτερο φάσμα της τεχνολογίας

[43] ENISA, Communication network dependencies for ICS/SCADA Systems, 2016 https://www.enisa.europa.eu/publications/ics-scada-dependencies

επιχειρησιακής λειτουργίας (Operation Technology). Η τεχνολογία OT, περιλαμβάνει όλα τα συστήματα και τις συσκευές που αλληλεπιδρούν με το φυσικό περιβάλλον και με τη χρήση της τεχνολογίας πληροφοριών (IT), το ελέγχουν και επιφέρουν αλλαγές σε αυτό.[44]

Η διαμόρφωση του νέου ψηφιακού περιβάλλοντος για τα συστήματα ΒΣΕ, δημιουργεί σε αυτά ευπάθειες, που οδηγούν σε μη εξουσιοδοτημένη πρόσβαση, κακόβουλο λογισμικό, Denial-of-Service επιθέσεις και γενικότερα κυβερνοαπειλές που δημιουργούν αντίστοιχους κινδύνους για τις ΚΥ. Οι επιθέσεις σε ΒΣΕ έχουν επιπτώσεις όπως διακοπές λειτουργίας, ζημιές σε εξοπλισμό, οικονομικές απώλειες, κλοπή δεδομένων και υπονόμευση της εθνικής ασφάλειας. Από την άλλη πλευρά, τα ΒΣΕ συχνά είναι συστήματα παλιάς τεχνολογίας, ευάλωτα σε επιθέσεις και ασύμβατα με άλλα συστήματα, εμποδίζοντας την ανάπτυξη της διαλειτουργικότητας.

Ο ENISA σε έρευνά του προτείνει την ενίσχυση της κυβερνοασφάλειας των ΒΣΕ και διατυπώνει τις εξής συστάσεις προς τα κράτη μέλη:[45]

- ΄Ενταξη της ασφάλειας των ΒΣΕ στην εθνική στρατηγική κυβερνοασφάλειας
- Ανάπτυξη καλών πρακτικών ειδικά για τον τομέα των ΒΣΕ/ SCADA
- Δημιουργία προτύπων για την ανταλλαγή πληροφοριών μεταξύ κρίσιμων τομέων και κρατών μελών
- Οικοδόμηση επίγνωσης για την κυβερνοασφάλεια ΒΣΕ/SCADA σε όλους τους εμπλεκόμενους φορείς
- Εκπαίδευση και επιμορφωτικά προγράμματα
- Υποστήριξη της έρευνας και των δοκιμών για την κυβερνοασφάλεια των ΒΣΕ/SCADA

Η CISA αντίστοιχα προτείνει ένα κυκλικό σχήμα διαχείρισης επικινδυνότητας των ΒΣΕ, που βασίζεται στις διεργασίες της αναγνώρισης/ανίχνευσης/προστασίας από τις κυβερνοαπειλές και απόκρισης /ανάκαμψης από περιστατικά ασφαλείας. Προωθεί επίσης μια ενοποιημένη στρατηγική, που στηρίζεται σε 4 πυλώνες:

- Συνεργασία μεταξύ των διαχειριστών ΒΣΕ και των αρμόδιων φορέων
- Υψηλό τεχνολογικό επίπεδο για την Κυβερνοασφάλεια
- Δυνατότητα για ανάλυση στο βάθος των δεδομένων και ανταλλαγή πληροφοριών
- Στοχευμένες επενδύσεις για την πρόληψη των επιθέσεων [46]

[44] NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security /https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
[45] ENISA, Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, 2015 https://www.enisa.europa.eu/publications/maturity-levels
[46] CISA SECURING INDUSTRIAL CONTROL SYSTEMS: A UNIFIED INITIATIVE FY 2019—2023 https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

2.3. Σχέδιο ασφαλείας και Διαχείριση επικινδυνότητας στις Κρίσιμες Υποδομές

2.3.1. Η ανάπτυξη Σχεδίου Ασφαλείας (ΣΔΑΠ) στις κρίσιμες Υποδομές

Οι Οδηγίες NIS 2 και CER θεσπίζουν ένα πλέγμα υποχρεώσεων για τις κρίσιμες οντότητες, όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους. Οι κρίσιμες οντότητες, με ευθύνη της ανώτατης διοίκησής τους, οφείλουν να λάβουν τεχνικά, επιχειρησιακά και οργανωτικά μέτρα διαχείρισης επικινδυνότητας, για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες. (*βλ. άρθρα 20,21 NIS 2, 14 NIS*).

Τα μέτρα αυτά πρέπει να ακολουθούν μια ολιστική προσέγγιση, που αποσκοπεί στη προστασία των συστημάτων δικτύου και πληροφοριών, καθώς και του φυσικού τους περιβάλλοντος, από περιστατικά που θα μπορούσαν να θέσουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών. Προκειμένου να διασφαλιστεί η συμμόρφωση με τις παραπάνω απαιτήσεις, συστήνεται από τις Οδηγίες, η υιοθέτηση από τις κρίσιμες οντότητες διεθνών προτύπων, όπως αυτά που περιλαμβάνονται στη σειρά ISO/IEC 27000 (*βλ. πρόταση αρ.79 NIS 2, άρθρο 16 CER*). Στην Οδηγία CER, τονίζεται η σημασία της διαχείρισης επικινδυνότητας από τις κρίσιμες οντότητες, σύμφωνα με τα ιδιαίτερα χαρακτηριστικά των κρίσιμων υποδομών, συνεκτιμώντας όλους τους φυσικούς και ανθρωπογενείς κινδύνους κάθε προελεύσεως, συμπεριλαμβανομένων των κινδύνων διατομεακού και διασυνοριακού χαρακτήρα, σε συνδυασμό με τις αλληλεξαρτήσεις μεταξύ ΚΥ ίδιου ή διαφορετικού τομέα και σε συνάρτηση με ΚΥ της ίδιας γεωγραφικής περιοχής εντός ή εκτός Ε.Ε.

Οι παραπάνω ρυθμίσεις υπογραμμίζουν την υποχρέωση που φέρουν οι κρίσιμες οντότητες να εφαρμόσουν ένα ολοκληρωμένο ΣΔΑΠ, που θα εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των υπηρεσιών τους. Το σχέδιο ασφαλείας, με επίκεντρο την επικινδυνότητα, ενσωματώνει τη στρατηγική, τις πολιτικές, τις διαδικασίες και τα τεχνικά μέτρα για την αποτελεσματική αντιμετώπιση όλων των πτυχών της ασφάλειας μιας ΚΥ. Επιπλέον, πρέπει να ανταποκρίνεται στις ανάγκες της συγκεκριμένης υποδομής και να προβλέπει μέτρα που τεκμηριώνονται από μία μελέτη διαχείρισης επικινδυνότητας.[47] Στις κατευθυντήριες γραμμές για τη συμμόρφωση των ΦΕΒΥ με τις απαιτήσεις της Οδηγίας NIS, ο ENISA συμπεριέλαβε σαν μέτρο ασφαλείας, που αφορά τη διακυβέρνηση, τη κατάρτιση ενός ΣΔΑΠ που θα ενσωματώνει την πολιτική ασφαλείας του ΦΕΒΥ. (βλ. ανωτ.υποσημ.28)

[47] Γ.Στεργιόπουλος ό.π. σελ.655 επ.

Ωστόσο οι ιδιομορφίες των ΚΥ επιβάλλουν τη συνεκτίμηση επιπρόσθετων παραγόντων για την ανάπτυξη ενός σχεδίου ασφαλείας. Η ιδιαιτερότητα των ΒΣΕ και της τεχνολογίας ΟΤ, που αποτελούν αναπόσπαστο τμήμα της λειτουργίας πολλών ΚΥ, δημιουργεί διαφορετικό περιβάλλον από το παραδοσιακό περιβάλλον της τεχνολογίας πληροφοριών, στο οποίο η προστασία από κυβερνοεπιθέσεις αποτελεί κύρια στόχευση. Τα μέτρα ασφαλείας για τα ΒΣΕ, θα πρέπει να ανταποκρίνονται στα επιμέρους χαρακτηριστικά τους, να αντιμετωπίζουν τους νέους κινδύνους κυβερνοασφάλειας και να συνδυάζονται με μέτρα φυσικής ασφάλειας. Από την άλλη, οι εξαρτήσεις και οι αλληλεξαρτήσεις των ΚΥ, είναι στοιχείο που επιδρά στην ασφάλεια πληροφοριών και πρέπει να συνεκτιμηθεί κατά την διαμόρφωση ενός ΣΔΑΠ. Το κυριότερο στοιχείο όμως είναι η έμφαση που πρέπει να δοθεί στη διαθεσιμότητα των υπηρεσιών των ΚΥ και στη διασφάλιση της ανθεκτικότητας.

2.3.2. Η ανθεκτικότητα των Κ.Υ.

΄Οπως προαναφέρθηκε, η νέα Οδηγία CER, αντικατέστησε την έννοια της προστασίας με την έννοια της ανθεκτικότητας, εισάγοντας παράλληλα την έννοια της κρίσιμης οντότητας. Η ανθεκτικότητα (resilience) είναι ευρύτερη, καθώς περιλαμβάνει τόσο τη προστασία των ΚΥ πριν εκδηλωθεί μια απειλή, όσο και τη διαχείριση μιας κρίσης από ένα περιστατικό ασφαλείας και την ανάκαμψη της κρίσιμης οντότητας από αυτό. Η μετάβαση στην ανθεκτικότητα υπαγορεύτηκε από τη παραδοχή ότι στο σύγχρονο τοπίο των απειλών, είναι ουτοπική η επιδίωξη της πλήρους αποφυγής του κινδύνου. Ο όρος αναφέρεται στην υποδομή, αλλά εστιάζει στην οντότητα που τη διαχειρίζεται, με κύριο στοιχείο την επιχειρησιακή της συνέχεια. Αν και δεν υπάρχει ένας κοινά αποδεκτός ορισμός της ανθεκτικότητας, μπορούμε να την ορίσουμε ως την ικανότητα προσαρμογής προκειμένου να αντιμετωπιστεί μια απρόβλεπτη συνθήκη ή περιστατικό. Στη περίπτωση των ΚΥ, σημαίνει την ικανότητα των διαχειριστών των κρίσιμων οντοτήτων να προστατεύουν τα αγαθά της υποδομής, ώστε να παρέχουν αδιάλειπτα τουλάχιστον ένα ελάχιστο όριο των ζωτικών υπηρεσιών της στο κοινό.

Σύμφωνα με το πνεύμα των νέων Οδηγιών, η αξιοπιστία των ΚΥ, συνδέεται άρρηκτα με την ανθεκτικότητα των διαχειριστών τους/κρίσιμων οντοτήτων. ΄Ετσι η ανθεκτικότητα περιλαμβάνει τις διαδικασίες διαχείρισης επικινδυνότητας, αλλά εκτείνεται στο στάδιο της ανάκαμψης, καθώς και σε οργανωσιακά θέματα διαχείρισης των περιστατικών ασφαλείας από την κρίσιμη οντότητα.[48] Η ανθεκτικότητα δεν αποτελεί μια προσέγγιση της διαχείρισης επικινδυνότητας, αλλά ενσωματώνει όλα τα μέτρα ασφαλείας που πρέπει να εφαρμοστούν για να εξασφαλιστεί η λειτουργία μιας ΚΥ. Αποτελεί μια έννοια που εφαρμόζεται τόσο στα αγαθά και τα δίκτυα μιας ΚΥ, όσο και σε υψηλότερο επίπεδο, στα συστήματα συστημάτων (Systems of Systems), όπου

[48] L. Petersen a, D. Lange b, M. Theocharidou "Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators"2020
https://doi.org/10.1016/j.ress.2020.106872

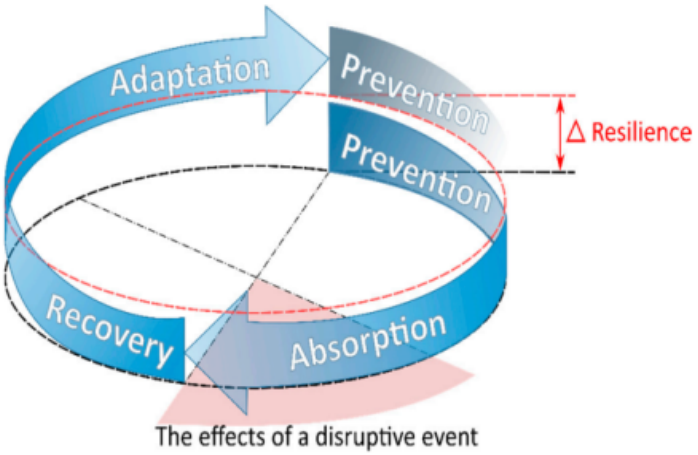
το ζητούμενο είναι η συνέχιση της λειτουργίας των υποδομών, μέσω της ενίσχυσης της ανθεκτικότητας.

Διαμορφώνεται επομένως ένας κύκλος ανθεκτικότητας, που αποτελείται από τις εξής φάσεις:

Φάση	*Ιδιότητες*	*Στόχοι*
1. Αποφυγή περιστατικού ασφαλείας (Prevention)	Αντίσταση στις απειλές (Resistance)	Συνεχής προετοιμασία για μελλοντικά περιστατικά διατάραξης
2. Απορρόφηση των επιπτώσεων του περιστατικού αμέσως μόλις συμβεί αυτό (Absorption)	Ευρωστία συστημάτων υποδομής (Robustness)	Μη διατάραξη της ροής παροχής των ζωτικών υπηρεσιών
3. Ανάκαμψη (Recovery)	΄Αμεση ενεργοποίηση οργανωσιακών διαδικασιών και χρήση εφεδρικών/ διαθέσιμων υλικών/οικονομικών μέσων /ανθρώπινου κεφαλαίου (Redundancy, Resourcefulness, Rapidity)	Δυνατότητα άμεσης επαναφοράς σε επαρκές επίπεδο λειτουργίας των στοιχείων που προσβλήθηκαν
4. Προσαρμογή της οντότητας στο περιστατικό (Adaptation)	Πολιτική Διοίκησης	Ικανότητα για αντιμετώπιση παρόμοιων περιστατικών στο μέλλον (αποτίμηση επικινδυνότητας, καινοτομία και εκπαίδευση)

Η πρώτη φάση της ανθεκτικότητας, ανταποκρίνεται στη προσέγγιση της προληπτικής προστασίας, ενώ οι επόμενες στη προσέγγιση της κατασταλτικής αντίδρασης. Αφορούν την τεχνολογική και την οργανωσιακή διάσταση της ανθεκτικότητας, πρέπει όμως να συνυπολογιστεί ότι λόγω του αντικτύπου των επιπτώσεων, η ανθεκτικότητα έχει παράλληλα κοινωνική και οικονομική διάσταση. Οι διαστάσεις αυτές, συνδυάζονται με τις βασικές ιδιότητες της ανθεκτικότητας που συνοψίζονται στα 4R, Robustness, Redundancy, Resourcefulness, Rapidity. [49]

[49] Rehak David et al. “Critical Entities Resilience Failure Indication” Nov.2023 https://www.sciencedirect.com/science/article/pii/S0925753523003132



Σχήμα 5:Μέτρηση της αύξησης της ανθεκτικότητας στο κύκλο ζωής της, μέσω της σύγκρισης της αρχικής και της ενισχυμένης ανθεκτικότητας [50]

Η εστίαση στην ανθεκτικότητα αντί για την επικινδυνότητα, καθώς και η μετατόπιση από τις υποδομές και τα αγαθά, στις οντότητες, έθεσε ερωτήματα αναφορικά με τη διαδικασία αποτίμησης της ανθεκτικότητας. Από τη θεωρία προτείνονται λύσεις μέτρησης της ανθεκτικότητας, μέσω ενδεικτικών μετρικών (indicators), αφού αντιμετωπιστούν οι προκλήσεις της αποτύπωσης των πολλαπλών αβεβαιοτήτων και αλληλεξαρτήσεων των ΚΥ. Όσο περιπλέκεται το τοπίο των απειλών, που δυνητικά εκδηλώνονται ταυτόχρονα και σε διαφορετικούς συνδυασμούς, τόσο γίνεται δυσκολότερη η διαχείριση επικινδυνότητας στις ΚΥ. Ωστόσο στο επίκεντρο δεν βρίσκεται η αποτροπή των απειλών, αλλά ο χρόνος αντίδρασης και επαναφοράς σε λειτουργία της ΚΥ.

Η διαμόρφωση νέων μεθοδολογιών και προτύπων που ενσωματώνουν προσεγγίσεις της αποτίμησης επικινδυνότητας με βάση την ανθεκτικότητα, είναι μια τάση που βρίσκεται στο προσκήνιο.[51] Στηρίζονται στη μοντελοποίηση της ανθεκτικότητας, των αλληλεξαρτήσεων και του αντικτύπου των περιστατικών, σε συνάρτηση με τον χρόνο. Προκειμένου να μοντελοποιηθεί η αποτίμηση της ανθεκτικότητας πρέπει να κατανοηθούν οι παράγοντες που καθορίζουν τις παραπάνω ιδιότητές της, καθώς και οι παράγοντες που τις επηρεάζουν. Προτείνονται νέα εργαλεία και τεχνικές μοντελοποίησης για πολύπλοκα αλληλεξαρτώμενα συστήματα, που περιλαμβάνουν εξειδικευμένες μεθόδους μέτρησης και προσδιορισμού του βαθμού ανθεκτικότητας. Σαν έξοδος της διαδικασίας αποτίμησης ανθεκτικότητας, θα μπορούσε να είναι

[50] Rehak David et al. “Complex Approach to Assessing Resilience of Critical Infrastructure Elements”,March 2019,International Journal of Critical Infrastructure Protection 25 https://www.researchgate.net/publication/332084463_Complex_Approach_to_Assessing_Resilience_of_Critical_Infrastructure_Elements

[51] Theocharidou, M., Galbusera, L., & Giannopoulos, G. (2018). Resilience of critical infrastructure systems: Policy, research projects and tools. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems. Lausanne, CH: EPFL International Risk Governance Center. *Theocharidou-et-al-for-IRGC-Resilience-Guide-Vol-2-2018.pdf

ένας δείκτης που προσδιορίζει τη μεταβαλλόμενη λειτουργικότητα των κρίσιμων αγαθών και υποδομών, σε σχέση με τον χρόνο ανάκαμψης από σενάρια κινδύνου. [52]

Παρόλα αυτά, η αποτίμηση επικινδυνότητας, αποτελεί ένα πεδίο με ισχυρή προτυποποίηση και πιστοποίηση, με το οποίο είναι εξοικειωμένες οι κρίσιμες οντότητες. Οι νέες Οδηγίες, δεν απομακρύνονται από αυτό και τα δημοφιλή Πρότυπα, Πλαίσια και μεθοδολογίες, στα οποία άλλωστε παραπέμπουν. Τα διεθνή Πρότυπα ISO 27001 και 27005, συνεχίζουν να αποτελούν το σταθερό σημείο αναφοράς. Η διαχείριση της επικινδυνότητας, δεν σημαίνει ότι λειτουργεί ανταγωνιστικά με τη διαχείριση ανθεκτικότητας, αλλά μπορεί να θεωρηθεί μία ουσιαστική πτυχή της.[53]

2.3.3. Μεθοδολογίες αποτίμησης επικινδυνότητας στις Κρίσιμες Υποδομές

Οι παραπάνω ιδιαιτερότητες της διαχείρισης επικινδυνότητας των ΚΥ, απαιτούν αντίστοιχη προσαρμογή των μεθοδολογιών και των εργαλείων αποτίμησης. Οι μεθοδολογίες αποτίμησης επικινδυνότητας των ΚΥ, εντάσσονται σε δύο μεγάλες κατηγορίες: Τις μεθοδολογίες ανά τομέα, που ασχολούνται ειδικά με ένα συγκεκριμένο τομέα ΚΥ και τις μεθοδολογίες συστημάτων, που ασχολούνται με αλληλεξαρτώμενες υποδομές, αντιμετωπίζοντάς τις σαν διασυνδεδεμένα δίκτυα. Διαφέρουν επίσης ως προς το επίπεδο εφαρμογής τους και διακρίνονται σε προσεγγίσεις σε επίπεδο αγαθών (asset level) , σε επίπεδο συστήματος και σε επίπεδο συστήματος συστημάτων (SoS). Το επίπεδο SoS αφορά μεγαλύτερου μεγέθους υποδομές, που λειτουργούν σε εθνικό και διεθνές επίπεδο, ενώ η προσέγγιση της αποτίμησης σε επίπεδο αγαθών, είναι αυτή που συναντάται συχνότερα, σε συνδυασμό με την αποτίμηση ανά τομέα και περιλαμβάνει τον διαχωρισμό των αγαθών σε κρίσιμα και μη κρίσιμα. Η διατομεακή προσέγγιση σε συνδυασμό με την προσέγγιση SoS, είναι τα στοιχεία που ενσωματώνουν πολλές νέες μεθοδολογίες αποτίμησης επικινδυνότητας των ΚΥ.

Υπάρχει ποικιλία μεθοδολογιών όσον αφορά τις προσεγγίσεις, τα εργαλεία και τις τεχνικές. Μπορούν διακριθούν σε:

➛Μεθοδολογίες που βασίζονται στον σκοπό που εξυπηρετούν και εστιάζουν σε ένα στάδιο ή σε περισσότερα του πλαισίου διαχείρισης επικινδυνότητας που υποστηρίζουν.
➛Τεχνικές προσεγγίσεις, όπου γίνεται χρήση μαθηματικών μοντέλων για τη προσομοίωση της συμπεριφοράς των συστημάτων των ΚΥ και ειδικότερα:

- Εμπειρική προσέγγιση→ Ανάλυση με βάση ιστορικά δεδομένα

[52] S.Argyroudis et al. “Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets” 2020- ScienceDirect https://doi.org/10.1016/j.scitotenv.2020.136854
[53] Pursiainen C.& Kytömaa E. (2023) From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and Resilient Infrastructure ό.π.

- Προσέγγιση Δυναμικής ανάλυσης του συστήματος → Top down ανάλυση σύνθετων συστημάτων με αλληλεξαρτήσεις μέσω βρόχων που υποδεικνύουν συνδέσεις και κατευθύνσεις των επιπτώσεων μεταξύ κρίσιμων υποδομών.
- Προσέγγιση οντοτήτων→ Bottom up αθροιστική ανάλυση της συμπεριφοράς μικρότερων αυτόνομων οντοτήτων που αλληλεπιδρούν, μιμούμενες τον τρόπο που θα αντιδρούσαν μέσω συστήματος πολλαπλών παραγόντων που αντιπροσωπεύουν μια υποδομή, ένα σύστημα ή ένα αγαθό.
- Προσέγγιση δικτύων → Μοντελοποίηση ΚΥ σαν δικτύου του οποίου οι κόμβοι αντιπροσωπεύουν τα στοιχεία της υποδομής και οι σύνδεσμοι τις μεταξύ τους σχέσεις

➛΄Αλλου τύπου προσεγγίσεις με βάση την οικονομική θεωρία, τη προσομοίωση πραγματικού χρόνου, τις μαθηματικές εξισώσεις.[54]

Στη πλειοψηφία τους οι μεθοδολογίες αποτίμησης επικινδυνότητας στις ΚΥ έχουν σαν βάση τις μεθοδολογίες που ακολουθούν οι μεμονωμένοι οργανισμοί, όπου υπάρχει γνώση της αρχιτεκτονικής και των αρχών λειτουργίας του συστήματος. Όταν όμως συνδέονται πολλά συστήματα μαζί, οι περίπλοκες μεταξύ τους αλληλεπιδράσεις μπορούν να αναλυθούν και να μοντελοποιηθούν, μόνο σύμφωνα με μια ολιστική οπτική από τη σκοπιά της ανθεκτικότητας. [55]

Στο πλαίσιο του προγράμματος της Ευρωπαϊκής Επιτροπής για την προστασία των ΚΥ (EPCIP), το ερευνητικό κέντρο της, Joint Research Center, παρουσίασε μια μεθοδολογική πρόταση για την αποτίμηση επικινδυνότητας στις ΚΥ, η οποία εστιάζει στις επιπτώσεις των διαδοχικών συνεπειών ενός περιστατικού διατάραξης, χωρίς να πραγματοποιεί λεπτομερή ανάλυση κάθε αγαθού της υποδομής. Τα δύο βασικά χαρακτηριστικά της μεθοδολογίας είναι:

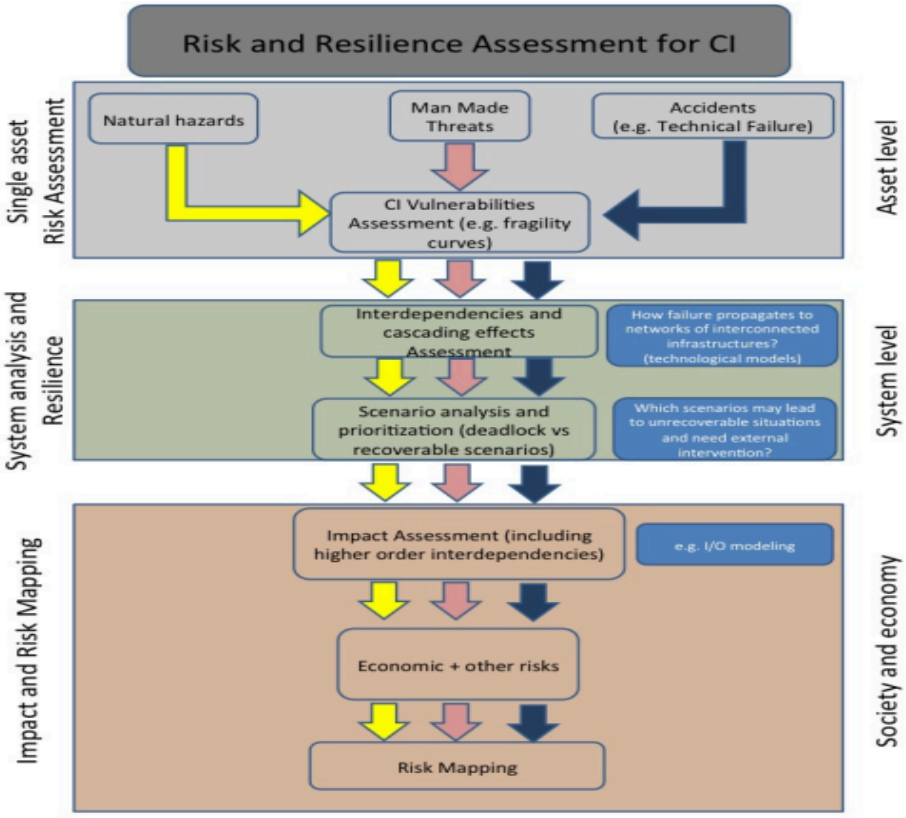
- Η αντιμετώπιση των ΚΥ σαν σύνθετων τεχνοοικονομικών συστημάτων και η μοντελοποίηση της συμπεριφοράς τους σε δύο επίπεδα, το τεχνολογικό (μοντελοποίηση αλληλεξαρτήσεων) και το οικονομικό (μοντελοποίηση πολυδιάστατων οικονομικών και κοινωνικών επιπτώσεων).
- Η αποτίμηση της επικινδυνότητας συνδυαστικά με την αποτίμηση της ανθεκτικότητας για να κατανοηθεί η δυναμική συμπεριφορά της ΚΥ, η σταθερότητα των συστημάτων της και η δυνατότητα ανάκαμψης.

Στόχος της μεθοδολογίας είναι η ανάλυση των αλληλεξαρτήσεων σε συνάρτηση με τις οικονομικές επιπτώσεις των αστοχιών της ΚΥ, η οποία μοντελοποιείται με τη τεχνική δικτύου, σαν ένα δίκτυο διασυνδεδεμένων κόμβων.

---

[54] Stergiopoulos G., Vasilellis R., Lykou G, Kotzanikolaou P., Gritzalis D. “Classification and Comparison of Critical Infrastructure Protection Tools” 10th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2016, Arlington, VA, USA pp.239-255, https://inria.hal.science/hal-01614869

[55] Giannopoulos G, Filippini R, Schimmer M. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. EUR 25286 EN. Luxembourg Publications Office of the European Union; 2012, JRC70046 https://publications.jrc.ec.europa.eu/repository/handle/JRC70046



Σχήμα 6:Σχηματική αναπαράσταση της προτεινόμενης μεθοδολογίας αποτίμησης επικινδυνότητας και ανθεκτικότητας στις Κρίσιμες Υποδομές [56]

Πολιτική της ΕΕ είναι η διαμόρφωση μιας κοινής μεθοδολογικής βάσης στην ΕΕ για την αποτίμηση επικινδυνότητας στις ΚΥ. Δείγμα της πολιτικής αυτής είναι η ανάπτυξη από το 2018 της πλατφόρμας GRRASP (Geospatial Risk and Resilience Assessment Platform) που παρέχει στα κράτη μέλη δεδομένα για την ανάλυση της διατάραξης της λειτουργίας των ΚΥ και την ενίσχυση της ανθεκτικότητας σε φυσικές καταστροφές, μέσα από την μοντελοποίηση των κινδύνων. Στο πλαίσιο αυτό, το JRC επισημαίνει στις έρευνές του, την ανάγκη για μοντελοποίηση και προσομοίωση με την ανάπτυξη μιας κοινής εργαλειοθήκης. Προτείνει την υιοθέτηση εναρμονισμένης κλίμακας επιπτώσεων στη διαδικασία αποτίμησης επικινδυνότητας, αναγνώριση κοινών διασυνοριακών σεναρίων και συνεργασία δημόσιου και ιδιωτικού τομέα. Σημαντικό στοιχείο μιας κοινής μεθοδολογίας σε ευρωπαϊκό επίπεδο, θα πρέπει να είναι η δυναμική ανάλυση, καθώς τα επίπεδα λειτουργικότητας των ΚΥ και οι αλληλεξαρτήσεις τους μεταβάλλονται στο χρόνο. [57]

[56] G. Giannopoulos et al. " Risk Assessment Methodology for Critical Infrastructure Protection" 2013 European Commission Joint Research Centre Risk Assessment Methodology for Critical Infrastructure ... JRC Publications Repository https://publications.jrc.ec.europa.eu › JRC78292

[57] Theocharidou M, Giannopoulos G. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. EUR 27332. Luxembourg (Luxembourg): Publications Office of the European Union; 2015. JRC96623 https://dx.doi.org/10.2788/621843

2.3.4. Αποτίμηση επικινδυνότητας Κυβερνοασφάλειας στις ΚΥ

2.3.4.1. Το Πλαίσιο της CSA Singapore

Στο πεδίο της Κυβερνοασφάλειας, δημοφιλές είναι το Πλαίσιο για την αποτίμηση επικινδυνότητας στις ΚΥ πληροφοριών της Αρχής Κυβερνοασφάλειας της Σιγκαπούρης (CSA Singapore), που δημοσιεύτηκε το 2019.[58] Στόχος του είναι η παροχή καθοδήγησης στους διαχειριστές των ΚΥ, για την διεξαγωγή μιας αποτελεσματικής διαδικασίας που περιλαμβάνει την αναγνώριση, την αποτίμηση και την αντιμετώπιση της επικινδυνότητας. Τα ειδικότερα προβλήματα που αντιμετωπίζει μια ΚΥ στην αποτίμηση της επικινδυνότητας της Κυβερνοασφάλειας, είναι σύμφωνα με το Πλαίσιο τα εξής:

- Αδύναμα και αόριστα σενάρια κινδύνου
- Αναγνώριση κινδύνου μέσω μιας προσέγγισης συμμόρφωσης που αρκείται στη συμπλήρωση ερωτηματολογίων (checklist behaviour)
- Απουσία ανοχής στον κίνδυνο για την κυβερνοασφάλεια (μη ενσωμάτωση του κινδύνου κυβερνοασφάλειας στο πρόγραμμα διοίκησης επικινδυνότητας του οργανισμού)
- Καθορισμός πιθανότητας κινδύνου με βάση ιστορικά γεγονότα. Στον τομέα της κυβερνοασφάλειας η πιθανότητα ενός περιστατικού ασφαλείας είναι ανεξάρτητη από τη συχνότητα παρελθόντων συμβάντων
- Αντιμετώπιση επικινδυνότητας με μέτρα και ελέγχους που δεν σχετίζονται άμεσα με την αιτία του προβλήματος.

Για τον καθορισμό του περιεχομένου, χρησιμοποιούνται έννοιες όπως απειλή, ευπάθεια, πιθανότητα και επίπτωση που είναι συμβατές με την ορολογία άλλων δημοφιλών προτύπων. Το επίπεδο επικινδυνότητας χαρακτηρίζεται από χαμηλό έως πολύ υψηλό σε μια κλίμακα αντιστοίχισης με το επίπεδο ανοχής στον κίνδυνο (risk tolerance), ενώ παράλληλα ορίζονται ρόλοι και αρμοδιότητες για τα εμπλεκόμενα μέρη. Βασικά σημεία της διαδικασίας είναι η αναγνώριση των κρίσιμων αγαθών και η κατασκευή ολοκληρωμένων σεναρίων κινδύνου. Η αποτίμηση περιλαμβάνει τρία βήματα:

[58] CSA Singapore Guide to conducting cybersecurity risk assessment for critical infrastructure , Feb.2021 https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_ttps://data.europa.eu/doi/10.2788/621843

Βήματα	*Καθήκοντα (Tasks)*	*Κατηγορίες/ Κλίμακες Μέτρησης 5 επιπέδων*
1. Αναγνώριση (Identification)	• Αναγνώριση αγαθών➔ • Αναγνώριση απειλών και μοντελοποίηση επιθέσεων • Κατασκευή σεναρίων κινδύνου με 4 στοιχεία ➔	1. Κρίσιμα αγαθά *(Crown jewels)* 2. Υποστηρικτικά αγαθά *(Stepping stones)* —---------- 1.Αγαθό 2.Απειλή 3.Ευπάθεια 4. Συνέπεια
2. Ανάλυση (Analysis)	• Καθορισμός πιθανότητας ➔ • Καθορισμός επιπτώσεων στην εμπιστευτικότητα-ακεραιότητα-διαθεσιμότητα πληροφοριών➔	Σπάνια (1) - Πολύ υψηλή (5) Αμελητέες (1) - -Πολύ σοβαρές (5)
3. Αξιολόγηση (Evaluation)	• Καθορισμός και προτεραιοποίηση επικινδυνότητας➔ • Τεκμηρίωση	Πίνακας συνδυασμού πιθανότητας-επιπτώσεων: Αμελητέα (1) - Πολύ σοβαρή (5)

Τα αγαθά διαχωρίζονται σε "κοσμήματα του Στέμματος" που αναφέρονται στα αγαθά που παίζουν κρίσιμο ρόλο για την επίτευξη των επιχειρησιακών στόχων, στα οποία υπάρχει μεγάλη πιθανότητα να κατευθυνθούν οι επιθέσεις, ενώ τα υπόλοιπα, είναι αγαθά των οποίων θα επιδιώξουν να λάβουν τον έλεγχο, προκειμένου να προσεγγίσουν τα "κοσμήματα". Η απόκριση στον κίνδυνο, που ακολουθεί την αποτίμηση, περιλαμβάνει 4 δυνατότητες, την αποδοχή, την αποφυγή, τη μεταβίβαση και τον μετριασμό του κινδύνου. Δεν υπάρχουν προβλέψεις αναφορικά με τις διεργασίες της παρακολούθησης και των ελέγχων, τομείς στους οποίους μπορούν να εφαρμοστούν συμπληρωματικά άλλα Πρότυπα. Γενικότερα, το Πλαίσιο, μπορεί να χρησιμοποιηθεί εύκολα σε συνδυασμό με δημοφιλή πλαίσια και πρότυπα για την αναγνώριση, ανάλυση και αξιολόγηση κινδύνων στον κυβερνοχώρο.[59]

[59] ENISA Compendium of Risk Management Frameworks with potential Interoperability 2022 σελ.28

2.3.4.2. Το Πλαίσιο NIST

Στις ΗΠΑ, λόγω των αυξανόμενων απειλών στο πεδίο της Κυβερνοασφάλειας, το 2013 εκδόθηκε Προεδρική Εντολή προς το Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) να αναπτύξει ένα Πλαίσιο - βάση για το πρόγραμμα κυβερνοασφάλειας των ΚΥ. Το Ινστιτούτο δημοσίευσε το Πλαίσιο για την Κυβερνοασφάλεια (CSF Version 1.0) το 2014, το οποίο στην μεταγενέστερη έκδοσή του το 2018 V.1.1., εξειδικεύτηκε ως Πλαίσιο για τη βελτίωση της Κυβερνοασφάλειας στις ΚΥ. [60] Ήδη στις 26-2-2024, το NIST προχώρησε σε νέα έκδοση του Πλαισίου (CSF 2.0), η οποία δεν περιορίζεται πλέον στις κρίσιμες υποδομές, αλλά επεκτείνεται σε κάθε είδους οργανισμό. [61]

Στο Πλαίσιο προτείνεται η χρήση βασικών λειτουργιών (core functions), βαθμίδων (Tiers) και Προφίλ (Profiles), για την κατανόηση και αποτίμηση, προτεραιοποίηση και επικοινωνία του κινδύνου κυβερνοασφάλειας. Η νέα έκδοση, εκτός από τις υπάρχουσες λειτουργίες (Αναγνώριση- Προστασία-Ανίχνευση-Απόκριση- Ανάκαμψη), εισάγει μια νέα λειτουργία, τη διακυβέρνηση, δίνοντας ιδιαίτερη βαρύτητα στην χάραξη μιας στρατηγικής για τη διαχείριση της επικινδυνότητας στη Κυβερνοασφάλεια, η οποία πρέπει με τη καθοδήγηση μιας ισχυρής ηγεσίας, να ενσωματωθεί στη συνολική διαχείριση της επικινδυνότητας του οργανισμού. Έμφαση υπάρχει παράλληλα στην επικοινωνία και τη ροή πληροφοριών μεταξύ των οργανωσιακών επιπέδων του οργανισμού (Executives/Managers/Practitioners). Οι λειτουργίες αναφέρονται σε όλο τα φάσμα της τεχνολογίας πληροφοριών του οργανισμού, περιλαμβάνοντας το Διαδίκτυο των Πραγμάτων και την τεχνολογία επιχειρησιακής λειτουργίας (IoT/OT). Για διευκόλυνση της εφαρμογής του Πλαισίου, παραπέμπει σε επιπρόσθετες ψηφιακές πηγές, όπως σύντομους οδηγούς (QSGs), παραδείγματα εφαρμογών, ενημερωτικές αναφορές, καθώς και ένα νέο ψηφιακό εργαλείο (reference tool).[62]

[60] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 April 16, 2018 https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
[61] The NIST Cybersecurity Framework (CSF) 2.0 National Institute of Standards and Technology, Feb 26, 2024 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[62] NIST Releases Version 2.0 of Landmark Cybersecurity Framework, Feb 26, 2024 https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

Σχήμα 7:Οι λειτουργίες του Πλαισίου CSF 2.0

Οι βαθμίδες αντιπροσωπεύουν την πρόοδο ενός οργανισμού στη διαχείριση του κινδύνου κυβερνοασφάλειας. Κυμαίνονται από τη βαθμίδα 1 (Μερική) έως 4 (Προσαρμοστική) και αντικατοπτρίζουν έναν αυξανόμενο βαθμό επάρκειας του οργανισμού στην αντιμετώπιση του κινδύνου. Αντίστοιχα τα προφίλ αντιπροσωπεύουν τον ειδικό τρόπο με τον οποίο το Πλαίσιο εντάσσεται στον οργανισμό ανάλογα με τις οργανωσιακές ανάγκες και τους στόχους του και διακρίνονται στα τρέχοντα Προφίλ και στα Προφίλ στοχοθεσίας (Current/Target Profiles). Το νέο Πλαίσιο είναι ευέλικτο, καθώς μπορεί να εφαρμοστεί σε οποιονδήποτε οργανισμό και εναρμονίζεται με τα δημοφιλή Πρότυπα και Πλαίσια. Μπορεί επίσης να συνδυαστεί με Πλαίσια όπως το COBIT για να εισαχθεί η Κυβερνοασφάλεια στο ευρύτερο πεδίο διακυβέρνησης και διοίκησης του οργανισμού.[63] Προτείνει τη διαχείριση επικινδυνότητας από τους κινδύνους του κυβερνοχώρου, ανάλογα με τις ειδικές ανάγκες κάθε οργανισμού και παρέχει μια κοινή βάση, ώστε να ενισχύσει την επικοινωνία μεταξύ των ενδιαφερομένων μερών όσον αφορά την κυβερνοασφάλεια.

2.3.5. Το Σχέδιο προστασίας Κ.Υ. των ΗΠΑ (NIPP)

Τα σύνθετα ζητήματα των ΚΥ καθιστούν απαραίτητη την ανάπτυξη μιας ολοκληρωμένης στρατηγικής και την υιοθέτηση ενός σχεδίου για την προστασία των ΚΥ σε εθνικό επίπεδο. Χαρακτηριστικό παράδειγμα τέτοιου σχεδίου είναι το Σχέδιο προστασίας ΚΥ των ΗΠΑ (National Infrastructure Protection Plan NIPP 2013), που έχει εκδώσει το Υπουργείο Εσωτερικών (Department Homeland Security), το οποίο αποτελεί επικαιροποίηση του σχεδίου προστασίας του 2009, σύμφωνα με την Προεδρική Οδηγία 21 (PPD 21) του 2013.[64] Η δομή του σχεδίου περιλαμβάνει το όραμα και τους στόχους του, την περιγραφή του περιβάλλοντος των

[63] Witte G., Connecting COBIT 2019 to the NIST Cybersecurity Framework
Connecting COBIT 2019 to the NIST Cybersecurity Framework (isaca.org)

[64] CISA NIPP 2013 Partnering for Critical Infrastructure Security and Resilience
https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

ΚΥ (επικινδυνότητα/πολιτικές/ λειτουργία), τις θεμελιώδεις αρχές, το Πλαίσιο διαχείρισης της επικινδυνότητας και τέλος τις ενέργειες που πρέπει να αναληφθούν (call to action).

Το σχέδιο εστιάζει στη διαχείριση επικινδυνότητας, σαν τη βάση για την ασφάλεια και την ανθεκτικότητα των ΚΥ. Πρωταρχικός στόχος του επικαιροποιημένου σχεδίου, είναι η ανθεκτικότητα των ΚΥ, που καθορίζονται κατά τομείς (βλ.παραπάνω κεφ.2.2.2.), ώστε να εξασφαλιστεί η αδιάλειπτη παροχή των ζωτικών υπηρεσιών τους. Δίνει έμφαση στην ενίσχυση της ανθεκτικότητας με τη λήψη επιχειρηματικών αποφάσεων που βασίζονται στην αποτίμηση επικινδυνότητας. Οι διαχειριστές των ΚΥ ενθαρρύνονται να επενδύσουν στην επιχειρησιακή συνέχεια και την ενίσχυση της δυνατότητας γρήγορης ανάκαμψης μετά από περιστατικά.[65]

Ενσωματώνει σε όλη τη διαδικασία διαχείρισης επικινδυνότητας την Κυβερνοασφάλεια, προβλέπει την εφαρμογή ειδικών Πλαισίων Κυβερνοασφάλειας και διεργασιών όπως ασκήσεις, αναφορές και διαμοιρασμό πληροφοριών για περιστατικά κυβερνοασφάλειας. Προβάλλει τη σημασία της συνεργασίας ιδιωτικού και δημόσιου τομέα, αλλά και τη διασυνοριακή συνεργασία. Για το λόγο αυτό, καθορίζει ένα πλέγμα ρόλων και αρμοδιοτήτων ιδιωτικών και κυβερνητικών φορέων, που συνεργάζονται σε ομοσπονδιακό και τοπικό επίπεδο, ανά τομέα και διατομεακά.

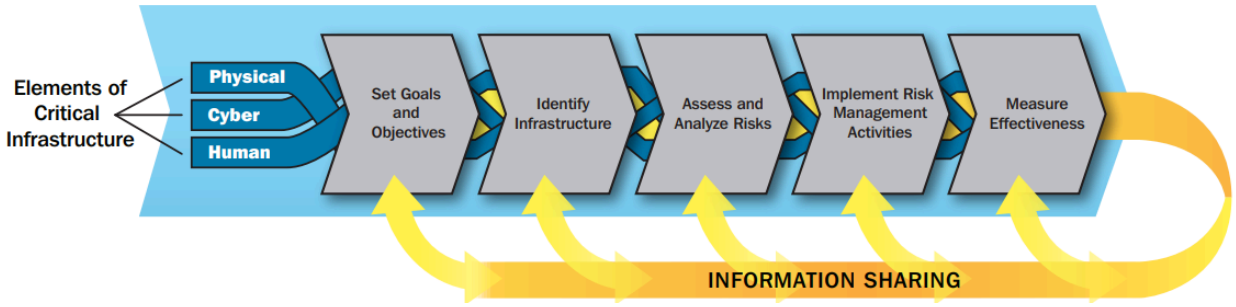
Οι στρατηγικοί στόχοι του Σχεδίου NIPP συνοψίζονται ως εξής:

- Διαχείριση επικινδυνότητας μέσω των διαδικασιών αποτίμησης και ανάλυσης των απειλών, των ευπαθειών και των συνεπειών για τις κρίσιμες υποδομές
- Ασφάλεια των κρίσιμων υποδομών έναντι απειλών (ανθρώπινων, φυσικών και κυβερνοχώρου) μέσω της μείωσης της επικινδυνότητας, λαμβάνοντας υπόψη το κόστος και τα οφέλη των επενδύσεων στην ασφάλεια.
- Ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών με ελαχιστοποίηση των αρνητικών συνεπειών των περιστατικών και εφαρμογή αποτελεσματικών μέτρων ανταπόκρισης για τη διάσωση της ανθρώπινης ζωής και την ανάκαμψη των ζωτικών υπηρεσιών.
- Διαμοιρασμός πληροφοριών στη κοινότητα των κρίσιμων υποδομών για την επίγνωση της επικινδυνότητας
- Προώθηση της μάθησης και της προσαρμογής κατά τη διάρκεια και μετά από ασκήσεις και περιστατικά.

Στο Πλαίσιο διαχείρισης επικινδυνότητας που προβλέπεται στο NIPP, αναγνωρίζονται τα τρία στοιχεία των ΚΥ που αφορούν τις φυσικές απειλές, τις ανθρώπινες απειλές και τις απειλές του κυβερνοχώρου, τα οποία ενσωματώνονται σε όλα τα στάδια. Η λήψη αποφάσεων αναφορικά με

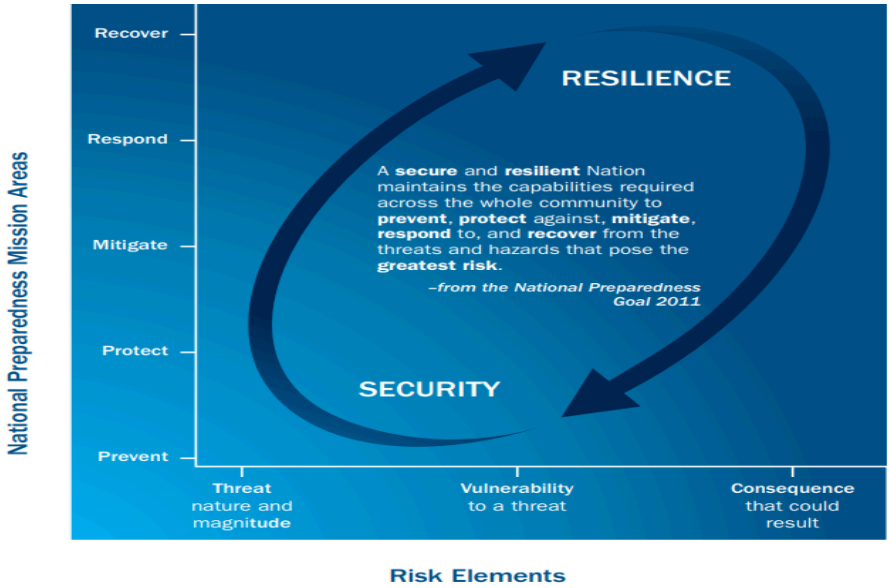
[65] CISA Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Incorporating-Resilience-into-CI-Projects-508.pdf

τις δραστηριότητες διαχείρισης επικινδυνότητας, εξαρτάται από τις επιλογές που θα εφαρμοστούν στο πεδίο του μετριασμού του κινδύνου. Παράλληλα, το σχέδιο τονίζει σταθερά τη σημασία συνεχούς ροής και διαμοιρασμού πληροφοριών σε όλα τα στάδια. Για την αποτίμηση και ανάλυση επικινδυνότητας είναι απαραίτητη η έγκαιρη και αξιόπιστη πληροφόρηση σχετικά με τις απειλές, τις ευπάθειες και τις συνέπειες ενός περιστατικού. Οι δραστηριότητες διαχείρισης επικινδυνότητας περιλαμβάνουν την αναγνώριση/ ανίχνευση/προετοιμασία για τους κινδύνους και τις απειλές, μείωση των ευπαθειών και μετριασμό των συνεπειών.



Σχήμα 8:Πλαίσιο NIPP διαχείρισης επικινδυνότητας στις Κρίσιμες Υποδομές

Οι πέντε διεργασίες που συνιστούν τη διαχείριση επικινδυνότητας (risk management activities) είναι: α) η αποφυγή που αφορά τις απειλές, β) η προστασία που αφορά τις ευπάθειες, γ) η απόκριση και η ανάκαμψη που αφορούν τις συνέπειες και δ) ο μετριασμός που αναφέρεται και στις τρεις παραπάνω έννοιες (απειλή-ευπάθεια-συνέπειες).



Σχήμα 9: Διεργασίες διαχείρισης επικινδυνότητας Κρίσιμων Υποδομών

Οι αρχές του σχεδίου (core tenets) όσον αφορά την διαχείριση επικινδυνότητας είναι:

- Συντονισμός και κοινές πρακτικές για την αναγνώριση και διαχείριση της επικινδυνότητας
- Κατανόηση και αντιμετώπιση επικινδυνότητας που οφείλεται στις εξαρτήσεις και αλληλεξαρτήσεις των ΚΥ
- Ασφάλεια και ανθεκτικότητα από το σχεδιασμό των αγαθών/συστημάτων/δικτύων
- Συνεργασία μεταξύ των φορέων της κοινότητας των ΚΥ
- Συνεργασία σε τοπικό/ ομοσπονδιακό επίπεδο του δημοσίου και ιδιωτικού τομέα
- Συνεργασία/παροχή βοήθειας/ συμφωνίες σε διασυνοριακό επίπεδο

Μεταξύ των ενεργειών που πρέπει να αναληφθούν, είναι η ανάλυση των αλληλεξαρτήσεων των ΚΥ του ιδίου και διαφορετικών τομέων καθώς και των διαδοχικών συνεπειών που σχετίζονται με αυτές, η αποτίμηση της επικινδυνότητάς τους και η απόκριση τόσο κατά τη διάρκεια, όσο και μετά τα περιστατικά ασφαλείας. Το σχέδιο υποστηρίζει την προτυποποίηση των διεργασιών και την ανάπτυξη της διαλειτουργικότητας των προτύπων, ώστε να υπάρχει ένα κοινό περιβάλλον απαιτήσεων και δεδομένων, στο οποίο διευκολύνεται ο διαμοιρασμός πληροφοριών μεταξύ των κρίσιμων οντοτήτων.

Ωστόσο το σχέδιο NIPP δεν ορίζει μια ενιαία μεθοδολογία ανάλυσης επικινδυνότητας, ώστε να είναι δυνατή η σύγκριση μεταξύ αγαθών και τομέων, καθώς και μία κοινή μετρική, που είναι το δομικό στοιχείο μιας ολοκληρωμένης στρατηγικής. Παρά τις προσπάθειες στη κατεύθυνση αυτή, εφαρμόζεται πληθώρα μεθοδολογιών, λόγω των ιδιαιτεροτήτων κάθε υποδομής.[66]

2.3.6. Η προστασία των Κ.Υ. στην Ελλάδα

Στη χώρα μας, δεν έχει αναπτυχθεί μια ολοκληρωμένη πολιτική για τις ΚΥ, πέρα από την ενσωμάτωση της Οδηγίας NIS στο εσωτερικό δίκαιο με το Ν.4577/18 και την έκδοση της σχετικής απόφασης του Υπουργού Επικρατείας ΥΑ 1027/19, με την οποία εξειδικεύθηκαν τα εφαρμοστικά μέτρα της Οδηγίας, για μια ενιαία πολιτική ασφάλειας συστημάτων δικτύου και πληροφοριών. Σχετικές μελέτες που εκπονήθηκαν από την Κοινωνία της Πληροφορίας ΑΕ το 2008 αναφορικά με την προστασία των ΚΥ της Δημόσιας Διοίκησης (βλ. υποσημ.25) και από το Οικονομικό Πανεπιστήμιο Αθηνών για την ολιστική προστασία και ανθεκτικότητα των ΚΥ το 2016, ανέδειξαν μια σειρά προβλημάτων και ιδιαίτερα την έλλειψη μιας ολιστικής στρατηγικής για τις ΚΥ στην Ελλάδα.[67]

---

[66] Richard White "Risk Analysis for Critical Infrastructure Protection"Methodologies and Strategies for Critical Infrastructure Protection, pp 35-54 In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer https://doi.org/10.1007/978-3-030-00024-0_2

[67] Γκρίτζαλης Δ, Κοτζανικολάου Π. κ.α. "Ολιστική Προστασία Κρίσιμων Υποδομών" Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών, Ιούνιος 2016 https://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo3_version_020616_2.pdf

Στον ψηφιακό τομέα, έγινε ένα βήμα για τη δημιουργία πλαισίου προστασίας, με το Ν.4961/2022 για τις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, με τον οποίο ορίστηκαν τα κριτήρια σύμφωνα με τα οποία χαρακτηρίζεται ως κρίσιμη μια ψηφιακή υποδομή. Συγκεκριμένα ισχύουν τα εξής κριτήρια: α) αν ο φορέας παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων της χώρας και β) αν σε περίπτωση συμβάντος ασφαλείας, η παροχή της υπηρεσίας υφίσταται σοβαρή διατάραξη. (άρθρο 21).Αντίστοιχα υπάρχουν ειδικές ρυθμίσεις και ανεξάρτητες αρχές ανά τομέα, χωρίς κεντρικό σχεδιασμό, με μόνο μηχανισμό αντιμετώπισης και πρόληψης εκτάκτων αναγκών, καθώς και φυσικών/τεχνολογικών καταστροφών, την πολιτική προστασία.

Στο πεδίο της Κυβερνοασφάλειας, δημιουργήθηκε η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ), ως υπηρεσίας του Υπουργείου Ψηφιακής Πολιτικής, αρμόδιας για την εφαρμογή της Οδηγίας NIS ως εθνικού ενιαίου κέντρου επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Με το ν.5002/2022 , ορίστηκε η Επιτροπή Συντονισμού και τα αρμόδια όργανα, που λειτουργούν ως ομάδες CSIRT (Δνση Κυβερνοάμυνας του ΓΕΕΘΑ) και Εθνικού CERT (Δνση Κυβερνοχώρου της ΕΥΠ που λειτουργεί σαν εθνική αρχή INFOSEC), μαζί με την ΕΛΑΣ. Παράλληλα, προβλέπεται η κατάρτιση από τους παραπάνω φορείς, εθνικού σχεδίου αποτίμησης επικινδυνότητας συστημάτων Τεχνολογίας πληροφορικής και επικοινωνιών (ΤΠΕ), το οποίο θα περιλαμβάνει την αναγνώριση, ανάλυση και αποτίμηση των κινδύνων και των επιπτώσεών τους για την ασφάλεια των συστημάτων ΤΠΕ σε εθνικό επίπεδο, αφού ληφθεί υπόψη κάθε κατηγορία πιθανής απειλής και ιδίως απειλές που σχετίζονται με κακόβουλες ενέργειες, φυσικά φαινόμενα, τεχνικές αστοχίες, δυσλειτουργίες ή ανθρώπινα λάθη, με σκοπό την αξιολόγηση της έκτασης και της κρισιμότητας των επιπτώσεων των απειλών αυτών σε εθνικό επίπεδο. Με τον πρόσφατο Ν.5086/2024, η Εθνική Αρχή Κυβερνοασφάλειας αποσπάσθηκε από τον στενό δημόσιο τομέα και επανασυστήθηκε σαν νομικό πρόσωπο δημοσίου δικαίου, με στόχο την αποτελεσματικότερη δράση της.

Για το ζήτημα των ΚΥ, δεν υπάρχουν ενιαίες ρυθμίσεις, αλλά αντιμετωπίζεται αποσπασματικά, με κυριότερο πρόβλημα τον κατακερματισμό των αρμοδιοτήτων, την εμπλοκή διαφορετικών υπηρεσιών και την έλλειψη συντονισμού. Συγχρόνως η έλλειψη κουλτούρας συνεργασίας μεταξύ φορέων δημόσιου και ιδιωτικού τομέα, δημιουργεί επιπρόσθετα προβλήματα. Η νέα μορφή της ΕΑΚ, σε συνδυασμό με τη προοπτική ενσωμάτωσης στο εσωτερικό δίκαιο των Οδηγιών NIS 2 και CER που θα αρχίσουν να ισχύουν από το φθινόπωρο του 2024, δημιουργούν ένα ευνοϊκότερο κλίμα για τη χάραξη μιας εθνικής πολιτικής για τις ΚΥ.[68]

[68] Καρατράντος Τ. "Από τις κρίσιμες υποδομές στις κρίσιμες οντότητες: μία σύνθετη διαδικασία ασφάλειας" ΕΛΙΑΜΕΠ Μάρτιος 2023 www.eliamep.gr/wp-content/uploads/2023/03/Policy-brief-177-Karatrantos-EL.pdf

ΚΕΦΑΛΑΙΟ 3 : ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΤΟΥ ΑΕΡΟΠΟΡΙΚΟΥ ΤΟΜΕΑ

3.1. Οι Αερολιμένες ως κρίσιμες υποδομές

3.1.1. Σημασία και αλληλεπιδράσεις με άλλες Κ.Υ.

Τα αεροδρόμια σήμερα αποτελούν βασικούς πυλώνες της παγκόσμιας σύγχρονης κινητικότητας και εμπορικής αλληλεπίδρασης. Ο τομέας των αερομεταφορών είναι ιδιαίτερα εξελιγμένος, οικονομικά αποδοτικός, εξαιρετικά ασφαλής και αποτελεί ένα σημαντικό παράγοντα που συμβάλλει στην παγκόσμια οικονομία.

Ως κρίσιμες υποδομές, οι αερολιμένες αναδεικνύουν τη σημαντική τους θέση στην παγκόσμια οικονομία. Αποτελούν το κύριο μεσάζοντα συνεργασίας μεταξύ χωρών, πόλεων και περιφερειών, επιτρέποντας τη μετακίνηση εκατομμυρίων ανθρώπων και τη μεταφορά τεράστιων ποσοτήτων εμπορευμάτων καθημερινά. Η κρίσιμη σημασία των αεροδρομίων ξεπερνά την απλή έννοια της μεταφοράς, καθώς αποτελούν βασικά κριτήρια για την οικονομική και κοινωνική ανάπτυξη μιας περιοχής, προσφέροντας ευκαιρίες για τη δημιουργία θέσεων εργασίας, την ανάπτυξη του τουρισμού, και την ενίσχυση του εμπορίου.

Η αεροπορία είναι ένα πολύπλοκο διασυνδεδεμένο "σύστημα συστημάτων" που αποτελείται από υποδομές ή συστήματα όπως το ATM(Air Traffic Management), τις επίγειες υπηρεσίες, τις τηλεπικοινωνίες κ.λπ. Όλα αυτά τα συστήματα και οι υποδομές, είναι διασυνδεδεμένα και αλληλοεξαρτώμενα με διαφορετικά επίπεδα κρισιμότητας, απειλών, τρωτών σημείων και κινδύνων. Η αεροπορία εξαρτάται από άλλες υποδομές και συστήματα όπως η ενέργεια, οι μεταφορές και οι τηλεπικοινωνίες, υποδομές που αντίστοιχα εξαρτώνται από την αεροπορία για την παροχή υπηρεσιών στους πολίτες.

Τα αεροδρόμια αποτελούν κρίσιμες υποδομές καθώς:

1. Υποστηρίζουν τον αεροπορικό τομέα, επιτρέποντας τη μεταφορά εκατομμυρίων ανθρώπων και τόνων εμπορευμάτων κάθε χρόνο. Αυτή η συνδετική λειτουργία τους, δίνει κρίσιμη σημασία για τη λειτουργία του παγκόσμιου εμπορίου και της παγκόσμιας οικονομίας.

2. Λειτουργούν ως κρίσιμοι κόμβοι μεταφοράς, επιτρέποντας την ανταλλαγή επιβατών, εμπορευμάτων και πόρων ανάμεσα σε διάφορες περιοχές του κόσμου.

3. Λόγω του μεγέθους και της σημασίας τους, αποτελούν σημαντικούς στόχους για πιθανές τρομοκρατικές επιθέσεις ή άλλες απειλές ασφάλειας, καθιστώντας την προστασία τους και των επιβατών προτεραιότητα για τις κυβερνήσεις και τις αρχές ασφαλείας.

Επιπλέον, οι αλληλεπιδράσεις των αεροδρομίων με άλλες κρίσιμες υποδομές μπορούν να είναι σημαντικές, καθώς τα αεροδρόμια εξαρτώνται από πολλούς άλλους τομείς για την ολοκληρωμένη λειτουργία τους. Συνολικά, οι αλληλεπιδράσεις αυτές επισημαίνουν το ρόλο της συνοχής και συνεργασίας μεταξύ των διαφόρων κρίσιμων υποδομών για τη διασφάλιση της ασφάλειας και της ομαλής λειτουργίας των αεροδρομίων και του αεροπορικού τομέα.[69]

ΑΛΛΗΛΕΠΙΔΡΑΣΕΙΣ ΑΕΡΟΔΡΟΜΙΩΝ ΜΕ ΑΛΛΕΣ Κ.Υ	
ΜΕΤΑΦΟΡΕΣ	Τα αεροδρόμια εξαρτώνται από καλές συγκοινωνιακές συνδέσεις με την πόλη ή την περιοχή που εξυπηρετούν, καθώς και από καλή λειτουργία του σιδηροδρομικού, οδικού και θαλάσσιου δικτύου για τη μεταφορά επιβατών και εμπορευμάτων προς και από το αεροδρόμιο.
ΕΝΕΡΓΕΙΑ	Η διαρκής παροχή ηλεκτρικής ενέργειας είναι ουσιώδης για τη λειτουργία των αεροδρομίων, καθιστώντας την ενεργειακή υποδομή μια σημαντική αλληλεπίδραση.
ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ	Η επικοινωνιακή υποδομή είναι απαραίτητη για τη διασφάλιση της επικοινωνίας μεταξύ των αεροδρομίων και των αεροσκαφών, καθώς και για την επικοινωνία με τους επιβάτες και το προσωπικό του αεροδρομίου.

3.1.2. Οργανισμοί για την ασφάλεια του αεροπορικού τομέα

- **ICAO**

Η βάση για την ασφάλεια της πολιτικής αεροπορίας είναι το Παράρτημα 17 της Σύμβασης του Σικάγο του 1944, με την οποία ιδρύθηκε σαν εξειδικευμένη υπηρεσία του ΟΗΕ ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (ICAO). Στη σύμβαση είναι πλέον συμβαλλόμενα μέρη 193

[69] Eurocontrol : ATM: navigating the challenging cybersecurity landscape, March 2023 https://www.eurocontrol.int/article/atm-navigating-challenging-cybersecurity-landscape
Eurocontrol : Aviation as a critical infrastructure: challenges and opportunities for a more resilient sector, March 2023

κράτη, τα οποία οφείλουν να ακολουθούν τα πρότυπα, τις πρακτικές και τους ελέγχους συμμόρφωσης που συστήνει ο ICAO για την ασφάλεια των διεθνών αεροπορικών μεταφορών, χωρίς ωστόσο να υπάρχει ένας δεσμευτικός μηχανισμός. Η σημαντικότερη αρμοδιότητα του ICAO είναι η διαμόρφωση και επικαιροποίηση των Προτύπων και Πρακτικών (Standards and Recommended Practices SARPs), που είναι προσαρτημένα σαν 19 τεχνικά παραρτήματα στη Σύμβαση, μεταξύ των οποίων είναι τα μέτρα αποφυγής των έκνομων ενεργειών σε βάρος της πολιτικής αεροπορίας. Ο Οργανισμός στη σύγχρονη στρατηγική του έχει θέσει σαν πρωταρχικό του στόχο να ηγηθεί διεθνώς στην ασφάλεια της πολιτικής αεροπορίας, σε συνδυασμό με την ψηφιοποίηση και την εφαρμογή των νέων τεχνολογιών.[70]

- **IATA**

Σημαντικός φορέας είναι η Διεθνής Ένωση Αεροπορικών Μεταφορέων (IATA), η οποία αποτελεί μια διεθνή εμπορική ένωση των αεροπορικών εταιρειών. Η IATA εργάζεται για τη βελτίωση της αποτελεσματικότητας και της κερδοφορίας της αεροπορικής βιομηχανίας, καθώς και για την προώθηση των συμφερόντων των αεροπορικών εταιρειών σε διεθνές επίπεδο. Στο πλαίσιο αυτό, αναπτύσσει στρατηγικες, πολιτικές και προγράμματα για όλο το φάσμα των επιχειρηματικών δραστηριοτήτων των εταιρειών. Η ασφάλεια (aviation security) αποτελεί ένα από τα βασικότερα πεδία παροχής υποστήριξης, με ολοκληρωμένη καθοδήγηση στην διαχείριση επικινδυνότητας μέσω ενός σχεδίου ασφαλείας (security management system).[71]

- **ACI**

Το Διεθνές Συμβούλιο Αεροδρομίων (ACI) είναι μια διεθνής ένωση αεροδρομίων, που έχει σαν αντικείμενο την ενιαία εφαρμογή των Προτύπων από τα αεροδρόμια, σύμφωνα με τη καθοδήγηση του ICAO. Στον τομέα της ασφάλειας, διαθέτει το πρόγραμμα APEX Security με στόχο την ενίσχυση της συμμόρφωσης στα διεθνή πρότυπα για την αεροπορική βιομηχανία και την ανάπτυξη ενός σχεδίου διαχείρισης της επικινδυνότητας.[72]

- **CANSO**

Η Ένωση Πολιτικών Υπηρεσιών Αεροναυτιλίας (CANSO) είναι ένας παγκόσμιος οργανισμός που εκπροσωπεί τα συμφέροντα των Παρόχων Υπηρεσιών Αεροναυτιλίας (ANSP). Στόχος είναι η προστασία και η ανθεκτικότητα του συστήματος εναέριας κυκλοφορίας (ATM) τόσο στο έδαφος όσο και στον αέρα.Η Κυβερνοασφάλεια είναι ένας τομέας στον οποίο δραστηριοποιείται εντατικά η CANSO, προωθώντας μια κουλτούρα πρόληψης. Το Πρότυπο για την Κυβερνοασφάλεια (CANSO Standard of Excellence in Cybersecurity, 2020) και ο Οδηγός για την αποτίμηση επικινδυνότητας στον κυβερνοχώρο (CANSO Cyber Risk Assessment Guide),

[70] https://www.icao.int/about-icao/Council/Pages/Strategic-Objectives.aspx
[71] https://www.iata.org/en/publications/store/security-management-system-manual/
[72] ACI Airport Excellence in Security https://aci.aero/wp-content/uploads/2021/08/APEX-in-Security.pdf

παρέχουν καθοδήγηση στους Παρόχους σχετικά με το σχέδιο ασφάλειας και το ΣΔΑΠ (SeMS/ ISMS), καθώς και τις διεργασίες αποτίμησης επικινδυνότητας. [73]

- **TSA /FAA**

Η Υπηρεσία Ασφάλειας Αεροπορίας των ΗΠΑ (TSA) είναι ο ομοσπονδιακός οργανισμός των ΗΠΑ που είναι υπεύθυνος για την ασφάλεια των αεροπορικών ταξιδιών. Η Ομοσπονδιακή Διοίκηση Αεροπορίας (FAA) έχει ευρύτερες αρμοδιότητες για την ασφάλεια της αεροναυτιλίας και συνεργάζεται με την TSA σε θέματα τεχνογνωσίας. Με βάση τα πρότυπα NIST για τη Κυβερνοασφάλεια, η FAA αναπτύσσει συμπληρωματικά πρότυπα για την διαχείριση επικινδυνότητας, μεθοδολογίες και εργαλεία ανάλυσης κινδύνου και απειλών.[74]

- **Οργανισμοί της Ευρωπαϊκής Ένωσης για την προστασία της αεροπορίας**

➢ **EASA**

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας είναι ο κύριος οργανισμός που είναι υπεύθυνος για την ασφάλεια της αεροπορίας στην Ευρωπαϊκή Ένωση. Θέτει πρότυπα και κανόνες για την εναέρια κυκλοφορία και την ασφάλεια των αεροδρομίων και παρέχει καθοδήγηση για την εφαρμογή των κανονισμών και οδηγιών της Ε.Ε. στον αεροπορικό τομέα. Η στρατηγική του στους τομείς της ασφάλειας πληροφοριών και της Κυβερνοασφάλειας είναι η ανάπτυξη ενός ασφαλούς και ανθεκτικού συστήματος αεροπλοΐας. Για την ανάπτυξη της ανθεκτικότητας, υποστηρίζει τις δραστηριότητες του Ευρωπαϊκού Κέντρου για την Κυβερνοασφάλεια στην Αεροπορία (ECCSA) για τη συνεργασία φορέων και οργανισμών στην αντιμετώπιση των κινδύνων και απειλών του κυβερνοχώρου στην αεροπορία.[75]

➢ **EUROCONTROL**

Ο Eurocontrol είναι ένας οργανισμός για την ασφάλεια της αεροναυτιλίας, που είναι υπεύθυνος για τη διαχείριση της εναέριας κυκλοφορίας στον Ευρωπαϊκό ουρανό. Διαχείριση του Ενιαίου (SES): Ο EUROCONTROL συνεργάζεται με κράτη μέλη, αεροπορικές εταιρείες, αεροδρόμια και άλλους εταίρους για την υλοποίηση του προγράμματος του ενιαίου Ευρωπαϊκού Ουρανού. Έχει καθοριστικό ρόλο στην ανάπτυξη του προγράμματος Διαχείρισης Εναέριας Κυκλοφορίας SESAR (Single European Sky Air Traffic Management Research) της ΕΕ για τον εκσυγχρονισμό και την αναβάθμιση του ευρωπαϊκού συστήματος διαχείρισης εναέριας κυκλοφορίας (ATM). Στο πεδίο της Κυβερνοασφάλειας, αναπτύσσει πολιτικές για την αντιμετώπιση των απειλών του Κυβερνοχώρου. Πέρα από την ενεργή υποστήριξη του

[73] https://canso.org/protecting-atm-systems/
[74] FAA Cybersecurity Risk (CyRM Modelling)
https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cas/cytf/cytf.pdf
[75] https://www.easa.europa.eu/en/domains/cyber-security

προγράμματος SESAR, συμβάλει στην έρευνα για την κυβερνοασφάλεια, παρέχει βοήθεια στα κράτη μέλη και συνεργάζεται με τους άλλους οργανισμούς προστασίας της αεροπορίας.[76]

- **Οργανισμοί στον ελληνικό χώρο**

➢ **ΥΠΑ**

Η Υπηρεσία Πολιτικής Αεροπορίας, υπήρξε ο κύριος δημόσιος φορέας αρμοδιοτήτων στον χώρο της πολιτικής αεροπορίας. Το 2020 μεταβλήθηκε το νομικό καθεστώς της και συστάθηκε σαν ΝΠΔΔ, με τις αρμοδιότητές του να περιορίζονται στη παροχή υπηρεσιών αεροναυτιλίας και διαχείρισης αεροδρομίων, δηλαδή υπηρεσιών εναέριας κυκλοφορίας, επικοινωνίας, πλοήγησης και επιτήρησης, μετεωρολογικές υπηρεσιών που προορίζονται για την αεροναυτιλία και υπηρεσιών αεροναυτικών πληροφοριών.

➢ **ΑΠΑ**

Η Αρχή Πολιτικής Αεροπορίας είναι ανεξάρτητη αρχή που ιδρύθηκε το 2020, με ρυθμιστικές και εποπτικές αρμοδιότητες στον τομέα των αερομεταφορών, της αεροναυτιλίας και των αερολιμένων. Με την ίδρυσή της, σε συμμόρφωση με τις προβλέψεις της Ε.Ε., διαχωρίστηκαν οι ρυθμιστικές και εποπτικές αρμοδιότητες από την οργάνωση των υπηρεσιών αεροναυτιλίας και διαχείρισης αεροδρομίων, που παρέμειναν στην ΥΠΑ. Η ΑΠΑ εισηγείται την χάραξη εθνικής στρατηγικής στον τομέα των αερομεταφορών και σκοπός της είναι η εφαρμογή της εθνικής και ενωσιακής νομοθεσίας, σχετικά με τη λειτουργία του Ενιαίου Ευρωπαϊκού Ουρανού, καθώς και των διεθνών συμβάσεων. Εποπτεύει τη λειτουργία του δικτύου διαχείρισης της εναέριας κυκλοφορίας και την ασφάλεια στη πολιτική αεροπορία. Συνεργάζεται με τους διεθνείς οργανισμούς για τους σκοπούς αυτούς και ειδικότερα με τους EASA και EUROCONTROL. Στο πλαίσιο αυτών των αρμοδιοτήτων, στην ΑΠΑ λειτουργεί Τμήμα Ασφάλειας από Έκνομες Ενέργειες για την ανάπτυξη κανονισμών και προτύπων ασφαλείας, όπως του Εθνικού Προγράμματος Ασφάλειας της Πολιτικής Αεροπορίας από έκνομες ενέργειες (Ε.Π.Α.Π.Α.). Λειτουργεί επίσης Τμήμα Ασφάλειας Αερομεταφορέων, Ασφάλειας στον Κυβερνοχώρο και Εξοπλισμού Ασφάλειας με αρμοδιότητες, μεταξύ άλλων, τη ρύθμιση, πιστοποίηση, εποπτεία και ανάπτυξη προτύπων ασφάλειας της πολιτικής αεροπορίας. Για τους σκοπούς αυτούς συνεργάζεται για θέματα ασφάλειας στον κυβερνοχώρο με την Εθνική Αρχή Κυβερνοασφάλειας, καθώς και με άλλες αρμόδιες αρχές όπως την Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ), την αντίστοιχη υπηρεσία του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ) και της Ελληνικής Αστυνομίας. [77]

[76] https://www.eurocontrol.int/cybersecurity
[77] Ιστοσελίδα ΑΠΑ https://hcaa.gov.gr/el/aeroporiki-asfaleia

3.1.3. Η εξέλιξη των Αεροδρομίων: Τα έξυπνα Αεροδρόμια

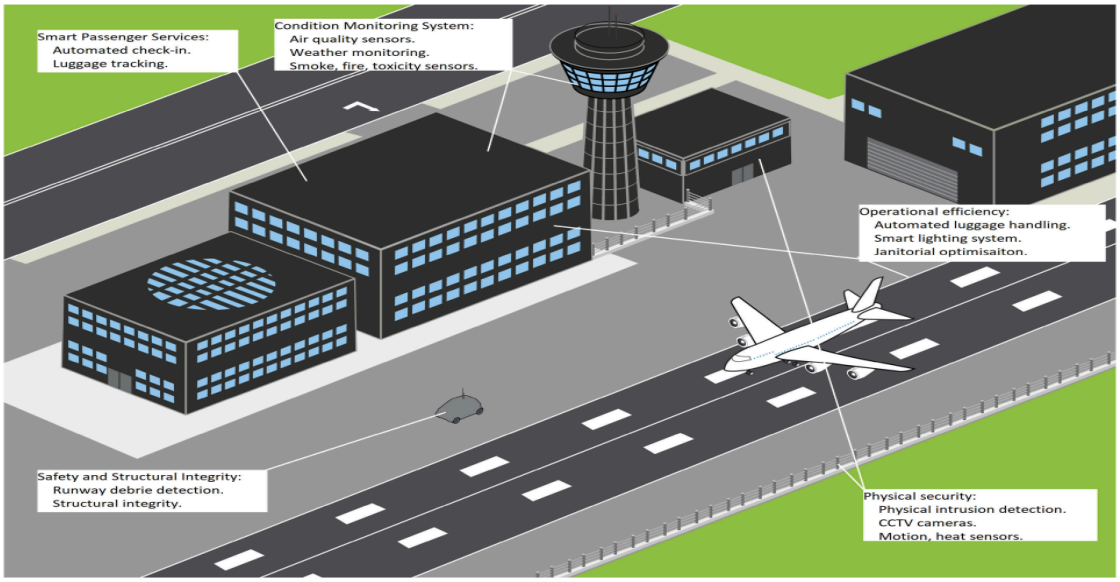
Κατά τη διάρκεια της ιστορίας τους, τα αεροδρόμια έχουν γνωρίσει σημαντικές αλλαγές στις λειτουργίες τους και στις υπηρεσίες που παρέχουν. Πέρα από την απλή παροχή υπηρεσίας μεταφοράς, μέσω της βελτίωσης της ποιότητας των υπηρεσιών τους, μπορούν να εξασφαλίσουν μια άνετη διαμονή και ψυχαγωγική εμπειρία στους επιβάτες. Η εξέλιξη των αερολιμένων , σαν αποτέλεσμα των τεχνολογικών εξελίξεων και της αφομοίωσης τεχνολογιών όπως το IoT, μπορεί να εξεταστεί σε τρία διαδοχικά στάδια, το Αεροδρόμιο 1.0, το Αεροδρόμιο 2.0 και το Αεροδρόμιο 3.0.[78]

Η εξέλιξη των αεροδρομίων	Χαρακτηριστικά	Σύγκριση / Ελλείψεις
Αεροδρόμιο 1.0	• Δίνεται μεγάλη προσοχή στην εξασφάλιση της ασφαλούς λειτουργίας των αεροσκαφών, όπως η απογείωση, ο ανεφοδιασμός και η προσγείωση. • Εξασφαλίζεται η παροχή τυποποιημένων υπηρεσιών για τους επιβάτες, σχετικά με την επιβίβαση και την αποβίβαση από το αεροσκάφος	• Οι ανέσεις είναι ελάχιστες. • Η συνεργασία των διαφόρων υπηρεσιών και των ενδιαφερομένων μερών δεν είναι σημαντική σε αυτά τα αεροδρόμια.
Αεροδρόμιο 2.0 "Ευέλικτο αεροδρόμιο"	• Περιλαμβάνει αεροδρόμια που είναι ευέλικτα και μπορούν να προσαρμόζουν το φόρτο εργασίας τους ανάλογα με τη ζήτηση. • Σε αυτά τα αεροδρόμια, η συνεργασία μέσω της απρόσκοπτης ανταλλαγής δεδομένων είναι εξέχουσα, με ένα μοναδικό δίκτυο να χρησιμοποιείται συχνά για	Σε σύγκριση με το Αεροδρόμιο 1.0, το Αεροδρόμιο 2.0 επιτρέπει: • Τη βελτίωση της αποτελεσματικότητας και εστιάζει περισσότερο στην εμπειρία των επιβατών.

[78] Koroniotis N et al.A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports, Jan. 2020, IEEE https://www.researchgate.net/publication/347832747_A_Holistic_Review_of_Cybersecurity_and_Reliability_Perspectives_in_Smart_Airports

	να συνδέσει τα διάφορα τμήματα του αεροδρομίου κάτω από ένα ενιαίο σύστημα διαχείρισης ● Συστήματα με δυνατότητα δικτύου, όπως η IP-τηλεφωνία ● Περιλαμβάνουν τη δυνατότητα της βιντεοεπιτήρησης	
Αεροδρόμιο 3.0 "Εξυπνο αεροδρόμιο"	Ο φυσικός διάδοχος του Αεροδρομίου 2.0. Οφείλει την ύπαρξή του στη Βιομηχανία 4.0. ● Τροφοδοτούμενα από το IoT, τα αεροδρόμια αυτής της κατηγορίας χρησιμοποιούν ενοποιημένο δίκτυο οντοτήτων, συμπεριλαμβανομένου του αεροδρομίου, των αεροσκαφών και των αεροπορικών εταιρειών, με πολλαπλούς αισθητήρες και ενεργοποιητές που αναπτύσσονται σε όλο το αεροδρόμιο για την παροχή υπηρεσιών. ● Το ενοποιημένο αυτό δίκτυο ενισχύει την εμπειρία των επιβατών, κάνοντας την ολοκληρωμένη. ● Βελτίωση περαιτέρω των λειτουργιών του αεροδρομίου μέσω της απρόσκοπτης συνεργασίας πολλαπλών υποσυστημάτων και της ανταλλαγής και ανάλυσης δεδομένων σε πραγματικό χρόνο. ● Αξιοποιούνται ισχυρές τεχνολογίες συμπεριλαμβανομένων των	● Τα έξυπνα αεροδρόμια δεν έχουν έναν σταθερό και κοινά αποδεκτό ορισμό, καθώς ακόμα υπάρχει μια γενική έλλειψη κοινών προτύπων για την εφαρμογή και την ανάπτυξη τους.

	μεγάλων δεδομένων, της βιομετρικής τεχνολογίας και της τεχνητής νοημοσύνης, για την τροφοδοσία του σύγχρονου έξυπνου αεροδρομίου.	



Σχήμα 10 : Η αρχιτεκτονική του έξυπνου αεροδρομίου

3.2. Ευπάθειες και απειλές των Κρισιμων Υποδομών των Αερολιμένων

3.2.1. Οι κατηγορίες απειλών στους Αερολιμένες

Στο σύγχρονο κόσμο, οι Αερολιμένες αντιπροσωπεύουν κρίσιμους και στρατηγικούς σταθμούς που καθορίζουν τη παγκόσμια κινητικότητα και σχετίζονται άμεσα με τη κοινωνική, πολιτική και οικονομική ανάπτυξη της κοινωνίας. Ωστόσο η αναπτυσσόμενη τεχνολογία αποτελεί πρόκληση για τις κρίσιμες υποδομές των Αερολιμένων και εισάγει απειλές που υπονομεύουν την ασφάλεια και τη λειτουργικότητα των σταθμών αυτών. Με αυτό το τρόπο αυξάνεται η πολυπλοκότητα των αεροπορικών επιχειρήσεων τοποθετώντας την ασφάλεια των υποδομών αυτών στο επίκεντρο της προσοχής καθώς οι απειλές μεταβάλλονται και εξελίσσονται συνεχώς.[79]

Οι τομείς που σχετίζονται με την ασφάλεια στις κρίσιμες υποδομές των Αερολιμένων σύμφωνα με τη Διεθνή Ένωση Αερομεταφορών (International Air Transport Association, IATA)

[79] Lykou, G. "Developing Resilience and Cyber-Physical Protection Capabilities in Critical Aviation Infrastructures" Εθνικό Αρχείο Διδακτορικών Διατριβών https://www.didaktorika.gr/eadd/handle/10442/49706

κατηγοριοποιούνται σε 29 ομάδες. Κάθε ομάδα αποτελείται από επιχειρησιακές διαδικασίες μέσα στις οποίες μπορεί να εμφανιστούν δυσλειτουργίες που εν δυνάμει μπορούν να αποτελέσουν απειλή για την υποδομή του Αερολιμένα. Παρακάτω παρατίθεται ένας πίνακας με τις 29 κατηγορίες συμβάντων όσον αφορά την αεροπορική ασφάλεια ομαδοποιημένες σε 18 ομάδες.

Κατηγορίες Συμβάντων Αεροπορικής Ασφάλειας	**Επιχειρησιακές καταστάσεις / Απειλές που οφείλονται στο συμβαν**
1. **α.** Απειλές στο έδαφος **β.** Απειλές στη περίμετρο εδάφους **γ.** Απειλές στο γενικό περιβάλλον	● Έκρηξη από εκρηκτικό μηχανισμό (Improvised Explosive Device, IED) ● Έκρηξη από ανθρώπινο παράγοντα IED ● Ένοπλη επίθεση ● Αφύλακτη/ Ύποπτη αποσκευή ● Χημική, Βιολογική ή ραδιενεργή επίθεση
2. Απειλές προς το πλήρωμα των αεροπορικών εταιρειών και τους υπαλλήλους	● Πιθανότητα κινδύνου κατα τη διαμονή και τη μεταφορά του πληρώματος
3. **α.** Ελεγχόμενες περιοχές στον αερολιμένα **β.** Περιοχές με περιορισμούς ασφαλείας στον αερολιμένα	● Μη εξουσιοδοτημένη πρόσβαση σε ελεγχόμενες περιοχές εντός και περιμετρικά του αερολιμένα ● Μη εξουσιοδοτημένη πρόσβαση σε προϊόντα εναέριας μεταφοράς ή στα συστήματα check-in
4. **α.** Έλεγχος αποσκευών,επιβατών & καμπίνας **β**. Έλεγχος προσωπικού & πληρώματος	● Εύρεση απαγορευμένων αντικειμένων ● Ελλείψεις στο σημείο ελέγχου ● Έκθεση επιβατών μετά τον ΄έλεγχο με επιβάτες που δεν έχουν ελεγχθεί ακόμα
5. **α.** Έλεγχος πρόσβασης σε αεροσκάφος **β.** Έλεγχος ασφάλειας αεροσκάφους	● Αεροσκάφους που δεν έχει περάσει τους σωστούς ελέγχους, άρα θεωρείται μη ασφαλές ● Μη εξουσιοδοτημένη πρόσβαση στο αεροσκάφος ● Ανύπαρκτη/ Μη έγκυρη/ Μη εμφανής κάρτα ταυτοποίησης ● Εύρεση ύποπτου αντικειμένου στο αεροσκάφος ● Ανεπαρκής/ Αναποτελεσματικός έλεγχος του αεροσκάφους

6. **α.** Η παραλαβή αποσκευών **β.** Έλεγχος παραλαβής αποσκευών **γ.** Η προσβολή της προστασίας της διαδικασίας παραλαβής αποσκευών	● Προβλήματα που μπορεί να προκύπτουν κατά τη διαδικασία αποδοχής των αποσκευών εντός και εκτός του αεροδρομίου ● Εκφόρτωση αποσκευών σε λάθος αεροσκάφος ● Προβλήματα στη διαδικασία χαμένης αποσκευής ● Η απόσπαση της αποσκευής από τον επιβάτη
7. **α**. Παραλαβή φορτίων & εμπορευμάτων **β.** Έλεγχος φορτίων & εμπορευμάτων **γ.** Η προσβολή της προστασίας φορτίων & εμπορευμάτων	● Ελλείψεις στη καταγραφή και τεκμηρίωση ως προς την ασφάλεια του φορτίου ● Εύρεση απαγορευμένων αντικειμένων ● Πραγματοποίηση λανθασμένων διαδικασιών κατά τον έλεγχο ● Ελλείψεις στη διαδικασία ασφάλισης του φορτίου και της αλληλογραφίας ● Μη εξουσιοδοτημένη πρόσβαση στις αποθήκες φορτίου και αλληλογραφίας
8. **α.** Έλεγχος ασφάλειας εφοδιασμού κατά τη διάρκεια της πτήσης **β.** Προσβολή της προστασίας εφοδιασμού κατα τη διάρκεια της πτήσης	● Παραβίαση του ελέγχου πρόσβασης των εγκαταστάσεων με τις προμήθειες των πτήσεων ● Εύρεση απαγορευμένων αντικειμένων στις εγκαταστασεις αυτές ● Παραβίαση ελέγχων ασφαλείας
9. **α.** Έλεγχος ασφαλείας εφοδιασμού του αεροδρομίου **β.** Προστασία εφοδιασμού αεροδρομίου	● Παραβίαση του ελέγχου πρόσβασης των εγκαταστάσεων με τις προμήθειες του αεροδρομίου ● Απαγορευμένα αντικείμενα ● Παραβίαση ελέγχων ασφαλείας
10. Απειλές από εσωτερικούς παράγοντες	● Ενεργητικός ή Παθητικός εσωτερικός δράστης αποτελεί απειλή για τη σωστή λειτουργία του αερολιμένα και προσβάλλει την ασφάλεια του
11. Ανυπάκουοι/Υπό την επήρεια ουσιών επιβάτες	● Αναστάτωση της ομαλής λειτουργίας του αεροδρομίου και του αεροσκάφους
12. Σαμποτάζ ή καταστροφή στο έδαφος του αερολιμένα	● Απειλή βόμβας στο αεροσκάφος όσο βρίσκεται στο έδαφος ● Απαγορευμένη ουσία ή αντικείμενο ● Πλαστογραφημένη υπογραφή
13. Απειλές κατά τη διάρκεια της πτήσης	● Απειλή βόμβας κατά τη διάρκεια της πτήσης ● Αεροπειρατεία ● Άλλη επικίνδυνη ουσία ή αντικείμενο (CBR) στη πτήση

	● Σύστημα πυραύλων που στοχεύουν το αεροσκάφος στον αέρα ● Στρατιωτικές αποστολές που επηρεάζουν την εναέρια κυκλοφορία ● Άτομα για την ασφάλεια της πτήσης (IFSO - In flight security officers) ● Παραβίαση της πολιτικής της καμπίνας του αεροσκάφους
14. Μεταφορά όπλων ή ένοπλων ατόμων	● Όπλα/Πυρομαχικά εντός της καμπίνας ● Όπλα/Πυρομαχικά εντός του χώρου φόρτωσης (λόγω παραβίασης ή μη εξουσιοδοτημένης διαδικασίας)
15. Ανώνυμα αεροσκάφη	● Κοντινή παρακολούθηση UAV (unmanned aerial vehicle) στο αεροσκάφος ● Σύγκρουση ● Απειλή UAV απέναντι στην υποδομή του αεροδρομίου, του αεροσκάφους και των επιβατών ● Εντοπισμός/ Παρατήρηση
16. Άλλες ποινικές πράξεις	● Πληροφορίες σχετικές με την ασφάλεια διαδικασιών/ χώρων και ατόμων ● Παράνομες ουσίες (ναρκωτικά) ● Ξέπλυμα χρήματος ● Κλοπή εντός της πτήσης ● Κλοπή περιουσίας της αεροπορικής εταιρείας
17. Αποδοχή επιβατών στο αεροδρόμιο & τις πτήσεις	● Αποτυχία ελέγχου των εγγράφων ● Επιβάτες που γίνονται αποδεκτοί με λάθος αριθμό κράτησης εισιτηρίου ● Τα στοιχεία της κάρτα επιβίβασης με τα στοιχεία του επιβάτη είναι διαφορετικά ● Λανθασμένα στοιχεία επιβάτη στα ταξιδιωτικά του έγγραφα ● Απελαθέντες/Συνοδευόμενοι επιβάτες(DEPA) ● Μη συνοδευόμενοι απελαθέντες (DEPU) ● Επιβάτες που δεν θα έπρεπε να τους επιτρέπεται η μεταφορά (INAD) ● Άτομο υπό κράτηση
18. Κυβερνοασφάλεια	● Παραβίαση της διαδικασίας πρόσβασης στο δίκτυο ή στον εξοπλισμό ασφαλείας και στα βασικά συστήματα που χρησιμοποιούνται για επιχειρησιακούς σκοπούς.

1. **Απειλές στο έδαφος/ στη περίμετρο εδαφους/ στο γενικό περιβάλλον**

Οποιαδήποτε πραγματική ή δυνητική κατάσταση απειλής εναντίον επιβατών, πληρώματος ή υποδομών που λαμβάνει χώρα στη περιοχή του τερματικού αεροσταθμού ή στο χώρο γύρω από αυτόν. Συμπεριλαμβάνεται ο τερματικός, οι περιοχές στάθμευσης του αεροσταθμού, τα ξενοδοχεία και οι δρόμοι πρόσβασης προς αυτόν. Όσον αφορά τη περίμετρο του εδάφους του αερολιμένα, οι απειλές μπορεί να αφορούν τη περίμετρο ή τις περιοχές επισυναπτόμενες της κρίσιμης υποδομής. Τέλος, οι παραπάνω απειλές μπορεί να σημειωθούν και στο γενικό περιβάλλον του αεροσταθμού , δηλαδή προς τα ξενοδοχεία, τη πόλη και την ευρύτερη περιοχή (πχ Δήμος), όπως και στην εναέρια περιοχή εντός και περιμετρικά της υποδομής.

2. **Απειλές προς το πλήρωμα των αεροπορικών εταιρειών και του υπαλλήλους**

Οποιαδήποτε πραγματική ή δυνητική κατάσταση απειλής που λαμβάνει χώρα στη πόλη ή και στην ευρύτερη περιοχή που βρίσκεται ο αερολιμένας που μπορεί να έχει αντίκτυπο στο πλήρωμα αεροπορικών εταιρειών ή και στο προσωπικό που η εργασία τους σχετίζεται με τον αεροπορικό κλάδο (πχ. Υπαλλήλους ξενοδοχείων και εστιατορίων, οδηγούς λεωφορείων και ταξί). Η συγκεκριμένη απειλή συμπεριλαμβάνει προσβολή της ασφάλειας όσον αφορά τη μεταφορά αλλά και τη διαμονή τους.

3. **Ελεγχόμενες περιοχές στον αερολιμένα / Περιοχές με περιορισμούς ασφαλείας στον αερολιμένα**

Οποιοδήποτε πραγματικό ή πιθανό συμβάν ή ευπάθεια σχετίζεται με μη εξουσιοδοτημένο άτομο στον αεροδρομιακό χώρο και στη περιοχή συντήρησης και επισκευής του αεροσκάφους αποτελεί απειλή προς την ασφάλεια του αερολιμένα.Όπως επίσης και η μη εξουσιοδοτημένη πρόσβαση σε προϊόντα εναέριας μεταφοράς ή του συστήματος check-in του αεροδρομίου. Αναλυτικότερα, συμπεριλαμβάνονται συμβάντα με λανθασμένες διαδικασίες που αφορούν τις αεροδρομιακές ταυτότητες, που εξουσιοδοτούν άτομα σε ένα σύστημα διαβαθμισμένης πρόσβασης σε περιοχές ελέγχου. Αυτό συμβαίνει λόγω έλλειψης ή ανεπαρκούς εκπαίδευσης, όπως επίσης και λόγω τεχνικών προβλημάτων των συστημάτων ελέγχου των ταυτοτήτων ελεγχόμενης πρόσβασης.

4. **Έλεγχος αποσκευών,επιβατών & καμπίνας/ Έλεγχος προσωπικού & πληρώματος**

Οποιαδήποτε πραγματική ή δυνητική κατάσταση όπου οι κανόνες στα σημεία ελέγχου επιβατών και αποσκευών δεν τηρούνται, λόγω έλλειψης ή μη επαρούς εκπαίδευσης ή επιθεώρησης. Στη κατηγορία αυτή συμπεριλαμβάνεται ο κίνδυνος της απειλής με όπλο ή πυρομαχικά κατα τη διάρκεια ελέγχου. Ακόμα απειλή μπορεί να αποτελεί και ο εξοπλισμός ελέγχου που ενδεχομένως υπολειτουργεί. Επιπλέον, ένα σημαντικό θέμα όσον αφορά την ασφάλεια είναι η πιθανή επαφή μεταξύ επιβατών που έχουν πραγματοποιήσει τον έλεγχο και επιβατών που δεν έχουν ελεγχθεί ακόμα. Για αυτή τη κατάσταση μπορεί να ευθύνεται η διαρρύθμιση της υποδομής του

αερολιμένα, όπως επίσης και περιστατικά όπου δεν ακολουθούνται οι σωστές διαδικασίες του ελέγχου των επιβατών και των χειραποσκευών. Ακολούθως της προηγούμενης κατηγορίας που αφορά τις απειλές ασφάλειας στον έλεγχο των επιβατών και χειραποσκευών, τα ίδια προβλήματα και δυσλειτουργίες είναι πιθανό να συμβούν και στον έλεγχο του προσωπικού του αερολιμένα και του πληρώματος των αεροπορικών εταιρειών.

5. Έλεγχος πρόσβασης σε αεροσκάφος/ Έλεγχος ασφάλειας αεροσκάφους

Οποιαδήποτε πραγματική ή πιθανή μή ελεγχόμενη ή μη εξουσιοδοτημένη πρόσβαση στη καμπίνα του αεροσκάφους ή στο χώρο εκφόρτωσης του, συμπεριλαμβανομένης της αποτυχίας πραγματοποίησης των απαραίτητων ελέγχων ασφαλείας, λόγω έλλειψης ή ανεπαρκούς εκπαίδευσης και επιθεώρησης. Όσον αφορά τον έλεγχο ασφαλείας του αεροσκάφους, απειλεί αποτελεί οποιαδήποτε κατάσταση (πχ όπλα ή πυρομαχικά) υφίσταται στο αεροσκάφος ή στη διαδικασία εκφόρτωσης του κατα τη διάρκεια ή έπειτα από την ολοκλήρωση του ελέγχου του. Μέρος των απειλών αυτών αποτελεί ο μη λειτουργικός εξοπλισμός και οι διαδικασίες των κανόνων του ελέγχου ασφάλειας του αεροσκάφους δεν πραγματοποιούνται.

6. Παραλαβή αποσκευών / Έλεγχος παραλαβής αποσκευών / Προσβολή της διαδικασίας Ελέγχου αποσκευών

Όσον αφορά τη προσβολή της ασφάλειας στο κομμάτι της παραλαβής αποσκευών, απειλή μπορεί να αποτελεί μια πραγματική ή δυνητική κατάσταση όπου μια αφύλακτη αποσκευή μπορεί να υποστεί λάθος μεταφορά. Εν δυνάμει μπορεί να αποτελέσει πρόβλημα και η κατάσταση όπου έχει δοθεί μη εξουσιοδοτημένη πρόσβαση όσον αφορά την κατοχή αποσκευών. Σε αυτό ενδέχεται να συμβάλλει η μη τήρηση των διαδικασιών και των κανόνων λόγω ανεπαρκούς εκπαίδευσης ή λόγω έλλειψης επιτήρησης. Ακόμα, στη διαδικασία ελέγχου αποσκευών μπορεί να προκύψει πρόβλημα όταν οι κανόνες ελέγχου δεν έχουν τηρηθεί σωστά ή μια σοβαρή απειλή (πχ όπλα/ πυρομαχικά) έχει εντοπιστεί κατά τη διάρκεια της διαδικασίας. Ο μη λειτουργικός εξοπλισμός μπορεί να είναι μια επιπλέον προϋπόθεση για τη λανθασμένη τήρηση των κανόνων της διαδικασίας ελέγχου.

7. Παραλαβή φορτίων και εμπορευμάτων/ Έλεγχος φορτίων και εμπορευμάτων/ Προσβολή της προστασίας φορτίων και εμπορευμάτων

Στο τομέα της παραλαβής φορτίων και εμπορευμάτων, απειλή μπορεί να αποτελέσει οποιαδήποτε πραγματική ή πιθανή παραβίαση της διαδικασίας αποδοχής των διαδικασιών, ειδικότερα της επαλήθευσης της αλυσίδας της κατοχής φορτίου και αλληλογραφίας με ασφάλεια και ακρίβεια ως προς το παραλήπτη και τον αποστολέα. Όσον αφορά στον έλεγχο φορτίου ή αλληλογραφίας ενδέχεται να μην έχουν τηρηθεί σωστά οι διαδικασίες που πρέπει να ακολουθηθούν ή μια σοβαρή απειλή να έχει εμφανιστεί κατά τον έλεγχο τους. Αυτή η κατάσταση αφορά προβληματικό ή μη λειτουργικό εξοπλισμό. Για αυτό μπορεί να ευθύνεται η ελλιπής ή ανεπαρκής εκπαίδευση ή επιτήρηση (πχ λανθασμένο σφράγισμα φορτίου/

συσκευασίας ή ελλιπής ασφάλεια κατά τη μεταφορά). Τέλος πιθανή απειλή μπορεί να αποτελέσει οποιαδήποτε κατάσταση όπου πραγματοποιείται μη εξουσιοδοτημένη πρόσβαση σε φορτίο περιορισμένης πρόσβασης αφού έχει ασφαλιστεί. Σε αυτή τη κατηγορία συμπεριλαμβάνεται η πρόσβαση στις αποθήκες φορτίου ή εσφαλμένος εξοπλισμός είτε η μη τήρηση των σωστών κανόνων και διαδικασιών.

8. Έλεγχος ασφάλειας εφοδιασμού κατά τη διάρκεια της πτήσης/ Προστασία εφοδιασμού κατά τη διάρκεια της πτήσης

Ο τομέας της ασφάλειας εφοδιασμού μπορεί να υποστεί ελλείψεις και απειλές όσον αφορά τη μεταφορά προμηθειών μιας πτήσης. Αυτό συμπεριλαμβάνει τις διαδικασίες της ασφάλειας τους, δηλαδή τον έλεγχο πρόσβασης στις εγκαταστάσεις των προμηθειών, την καταγραφή και ταυτοποίηση τους και τον έλεγχο τους (αν χρειάζεται). Ακόμα, οποιαδήποτε πραγματική ή πιθανή κατάσταση παρεμβολής με τις προμήθειες της πτήσης αποτελεί πρόβλημα για τη διαδικασία εφοδιασμού της πτήσης. Μπορεί να επηρεάσει η λανθασμένη ή προβληματική λειτουργία του εξοπλισμού ελέγχου (πχ εξοπλισμός σφραγίσματος προμηθειών) όπως και τη μη τήρηση κανόνων και διαδικασιών λόγω ελλιπούς ή ανεπαρκούς εκπαίδευσης ή επιτήρησης (πχ έλλειψης στη διαδικασία σφραγίσματος ή ανεπαρκή ασφάλεια κατά τη διάρκεια της μεταφοράς).

9. Έλεγχοι ασφαλείας εφοδιασμού αεροδρομίου/ Προσβολή προστασίας εφοδιασμού αεροδρομίου

Παρόμοια με τον έλεγχο ασφαλείας εφοδιασμού κατά τη διάρκεια της πτήσης, στο αεροδρόμιο, η συγκεκριμένη διαδικασία μπορεί να υποστεί ελλείψεις ή απειλές σχετικές με τις διαδικασίες ασφαλείας για τις προμήθειες του αεροδρομίου συμπεριλαμβανομένου του ελέγχου πρόσβασης στις εγκαταστάσεις των προμηθειών, την καταγραφή και ταυτοποίηση τους και τον έλεγχο τους. Τέλος, η διαδικασία της προστασίας του εφοδιασμού του αεροδρομίου μπορεί να εμφανίσει προβλήματα στη περίπτωση που υπάρξει οποιαδήποτε κατάσταση παρεμπόδισης με τις προμήθειες του αεροδρομίου. Αυτή η κατάσταση συμπεριλαμβάνει λανθασμένη ή προβληματική λειτουργία του εξοπλισμού ελέγχου (πχ εξοπλισμός σφραγίσματος προμηθειών) όπως και τη μη τήρηση κανόνων και διαδικασιών λόγω ελλιπούς ή ανεπαρκούς εκπαίδευσης ή επιτήρησης (πχ έλλειψης στη διαδικασία σφραγίσματος ή ανεπαρκή ασφάλεια κατά τη διάρκεια της μεταφοράς).

10. Ανυπάκουος / Υπό την επήρεια ουσιών επιβάτης

Όταν ένα άτομο αποτυγχάνει να ακολουθήσει και να σεβαστεί τους κανόνες συμπεριφοράς κατά τη διάρκεια που βρίσκεται στο αεροδρόμιο είτε στο αεροσκάφος χαρακτηρίζεται ως ανυπάκουος επιβάτης. Αυτή η κατάσταση συμπεριλαμβάνει την άρνηση αυτού του ατόμου να τηρήσει τις οδηγίες στου προσωπικού του αεροδρομίου ή των μελών του πληρώματος. Ως αποτέλεσμα έχει την αναστάτωση της σωστής λειτουργίας του αεροδρομίου και του αεροσκάφους.

(συμπεριλαμβάνονται καταστάσεις απειθαρχίας στο έδαφος αλλά και στον αέρα, κατά τη διάρκεια της πτήσης).

11. Σαμποτάζ ή καταστροφή στο έδαφος

Σαμποτάζ χαρακτηρίζεται οποιαδήποτε πραγματική ή ύποπτη κατάσταση όπου διακυβεύεται η ασφάλεια του αεροσκάφους όσο βρίσκεται ακόμα στο έδαφος. Τέτοια κατάσταση μπορεί να είναι η πειρατεία, βομβιστική επίθεση, συσκευή ή ουσία που απειλεί την ασφάλεια του αεροσκάφους και των επιβατών. Συμπεριλαμβάνονται και καταστάσεις σαμποτάζ σε αυτή τη κατηγορία (πχ CBR agents, σύστημα πυραύλων, πλαστογραφημένη υπογραφή).

12. Απειλές κατά τη διάρκεια της πτήσης

Παρόμοια με το σαμποτάζ στο έδαφος, έτσι και οποιαδήποτε πραγματική ή ύποπτη κατάσταση όπου διακυβεύεται η ασφάλεια του αεροσκάφους όσο βρίσκεται στον αέρα μπορεί να φέρει καταστροφή κατά τη διάρκεια της πτήσης. Τέτοια κατάσταση μπορεί να είναι η αεροπειρατεία, βομβιστική επίθεση, συσκευή ή ουσία που απειλεί την ασφάλεια του αεροσκάφους και των επιβατών. (πχ CBR agents, σύστημα πυραύλων που στοχεύουν κίνηση στον αέρα, προβλήματα που αφορούν τη πόρτα του αεροσκάφους, στρατιωτικές αποστολές που επηρεάζουν την εναέρια κυκλοφορία).

13. Μεταφορά όπλων και ένοπλων ατόμων

Η ενότητα αναφέρεται στη μη εξουσιοδοτημένης μεταφορά όπλων ή ένοπλων ατόμων. Αυτή η κατάσταση προϋποθέτει την μη τήρηση των κανόνων (όσον αφορά λανθασμένο τρόπο συσκευασίας ή λανθασμένη καταγραφή γεγονότων που οφείλεται σε ελλιπή εκπαίδευση η επιτήρηση).

14. Ανώνυμα αεροσκάφη

Απειλή η οποία προκαλείται από drone ή από UAV (unmanned aerial vehicle) που χρησιμοποιείται για την προσβολή της ασφάλειας του αεροσκάφους, των επιβατών ή της υποδομής του αεροδρομίου.

15. Άλλες ποινικές πράξεις

Στις λοιπές ποινικές πράξεις που επηρεάζουν αρνητικά τη λειτουργία του αερολιμένα και μπορεί να θέσουν σε κίνδυνο τη ζωή όλων των εμπλεκόμενων ατόμων είναι τα Ναρκωτικά / Παράνομα χρήματα / Κλοπές εντός του αεροδρομίου και κατά τη διάρκεια της πτήσης / Διακίνηση λευκής σαρκός. Επιπρόσθετα, οποιαδήποτε πραγματική ή πιθανή παράνομη πρόσβαση σε πληροφορίες σχετικές με την ασφάλεια, οι οποίες μπορεί να οδηγήσουν σε μια πράξη παράνομης εμπλοκής.

16. Αποδοχή επιβατών στο αεροδρόμιο και στις πτήσεις

Αυτή η κατηγορία περιλαμβάνει οποιαδήποτε πραγματική ή πιθανή παραβίαση της αποδοχής των διαδικασιών ελέγχου λαμβάνει χώρα στην υποδομή του αερολιμένα και εντός των πτήσεων. (πχ ταυτοποίηση λίστας επιβατών, τήρηση των κανόνων των προσωπικών δεδομένων των επιβατών, παραβίαση της διαδικασίας των απελαθέντων και των συνοδευόμενων (DEPA), ασυνόδευτοι απελαθέντες (DEPU), ανεπίτρεπτοι επιβάτες (INAD) σε μια πτήση όσον αφορά τη διαδικασία μεταφοράς τους, μη δηλωμένοι επιβάτες και λανθασμένα στοιχεία και δεδομένα επιβατών). Αυτή η κατάσταση περιλαμβάνει ελλιπή λειτουργία του εξοπλισμού, όπως και καταστάσεις που οι σωστές διαδικασίες δεν έχουν ακολουθηθεί.

17. Κυβερνοασφάλεια

Απειλή στη κυβερνοασφάλεια χαρακτηρίζεται οποιαδήποτε πραγματική ή πιθανή παραβίαση της διαδικασίας πρόσβασης στο δίκτυο ή στον εξοπλισμό ασφαλείας και στα βασικά συστήματα που χρησιμοποιούνται για επιχειρησιακούς σκοπούς. Η συγκεκριμένη κατηγορία αφορά τον έλεγχο πρόσβασης υλικού και λογισμικού σχετικά με το αεροσκάφος, τον αερολιμένα των κρίσιμων συστημάτων ασφαλείας που σχετίζονται με τη διαχείριση της αεροπορικής κυκλοφορίας ATM, όπως τον προγραμματισμό πτήσεων, προετοιμασία πτήσεων και επικοινωνία εν μέσω πτήσης[80].

Το πεδίο των κυβερνοαπειλών έχει πρόσφατα εισάγει ένα νέο τοπίο απειλών. Επιπλέον, πρόσφατες ερευνητικές μελέτες αποκάλυψαν ότι η κυβερνοαπειλή πιθανότατα θα είναι ένα από τα κύρια θέματα ασφαλείας στην αεροπορία, καθώς σύμφωνα με τα προγράμματα SESAR και NextGen το συνολικό σύστημα αερομεταφορών θα μεταβεί μαζικά σε υποδομές βασισμένες σε IP και θα λειτουργεί σύμφωνα με τον συνεκτικό δικτυακό τρόπο λειτουργίας, με κοινοποίηση πραγματικού χρόνου πληροφοριών. Ως κρίσιμος πόρος, οι πληροφορίες πρέπει να αντιμετωπίζονται όπως οποιοδήποτε άλλο κρίσιμο ενεργητικό που είναι απαραίτητο για την αποτελεσματικότητα και την επιτυχή παράδοση των συστημάτων Διαχείρισης της Αεροπορικής Κυκλοφορίας (ATM). Στον τομέα της κυβερνοασφάλειας της αεροπορίας, ερευνητικό έργο έχει δείξει ότι η πολυπλοκότητα και η κρισιμότητα της ασφάλειας των πληροφοριών και η διακυβέρνησή της απαιτούν το υψηλότερο επίπεδο οργανωτικής ασφάλειας.[81]

3.2.2. Οι κυριότεροι παράγοντες απειλών

Ο τομέας της Αεροπορίας και οι αερολιμένες αντιμετωπίζουν συνεχείς προκλήσεις και απειλές που επηρεάζουν τη λειτουργία και την ασφάλεια των επιβατών και των εργαζομένων. Οι απειλές αυτές ποικίλλουν, από φυσικά φαινόμενα, καιρικές συνθήκες αλλά και προκλήσεις σχετικές με

[80] IATA - Categories of Aviation Security Occurrences SeMS Edition 5 (iata.or g)
[81] Lykou, G., Iakovakis, G., Gritzalis, D. (2019):
(PDF) Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies (researchgate.net)

την ασφάλεια, οπως τρομοκρατικές επιθέσεις και κυβερνοεπιθέσεις. Η σημαντικότερη προσέγγιση για το περιορισμό και την εξάλειψη των απειλών είναι η ανάλυση των παραγόντων τους, δηλαδή η κατανόηση της πηγής των απειλών και των κινητήριων δυνάμεων πίσω από ένα περιστατικό . Η αναγνώριση επομένως των κινήτρων και των στόχων που βρίσκονται πίσω από τις απειλές σε μια υποδομή ενός αερολιμένα, είναι η αρχή για την επίλυση του προβλήματος.

Αναλυτικότερα, η αναγνώριση του κινήτρου μπορεί να καθορίσει το σκοπό του επιτιθέμενου και να βοηθήσει τον εκάστοτε οργανισμό να προσδιορίσει ποιά είναι τα αγαθά που πρέπει να προστατεύσει και πώς πρέπει να ενεργήσει. Επιπλέον βοηθά στην κατανόηση των προθέσεων των επιτιθέμενων, ώστε να υπάρξει εστίαση των προσπαθειών προς την άμυνα εναντίον του πιο πιθανού σεναρίου επίθεσης για οποιοδήποτε περιουσιακό στοιχείο αξίας. [82]

Σύμφωνα με τον ENISA, η αξιολόγηση των κινήτρων πίσω από τα περιστατικά που παρατηρήθηκαν κατά τη διάρκεια της περιόδου αναφοράς της έρευνας, καθορίζει 5 διαφορετικές μορφές κινήτρων που μπορούν να συνδεθούν με τις απειλές στην υποδομή του αερολιμένα:

- Οικονομικό κέρδος

Είναι γεγονός ότι ο τομέας των αερομεταφορών θεωρείται επικερδής επιχείρηση και πολλοί μπορούν να στραφούν προς αυτόν για το οικονομικό κέρδος. Όσον αφορά το συγκεκριμένο κίνητρο, οποιαδήποτε παρεμβατική ενέργεια που έχει απώτερο σκοπό το οικονομικό κέρδος για τον επιτιθέμενο αποτελεί απειλή για τον αερολιμένα.

- Κατασκοπευτική δραστηριότητα

Τα δεδομένα των επιβατών θεωρούνται εμπορεύσιμα και οι πληροφορίες που αφορούν την εφοδιαστική αλυσίδα των μεταφορών έχουν υψηλή αξία. Συνεπώς προκύπτει η ανάγκη κατοχής τους από κακόβουλους με αποτέλεσμα να προβαίνουν σε κατασκοπευτική δραστηριότητα που μπορεί να θέσει σε κίνδυνο διαδικασίες και προσωπικές πληροφορίες επιβατών και εργαζομένων.

- Γεωπολιτική διαταραχή / Λειτουργική διαταραχή

Ένα σημαντικό κίνητρο επιθέσεων είναι επίσης η διαταραχή του γεωπολιτικού περιβάλλοντος και η λειτουργική διαταραχή του αερολιμένα. Κυρίως αυτές οι απειλές εκτελούνται από ομάδες υποστηριζόμενες από το κράτος. Οι συνέπειες των διαταραχών εν δυνάμει μπορούν να επηρεάσουν όλες τις επιχειρησιακές λειτουργίες του αερολιμένα.

- Καταστροφή

[82] ENISA Threat Landscape, 2023:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ένα κίνητρο που αποτελεί απειλή για την υποδομή ενος αερολιμένα είναι οποιαδήποτε κακόβουλη κίνηση αποσκοπεί σε καταστροφικές συνέπειες για τον αερολιμένα και τη λειτουργία του (πχ τρομοκρατικές ενέργειες). Μπορεί να υποκινείται από οργανωμένες ομάδες ή μεμονωμένα άτομα.

- Ιδεολογικό κίνητρο

Το ιδεολογικό κίνητρο είναι οποιαδήποτε ενέργεια υποστηρίζεται από μια ιδεολογία και σκοπεύει στη παρενόχληση διαδικασιών και επιχειρησιακών λειτουργιών του αερολιμένα (όπως πχ το hacktivism όσον αφορά την απειλή της κυβερνοασφάλειας).[83]

Οι αερολιμένες έρχονται αντιμέτωποι με διάφορους στόχους απειλών λόγω της κρίσιμης σημασίας τους στην εθνική και διεθνή μεταφορά. Βασιζόμενοι λοιπόν στο πίνακα των πιθανών απειλών των αερολιμένων ανα κατηγορία (3.2.1) αλλά και στα κίνητρα που κρύβονται πίσω από αυτές τις απειλές αυτές (3.2.2), γίνονται ξεκάθαροι οι στόχοι των απειλών αυτών προς τους αερολιμένες.

- Ασφάλεια Πτήσεων και Επιβατών

Σε αυτή τη κατηγορία συμπεριλαμβάνονται επιθέσεις προς την αεροπορική ασφάλεια, όπως τρομοκρατικές επιθέσεις ή εισαγωγή παράνομων αντικειμένων στο αεροδρόμιο που μπορεί να απειλήσουν την ασφάλεια των επιβατών και των πτήσεων.

- Παρεμπόδιση λειτουργικότητας και Ασφάλειας υποδομής

Οι αερολιμένες αντιμετωπίζουν φυσικές επιθέσεις ή κυβερνοεπιθέσεις σε κτήρια, σε πίνακες ελέγχου, συστήματα εντοπισμού και ελέγχου (πχ η διακοπή της λειτουργίας μπορεί να είναι είναι στόχοι μιας επίθεσης).

- Προσβολή κυβερνοασφάλειας

Οποιαδήποτε επίθεση σχετίζεται με την ασφάλεια των πληροφοριακών συστημάτων του αερολιμένα εμπεριέχεται σε αυτή τη κατηγορία. Από τα πιο συχνά παραδείγματα τέτοιων επιθέσεων σε υποδομές αερολιμένων είναι το κακόβουλο hacking, με στόχο την μη εξουσιοδοτημένη πρόσβαση χρησιμοποιώντας γνωστές τεχνικές αποκρυπτογράφησης κωδικών πρόσβασης, οι επιθέσεις υποκλοπής δεδομένων & η μόλυνση συστημάτων με κακόβουλο λογισμικό.

- Οικονομικές απειλές

[83] ENISA Transport Threat Landscape,2023
https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

Στόχος του επιτιθέμενου μπορεί να είναι η αναστάτωση της οικονομικής σταθερότητας του αερολιμένα και της ομαλής ροής των επικερδών επιχειρήσεων του.

- Εθνική Ασφάλεια

Οι υποδομές των αερολιμένων είναι κομβικά σημεία για την εθνική ασφάλεια και για αυτό το λόγο αποτελούν στόχο για απειλές που σχετίζονται με γεωπολιτικά ή και εθνικά συμφέροντα.[84]

3.3. Διαχείριση επικινδυνότητας και ανθεκτικότητα

3.3.1. Αποτίμηση επικινδυνότητας των απειλών των Αερολιμένων

Η αποτίμηση της επικινδυνότητας των απειλών στους αερολιμένες αποτελεί το δεύτερο βήμα του σχεδίου διαχείρισης των απειλών για την ασφάλεια της υποδομής, καθώς το πρώτο αποτελεί η αναγνώριση των πιθανών απειλών και κινδύνων που αναλύθηκαν στη προηγούμενη ενότητα. Η αποτίμηση επικινδυνότητας είναι ένα διαδικαστικό βήμα κατά το οποίο εκτιμάται ο βαθμός κινδύνου που συνδέεται με μια συγκεκριμένη δραστηριότητα, κατάσταση ή συμβάν. Στην ασφάλεια του αεροπορικού τομέα, η διαδικασία αυτή περιλαμβάνει τον προσδιορισμό & τον χαρακτηρισμό των πιθανών κινδύνων και παραγόντων που επηρεάζουν την εκτίμηση των απειλών.[85]

Η διαδικασία της αποτίμησης της επικινδυνότητας ακολουθεί συγκεκριμένα βήματα τα οποία μπορούν να οδηγήσουν στην απόφαση για την εξάλειψη των πιθανών κινδύνων που εγκυμονούν για την υποδομή του αερολιμένα, με σκοπό την εξασφάλιση της ασφάλειας του.Τα βήματα είναι τα εξής:

1. **Αναγνώριση κινδύνων**

Σε αυτό το βήμα πραγματοποιείται ο προσδιορισμος όλων των πιθανών κινδύνων που μπορεί να προκύψουν σε έναν αερολιμένα. Στη προηγούμενη ενότητα (3.2.1) αναφέρθηκαν όλες οι περιπτώσεις πιθανών απειλών για τις κρίσιμες υποδομές των αερολιμένων, σύμφωνα με τον πίνακα της Διεθνούς Ένωσης Αερομεταφορών (IATA). Η αναγνώριση κινδύνων αποτελεί απαραίτητη προϋπόθεση για την αποτίμηση επικινδυνότητας καθώς η αναγνώριση των γεγονότων, των συμβάντων και των εμπλεκόμενων είναι το πρώτο βήμα για την εξάλειψη της απειλής.

2. **Αξιολόγηση πιθανότητας**

[84] Ukwandu E. et al.Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information 2022, 13, 146, Academic Editor: Sokratis Katsikas https://doi.org/10.3390/info13030146

[85] ICAO (2011) Manual on Threat Assesment and Risk Management Methodology https://www.icao.int/SAM/Documents/2012/ICAOLACACAVSECRG2/Manual%20on%20Threat%20Assessment%20and%20Risk%20Management%20Methology%20NoLogos.pdf

Η αξιολόγηση της πιθανότητας κάθε απειλής αποτελεί σημαντικό κομμάτι στο σχέδιο της αποτίμησης επικινδυνότητας, καθώς σε αυτό το βήμα γίνεται εκτίμηση της πιθανότητας εκδήλωσης κάθε κινδύνου, γεγονός που βοηθάει στην προτεραιοποίηση των απειλών για τον αερολιμένα άρα και στην πιο γρήγορη και εύστοχη δημιουργία ενός σχεδίου εξάλειψης των απειλών της κρίσιμης υποδομής.

3. **Αξιολόγηση σοβαρότητας**

Αναλόγως την εκάστοτε απειλή που κρίνεται να αντιμετωπίσει ο αερολιμένας, πραγματοποιείται εκτίμηση του βαθμού σοβαρότητας και των επιπτώσεων της απειλής, έτσι ώστε να γίνει η κατηγοριοποίηση των απειλών. Ο σκοπός αυτού του βήματος είναι να δοθεί προτεραιότητα σε κινδύνους που παράδειγμα αποτελούν μεγαλύτερη απειλή για τον αερολιμένα ή συμβαίνουν με μεγαλύτερη συχνότητα και αποφέρουν σοβαρότερες συνέπειες στην υποδομή.

4. **Αξιολόγηση κινδύνου**

Αυτό το βήμα συνδυάζει τα αποτελέσματα από τα δύο προηγούμενα βήματα. Μέσω της αξιολόγησης της πιθανότητας και της σοβαρότητας του κινδύνου μπορεί να γίνει η τελική αξιολόγηση του. Μέσα από αυτή την αξιολόγηση πλέον η απειλή έχει κατηγοριοποιηθεί σύμφωνα με το πόσο πιθανό είναι να συμβεί στον αερολιμένα και έχει καθοριστεί πόσο ψηλά βρίσκεται στη κλίμακα της σοβαρότητας για τη συγκεκριμένη υποδομή.

5. **Λήψη αποφάσεων**

Τέλος, αφού οι απειλές έχουν αναγνωρισθεί και κατηγοριοποιηθεί σύμφωνα με τα παραπάνω κριτήρια βήματα, η λήψη αποφάσεων για την αντιμετώπιση της απειλής αποτελεί το τελευταίο βήμα για την αποτίμηση της επικινδυνότητας των απειλών των αερολιμένων. Σε αυτό το βήμα παίρνονται αποφάσεις και αποφασίζονται οι κατάλληλες παρεμβάσεις με σκοπό τη διαχείριση του κινδύνου της απειλής με ορισμενες δράσεις.[86]

Σύμφωνα με τον ENISA (2016), υπάρχουν 5 κατηγορίες απειλών για τη κυβερνοασφάλεια στους αερολιμένες, κάθε μια από τις οποίες αποτελείται από επιμέρους κινδύνους. Παρακάτω παρατίθεται ένας πίνακας που περιέχει δύο παραδείγματα για την απειλής της κυβερνοασφάλειας ενός αερολιμένα. Με βάση τις συγκεκριμένες απειλές έχουν εφαρμοστεί τα βήματα της αποτίμησης επικινδυνότητας.[87]

[86] ENISA Threat Landscape, 2023:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[87] ENISA. (2016). Securing Smart Airports [Report/Study]
https://www.enisa.europa.eu/publications/securing-smart-airpor

ΑΠΟΤΙΜΗΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΑΠΕΙΛΗΣ		
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
1. ΑΝΑΓΝΩΡΙΣΗ ΚΙΝΔΥΝΩΝ	Κακόβουλη χρήση εξουσίας / αδειοδότησης	DoS attack (Denial of Service / Επίθεση άρνησης εξυπηρέτησης)
2. ΑΞΙΟΛΟΓΗΣΗ ΠΙΘΑΝΟΤΗΤΑΣ	ΠΟΛΥ ΠΙΘΑΝΟ ● Η κακόβουλη χρήση διαπιστευτηρίων για εξουσιοδότηση γίνεται κυρίως μέσω phishing. Το Phishing αποτελεί μια εύκολη και φθηνή τεχνική για τον επιτιθέμενο.	ΕΛΑΧΙΣΤΑ ΠΙΘΑΝΟ ● Ο επιτιθέμενος χρειάζεται εξειδικευμένο και ακριβό εξοπλισμό που αναλογικά με τον εξοπλισμό ενός αερολιμένα είναι δύσκολο να αποκτήσει.
3. ΑΞΙΟΛΟΓΗΣΗ ΣΟΒΑΡΟΤΗΤΑΣ	ΜΙΚΡΗ ΕΩΣ ΜΕΓΑΛΗ ● Εξαρτάται από το επίπεδο προνομίων που έχει το άτομο του οποίου τα διαπιστευτήρια εκμεταλλεύεται ο επιτιθέμενος.	ΜΕΓΑΛΗ ● Μια επιτυχημένη DoS attack μπορεί να “παγώσει” τη λειτουργία του αερολιμένα.
4. ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΟΥ	ΕΠΙΚΙΝΔΥΝΟ ΕΩΣ ΠΟΛΥ ΕΠΙΚΙΝΔΥΝΟ Επιπτώσεις: ● Κλοπή διαπιστευτηρίων μέσω phishing ● Εκμετάλλευση λογισμικού ● Επιθέσεις διακομιστών ● Κακόβουλο λογισμικό ● Κατάχρηση προνομίων	ΠΟΛΥ ΕΠΙΚΙΝΔΥΝΟ Επιπτώσεις: ● Πιθανή ολική διακοπή δικτύου και συστημάτων ● Επιβράδυνση ελέγχου ασφαλείας ● Καθυστερήσεις επιβατών ● Ακυρωμένες πτήσεις ● Απώλεια εμπιστοσύνης ● Οικονομικές ζημιές

5. ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ	Ο αερολιμένας πρέπει να ενσωματώσει πολιτικές και να εκπαιδεύσει σωστά τους χειριστές/ χρήστες για τη προστασία των διαπιστευτηρίων τους.	Ο αερολιμένας πρέπει να λάβει δραστικά μέτρα και να κατέχει τον απαραίτητο εξοπλισμό και τους χειριστές για την αντιμετώπιση και την πρόληψη μιας τέτοιας επίθεσης

3.3.2. Μέτρα ασφαλείας και μείωσης κινδύνου

Η ασφάλεια αποτελεί υψηλή προτεραιότητα για τη βιομηχανία της αεροπορίας και περιλαμβάνεται σε όλες τις λειτουργίες της. Γι' αυτό το λόγο είναι κρίσιμη η διαχείριση της ασφάλειας με το καλύτερο δυνατό τρόπο. Οι απειλές στο τομέα της αεροπορίας συνεχίζουν να εξελίσσονται. Αεροπορικές εταιρείες, αεροδρόμια, κυβερνήσεις, διεθνείς οργανισμοί και ανεξάρτητοι φορείς της αεροπορίας προσπαθούν να ενισχύσουν και να αναπτύξουν τις δυνατότητες ασφαλείας της αεροπορίας. Η σημασία της διαχείρισης περιστατικών, της συνεργασίας των φορέων και της διασφάλισης της ασφάλειας συνεπώς δεν πρέπει να υποβιβάζονται. Η βιομηχανία πρέπει να προσαρμόζεται διαρκώς στους συνεχώς μεταβαλλόμενους κανονισμούς. και τις προκλήσεις που παρουσιάζονται, καθώς ταυτόχρονα να επιχειρεί τη διεύρυνση και την εξέλιξη των λειτουργιών της.[88]

Το τρίτο βήμα για την επιτευξη της ασφάλειας στον αεροπορικό τομέα αποτελεί η λήψη μέτρων ασφαλείας για τη μείωση των κινδύνων που έχουν εντοπιστεί για τον αερολιμένα από την αποτίμηση της επικινδυνότητας των απειλών του. Ακολουθώντας τις προαναφερθείσες απειλές των υποδομών των αερολιμένων, τα μέτρα ασφαλείας για τη μείωση του κινδύνου κατηγοριοποιούνται σε 7 κατηγορίες. Κάθε αερολιμένας πρέπει να εξασφαλίζει μέτρα ασφαλείας για τη :

1. Φυσική ασφάλεια, που περιλαμβάνει:

- Έλεγχο πρόσβασης στην υποδομή του αερολιμένα
- Περιφερειακή προστασία της υποδομής και της περιοχής γύρω από αυτή
- Ανίχνευση ύποπτων και επικίνδυνων αντικειμένων, εμπορευμάτων και επιβατών
- Ελέγχους στις διαδικασίες του ελέγχου εμπορευμάτων και επιβατών
- Προστασία περιβάλλοντος εντός και περιφερειακά του αερολιμένα (πχ χλωρίδα, πανίδα, ηχορύπανση κλπ)

[88] IATA, 2023:IATA - What You Need to Know About Aviation Security

2. Ασφάλεια προσωπικού, που περιλαμβάνει:

- Διαχείριση πρόσβασης χρηστών και των προνομίων τους στα πληροφοριακά συστήματα του αεροδρομίου
- Αποσαφήνιση των διαδικασιών ασφαλείας που πρέπει να ακολουθούν εντός και εκτος του αερολιμένα
- Διαχωρισμός καθηκόντων στην εκάστοτε θέση εργασίας
- Πολιτική πρόσληψης του προσωπικού
- Κανονισμούς προσωπικού
- Εκπαίδευση / Ευαισθητοποίηση και κατάρτιση του προσωπικού

3. Ασφάλεια πληροφοριών, που περιλαμβάνει:

- Προστασία πληροφοριών, ακολουθώντας την αρχή CIA: Εμπιστευτικότητα, Διαθεσιμότητα, Ακεραιότητα
- Κρυπτογραφία για τη προστασία των ευαίσθητων δεδομένων και επικοινωνιών μεταξύ των συστημάτων των αερολιμένων
- Χειρισμό μέσων από καταρτισμένο προσωπικό που έχει λάβει τη κατάλληλη εκπαίδευση
- Αντίγραφα ασφαλείας συστημάτων και δεδομένων πτήσεων, λογισμικού, εξοπλισμού, συστημάτων δικτύου και επικοινωνιών
- Ενημερώσεις λογισμικού και ενημερώσεις προγραμμάτων

4. Ασφάλεια επικοινωνίας, που περιλαμβάνει:

- Απομόνωση δικτύου, που συνίσταται στο διαχωρισμό δικτύων σε διαφορετικές διαδικασίες ή φυσικά δίκτυα για το περιορισμό πρόσβασης και την ελαχιστοποίηση του κινδύνου διαρροής πληροφοριών ή επιθέσεων.
- Διαχείριση ασφαλείας επικοινωνίας ανάμεσα στο προσωπικό, τους επιβάτες, τις εγκαταστάσεις και τα αεροσκάφη
- Διαχείριση ανίχνευσης εισβολών στον αερολιμένα
- Καταγραφή συμβάντων
- Πολιτικές για τηλεργασία και φορητές συσκευές του προσωπικού του αερολιμένα

5. Υποστήριξη Πληροφοριών, που είναι μια απαραίτητη προϋπόθεση για τις αξιολογήσεις απειλών και περιλαμβάνει:

- Την παρακολούθηση των απειλών και τον καθορισμό των επιπέδων ειδοποίησης ασφαλείας

6.Ανταλλαγή πληροφοριών ασφάλειας, που περιλαμβάνει:

- Ανταλλαγή πληροφοριών μεταξύ εθνικών αρχών, οργανισμών ασφάλειας και πληροφοριών
- Αναγνώριση και ειδοποίηση περιστατικών
- Προειδοποιήσεις ασφάλειας και τα επίπεδα ειδοποίησης
- Αναφορά και παρακολούθηση επιπτώσεων περιστατικών

7. Λειτουργική συνέχεια, που περιλαμβάνει:

- Ανταπόκριση σε έκτακτες καταστάσεις
- Διαχείριση συνέχειας επιχειρήσεων και σχεδίαση των πιθανών κινδύνων[89]

3.3.3. Καλές πρακτικές ανθεκτικότητας

Όσο εξελίσσονται οι καιροί τεχνολογικά και ο φόρτος εργασίας στα αεροδρόμια αυξάνεται, οι πιθανές απειλές που μπορεί να εμφανιστούν ποικίλλουν και πολλές φορές αποτελούν πρόκληση στην επίλυση τους. Είναι απαραίτητο να θεσπιστεί ένα συνεργατικό μοντέλο για τον καθορισμό στόχων και τον ορισμό μιας κατάλληλης προσέγγισης για την επίλυση των προβλημάτων που μπορεί να προκύψουν, προκειμένου να ενισχυθεί η ανθεκτικότητα του συστήματος αεροπορίας ενάντια στις επιθέσεις. Γι' αυτό το σκοπό, σημαντικές προσπάθειες καταβάλλονται σε διάφορα επίπεδα στην αεροπορική κοινότητα, συμπεριλαμβανομένης της κανονιστικής ρύθμισης, των ομάδων εργασίας για την ασφάλεια, της έρευνας και της εκπαίδευσης. Η αναγνώριση των προκλήσεων που δημιουργούν οι απειλές, οι προσεγγίσεις αξιολόγησης κινδύνου και οι κατευθυντήριες γραμμές για τη βελτίωση της ασφάλειας, είναι προτεραιότητες που αντιμετωπίζονται επί του παρόντος.

Το Ευρωπαϊκό Ινστιτούτο Δικτύων και Πληροφοριών (ENISA) έχει παρουσιάσει μέσω μιας έρευνας, τα Έξυπνα Αεροδρόμια (2016). Αναλυτικότερα, παρουσιάζει το σύγχρονο αεροδρόμιο, τις ανάγκες του, τα προβλήματα που αντιμετωπίζει και το τρόπο που πρέπει να κινηθεί για την ελαχιστοποίηση των απειλών του. Η συγκεκριμένη έρευνα αναφέρει λύσεις για τις απειλές που μπορεί να προκύψουν στις κρίσιμες υποδομές των αεροδρομίων, προκειμένου να βοηθήσει τους ιδιοκτήτες περιουσιακών στοιχείων και όλους τους εμπλεκόμενους όσον αφορά την ασφάλεια των υποδομών αυτών. Ένα από τα κύρια μέρη αυτής της έρευνας είναι η ανασκόπηση των καλών πρακτικών (Good Practices) που μπορεί να εφαρμόσει ο αερολιμένας για την εξασφάλιση της ανθεκτικότητας του απέναντι στις απειλές που παρουσιάζονται.

Οι καλές πρακτικές σύμφωνα με τον ENISA για τα Έξυπνα αεροδρόμια χωρίζονται σε τρεις κύριες ομάδες:

[89] Lykou, G., Iakovakis, G., Gritzalis, D. (2019). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer, Cham. (PDF) Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies (researchgate.net)

- Τεχνικές / με βάση εργαλεία,
- Πολιτικές και πρότυπα
- Οργανωτικές, Ανθρώπινοι πόροι και Διαδικασίες.

Για τη καλύτερη κατανόηση των καλών πρακτικών των Έξυπνων Αεροδρομίων θα γίνει μια μελέτη περίπτωσης σε αντιστοιχία με τις απειλές στις οποίες πραγματοποιήθηκε αποτίμηση επικινδυνότητας στην ενότητα 3.3.1.Αναλυτικότερα, η κακόβουλη χρήση εξουσίας/ αδειοδότησης όπως αναφέρθηκε γίνεται κυρίως μέσω του phishing. Ακόμα θα γίνει ανάπτυξη των καλών πρακτικών για την επίθεση DoS attack (Επίθεση άρνησης εξυπηρέτησης).[90]

Καλές Πρακτικές (Good Practices)	Phishing (Κακόβουλη χρήση εξουσίας / αδειοδότησης)	DoS attack (Επίθεση άρνησης εξυπηρέτησης)
1. Τεχνικές /Με βάση εργαλεία	Έρευνα με χρήση εικονικών περιβαλλόντων	Εργαλεία ανίχνευσης/ ταξινόμησης/αντίδρασης
2. Πολιτικές & Πρότυπα	Διεξαγωγή τεχνικών αποτίμησης της επικινδυνότητας (risk assessment management)	Τακτική άσκηση σε δοκιμαστικά περιστατικά ● Προετοιμασίας ● Χρόνου αντίδρασης
3.Οργανωτικές, Ανθρώπινοι πόροι & Διαδικασίες	Οι επιθέσεις phishing και κοινωνικού μηνύματος λειτουργούν εκμεταλλευόμενες αδυναμίες στην ανθρώπινη ψυχολογία και τον οργανωσιακό πολιτισμό. Συνεπώς η καλύτερη πρακτική όσον αφορά τη μακροχρόνια επίλυση του συγκεκριμένου κινδύνου για τους αερολιμένες είναι η σωστή εκπαίδευση εργαζομένων	Επικοινωνία σε ανωμαλία δραστηριότητας & κακόβουλες επιθέσεις σε διατμηματικό επίπεδο. Οι εμπλεκόμενοι μπορεί να είναι: ● Προσωπικό πληροφορικής ● Ανώτερη διοίκηση ● Οποιοδήποτε ενδιαφερόμενο μέρος ● Προσωπικό επιβολής του νόμου

[90] ENISA. (2016). Securing Smart Airports [Report/Study] ό.π.

Η εξασφάλιση πρακτικών ανθεκτικότητας στα αεροδρόμια είναι σημαντική για τη προστασία της υποδομής από απειλές.[91]

Σύμφωνα με το παραπάνω παράδειγμα, οι επιθέσεις στο κυβερνοχώρο του αερολιμένα μπορούν να προκαλέσουν διακοπές στη λειτουργία των συστημάτων του αεροδρομίου, προκαλώντας προβλήματα στη ασφάλεια, την ακεραιότητα των δεδομένων και την αναλογία των πτήσεων. Η ανθεκτικότητα στις κυβερνοεπιθέσεις βοηθάει τα αεροδρόμια να προστατεύσουν τα συστήματα τους και να διατηρήσουν την ακεραιότητα των λειτουργιών τους. Όπως επίσης προτεραιότητα για τους αερολιμένες αποτελεί και η ασφάλεια των επιβατών και του προσωπικού τους. Η ενίσχυση των μέτρων ανθεκτικότητας μπορεί να προστατεύσει τους επιβάτες και το προσωπικό του αεροδρομίου από τη διακοπή υπηρεσιών και κρίσιμων λειτουργιών του αερολιμένα.

Η διατήρηση της λειτουργικότητας, δηλαδή η έγκαιρη ανίχνευση και αντιμετώπιση επιθέσεων εξασφαλίζει ότι τα αεροδρόμια μπορούν να συνεχίσουν τη λειτουργία τους με τον πλέον αποτελεσματικό τρόπο, ακόμα και κατά περιόδους κρίσης ή επιθέσεων. Ακόμα, η ενίσχυση των μέτρων ασφάλειας και ανθεκτικότητας στα αεροδρόμια εμπνέει εμπιστοσύνη στο κοινό, καθώς αισθάνονται πιο ασφαλείς όταν ταξιδεύουν ή όταν βρίσκονται στο αεροδρόμιο.Συνολικά η εξασφάλιση πρακτικών ανθεκτικότητας στα αεροδρόμια είναι ζωτικής σημασίας για τη διασφάλιση της λειτουργικότητας, της ασφάλειας και της εμπιστοσύνης του κοινού.

ΚΕΦΑΛΑΙΟ 4 : ΑΝΑΠΤΥΞΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΑΕΡΟΠΟΡΙΚΟ ΤΟΜΕΑ

4.1 Εξέλιξη της κυβερνοασφάλειας στον Αεροπορικό Τομέα

4.1.1. Το θεσμικό πλαίσιο στην Ε.Ε. για την ασφάλεια πληροφοριών

Στο πεδίο της αεροπορικής ασφάλειας, ο Βασικός Κανονισμός της Ε.Ε. 2018/1139 του 2018 θέσπισε κοινούς κανόνες στον τομέα της πολιτικής αεροπορίας και ίδρυσε τον EASA σαν αρμόδια αρχή για την εποπτεία της εφαρμογής του. Ο Κανονισμός προβλέπει απαιτήσεις με σκοπό την μείωση της πιθανότητας ατυχημάτων που οφείλονται σε αστοχίες, ανθρώπινα λάθη και φυσικούς κινδύνους. Δεν αντιμετωπίζει ωστόσο το ζήτημα της ασφάλειας πληροφοριών στο περιβάλλον της αεροπορίας και ιδιαίτερα τις κακόβουλες απειλές του κυβερνοχώρου. Με τον εκτελεστικό Κανονισμό 2019/1583 του 2019, καθορίστηκαν προληπτικά μέτρα ασφάλειας στον κυβερνοχώρο, σύμφωνα με νεότερη τροποποίηση του παραρτήματος 17 (security program) της Σύμβασης από τον ICAO. Συγκεκριμένα οι αερομεταφορείς και οι φορείς εκμετάλλευσης αεροδρομίων, οφείλουν να προσδιορίζουν και να προστατεύουν τα κρίσιμα συστήματα πληροφορικής/επικοινωνιών/ δεδομένων τους από επιθέσεις στον κυβερνοχώρο που ενδέχεται

[91] Lykou, G., Iakovakis, G., Gritzalis, D. (2019). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management ό.π.

να επηρεάσουν την ασφάλεια της πολιτικής αεροπορίας και να λαμβάνουν μέτρα για την προστασία τους από έκνομες ενέργειες, τα οποία πρέπει να προσδιορίζονται, αναπτύσσονται και εφαρμόζονται σύμφωνα με αποτίμηση επικινδυνότητας. [92]

Η αυξανόμενη πιθανότητα εκμετάλλευσης των ευπαθειών των πληροφοριακών συστημάτων που υποστηρίζουν τις λειτουργίες της πολιτικής αεροπορίας, με σκοπό τη διατάραξη της ασφάλειας των αερομεταφορών, κατέστησε αναγκαία τη κανονιστική ρύθμιση της διαχείρισης επικινδυνότητας στην ασφάλεια πληροφοριών, με τη προσθήκη νέων απαιτήσεων (Part I.S.), που καλύπτουν ολοκληρωμένα τον τομέα της Κυβερνοασφάλειας. Οι νέες ρυθμίσεις αντιμετωπίζουν τα πληροφοριακά συστήματα που υποστηρίζουν την αεροπορία σαν ένα σύστημα συστημάτων με υψηλό βαθμό διασύνδεσης και αλληλεξάρτησης.Το κανονιστικό πακέτο του Part-IS αποσκοπεί στην παροχή ενός ευέλικτου εργαλείου με τη μορφή ενός ΣΔΑΠ (ISMS) που είναι προσαρμοσμένο στις ανάγκες του τομέα της αεροπορίας. [93]

Παράλληλα με την έκδοση των Οδηγιών NIS 2 και CER, που έχουν ως πεδίο εφαρμογής όλες τις κρίσιμες οντότητες και υποδομές, οι νέοι Κανονισμοί που εκδόθηκαν το 2022 ειδικά για τη διαχείριση επικινδυνότητας στον αεροπορικό τομέα, προβλέπουν την καθιέρωση, εφαρμογή και διατήρηση από τους αερομεταφορείς, παρόχους υπηρεσιών αεροναυτιλίας και άλλους εμπλεκόμενος φορείς, ενός Συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ISMS). Στόχος είναι η ορθή διαχείριση των κινδύνων για την ασφάλεια των πληροφοριών, οι οποίοι ενδέχεται να έχουν αντίκτυπο στην ασφάλεια της αεροπορίας. Τα κύρια βήματα της διεργασίας αποτίμησης επικινδυνότητας είναι η ανίχνευση των περιστατικών ασφαλείας, η αναγνώρισή τους, η απόκριση και η ανάκαμψη μετά από αυτά, σε συνδυασμό με τη συνεχή βελτίωση του ΣΔΑΠ, την αναθεώρηση της αποτίμησης επικινδυνότητας και κυρίως τον διαμοιρασμό πληροφοριών με τους ενδιαφερόμενους φορείς [94]

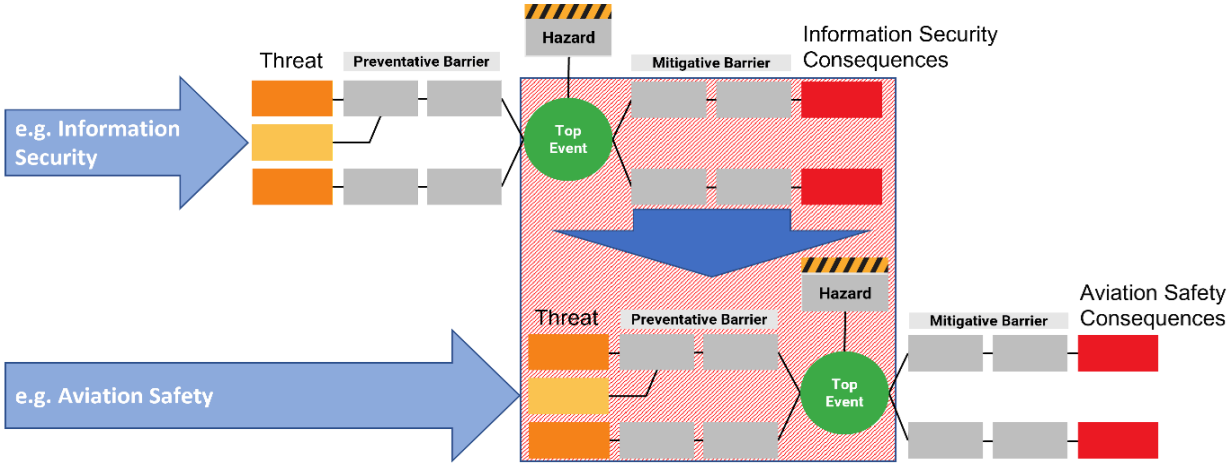
Οι απαιτήσεις για εγκατάσταση ενός ΣΔΑΠ, όπως προβλέπονται στο Part I.S., σε γενικές γραμμές είναι συμβατές με το Πρότυπο ISO/IEC 27001, με το οποίο είναι πιστοποιημένες πολλές επιχειρήσεις του αεροπορικού τομέα, ωστόσο υπάρχουν εξειδικευμένες απαιτήσεις στον τομέα της αεροπορικής ασφάλειας. Υπάρχει δυνατότητα επέκτασης του ΣΔΑΠ που βασίζεται στο ISO, προκειμένου να περιλάβει και τις απαιτήσεις του Part I.S. Παράλληλα όμως, θα πρέπει να συμπεριληφθεί η αεροπορική ασφάλεια στην οργανωσιακή διαχείριση επικινδυνότητας, με

[92] ΕΕ -ΚΑΝΟΝΙΣΜΟΣ 2019/1583 της 25 Σεπτ 2019 για την τροποποίηση του εκτελεστικού κανονισμού 2015/1998 σχετικά με τον καθορισμό λεπτομερών μέτρων εφαρμογής των κοινών βασικών προτύπων ασφάλειας των αερομεταφορών από έκνομες ενέργειες, όσον αφορά τα μέτρα ασφάλειας στον κυβερνοχώρο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R1583

[93] EASA Opinion 03/2021 Management of information security risks, June 2021 https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

[94] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/1645 της 14 Ιουλίου 2022 και ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2023/203 της 27 Οκτ 2022 για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις απαιτήσεις για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj

προσαρμογή του επιπέδου αποδοχής κινδύνου. Διαφορετικού τύπου κίνδυνοι αλληλεπιδρούν μεταξύ τους, κατά τρόπο ώστε η εφαρμογή ενός μέτρου μπορεί να αφορά περισσότερους κινδύνους. Λόγω των αλληλεπιδράσεων, μπορεί να απαιτείται να εφαρμοστούν διαφορετικές διεργασίες αποτίμησης επικινδυνότητας για κάθε τομέα, ώστε να διαμορφωθεί μια κοινή συνισταμένη για τη διαχείριση της επικινδυνότητας.[95]



Σχήμα 11: Διαχείριση επικινδυνότητας στην αεροπορική ασφάλεια λόγω απειλών κατά της ασφάλειας πληροφοριών

Στόχος της Ευρωπαϊκής Ένωσης είναι μέσω της συμμόρφωσης στις νέες απαιτήσεις Part I.S., που θα ολοκληρωθεί στις 22-2-2026, να διαμορφωθεί στον αεροπορικό τομέα ένα σύστημα που σε συνδυασμό με την οδηγία CER, θα εξασφαλίσει την ανθεκτικότητα απέναντι στις κυβερνοεπιθέσεις.

4.1.2. Στρατηγικές και πολιτικές κυβερνοασφάλειας

Το μεταβαλλόμενο τοπίο των κυβερνοαπειλών και η αυξανόμενη εξάρτηση του αεροπορικού τομέα από τα πληροφοριακά συστήματα, απαιτούν τη χάραξη μιας ολοκληρωμένης στρατηγικής για την Κυβερνοασφάλεια. Ο ICAO, ως κύριος φορέας για την προστασία της πολιτικής αεροπορίας, έχει θέσει σαν στόχο να ενισχύσει την ανθεκτικότητα του αεροπορικού τομέα στις απειλές του κυβερνοχώρου και να διασφαλίσει την αξιοπιστία του διεθνώς, σε ένα πλαίσιο συνεχούς ανάπτυξης και καινοτομίας. Η στρατηγική του στηρίζεται σε επτά πυλώνες, που συνιστούν αντίστοιχα υποχρεώσεις για τα τα κράτη που είναι μέλη του:

1. Ανάπτυξη διεθνούς συνεργασίας
2. Διακυβέρνηση κυβερνοασφάλειας
3. Αποτελεσματική νομοθεσία
4. Ανάπτυξη Πολιτικών για τη Κυβερνοασφάλεια
5. Διαμοιρασμός πληροφοριών

[95] EASA Information Security (Part-IS)
https://www.easa.europa.eu/en/the-agency/faqs/information-security-part#category-delegation-of-tasks

6. Διαχείριση περιστατικών και σχεδιασμός έκτακτης ανάγκης
7. Ανάπτυξη ικανοτήτων, εκπαίδευση, καλλιέργεια κουλτούρας κυβερνοασφάλειας

Μεταξύ των πολιτικών που πρέπει να υλοποιηθούν για να επιτευχθούν οι στρατηγικοί στόχοι, είναι η υιοθέτηση ενός περιεκτικού πλαισίου αποτίμησης της επικινδυνότητας. Ενόψει της πληθώρας των πλαισίων και μεθοδολογιών που εφαρμόζονται, ο ICAO υπογραμμίζει τη σημασία της δυνατότητας εξαγωγής συγκρίσιμων αποτελεσμάτων. Οι πολιτικές για την Κυβερνοασφάλεια, θα πρέπει να στραφούν γύρω από τα εξής σημεία:

- Προώθηση της ασφάλειας από το σχεδιασμό : Η ενσωμάτωση μέτρων ασφαλείας κατά το σχεδιασμό και την ανάπτυξη συστημάτων και υποδομών αεροπορίας.
- Ασφάλεια της εφοδιαστικής αλυσίδας για λογισμικό και υλικό: Διασφάλιση ότι το λογισμικό και το υλικό που χρησιμοποιούνται στα αεροπορικά συστήματα προέρχονται από αξιόπιστες πηγές και είναι απαλλαγμένα από ευπάθειες.
- Διασφάλιση της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των πληροφοριών/ δεδομένων που χρησιμοποιούνται στα αεροπορικά συστήματα.
- Κατάλληλος έλεγχος πρόσβασης: Περιορισμός της πρόσβασης στα αεροπορικά συστήματα μόνο σε εξουσιοδοτημένο προσωπικό.
- Προληπτική διαχείριση ευπαθειών: Ενεργός αναζήτηση και αποκατάσταση ευπαθειών στα αεροπορικά συστήματα πριν από την εκμετάλλευσή τους από τους επιτιθέμενους.
- Βελτίωση της ευελιξίας στις ενημερώσεις ασφαλείας: Εφαρμογή ενημερώσεων ασφαλείας έγκαιρα, διασφαλίζοντας παράλληλα ότι δεν επηρεάζεται η λειτουργία των συστημάτων.
- Ενσωμάτωση συστημάτων και διαδικασιών για την παρακολούθηση δεδομένων σχετικών με την κυβερνοασφάλεια: Συλλογή και ανάλυση δεδομένων για την ανίχνευση και την πρόληψη κυβερνοεπιθέσεων.[96]

Ο EASA αντίστοιχα, εκφράζοντας την στρατηγική της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, επισημαίνει την ανάγκη για κοινές στρατηγικές στον ευρωπαϊκό χώρο, που θα εξασφαλίσουν για το μέλλον:

- Ένα αξιόπιστο περιβάλλον, έτσι ώστε οι φορείς του τομέα της αεροπορίας να μπορούν να βασίζονται στις υπηρεσίες και τις πληροφορίες που παρέχονται από άλλους για την επίτευξη των επιχειρησιακών τους στόχων.

[96] ICAO Aviation Cybersecurity Strategy , October 2019
www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf
ICAO Cybersecurity Policy Guidance, Published by authority of the Secretary General January 2022
www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf

- Ένα "σύστημα συστημάτων" προσαρμοστικό και ανθεκτικό σε νέες απειλές, χωρίς διαταράξεις της λειτουργίας του, που αναπτύσσεται μέσω μιας συστημικής προσέγγισης στον τομέα της κυβερνοασφάλειας[97]

Τους ίδιους στρατηγικούς στόχους θέτει και η IATA, που αναπτύσσει πολιτικές για την αντιμετώπιση των προκλήσεων στο χώρο της Κυβερνοασφάλειας, στη βάση της συνεργασίας μεταξύ των μελών της αεροπορικής κοινότητας, με τη δημιουργία εργαστηρίων και forums ανταλλαγής πληροφοριών, ιδιαίτερα στο πεδίο των ευπαθειών των συστημάτων και ανάπτυξης προτύπων. [98]

Η Μ.Βρεττανία, παρά την έξοδό της από την Ε.Ε., στη στρατηγική της για την κυβερνοασφάλεια στον αεροπορικό τομέα, συνεχίζει να ακολουθεί την ευρωπαϊκή πολιτική και τα θεσμικά κείμενά της, όπως την Οδηγία NIS, για την εξασφάλιση της λήψης από τους εμπλεκόμενους στη πολιτική αεροπορία των βασικών μέτρων προστασίας. Η στρατηγική της, όπως εκφράζεται από το Υπουργείο Μεταφορών, περιλαμβάνει τα εξής στοιχεία: [99]

- Κατανόηση κινδύνων που θέτουν οι απειλές και οι ευπάθειες και δυνητικών συνεπειών
- Διαχείριση επικινδυνότητας κυβερνοασφάλειας/ προστασία κρίσιμων αγαθών
- Απόκριση και ανάκαμψη από περιστατικά ασφαλείας/ απόκτηση γνώσης
- Επίγνωση/Οικοδόμηση κουλτούρας κυβερνοασφάλειας και διεθνούς συνεργασίας

4.1.3. Η αποτίμηση επικινδυνότητας κυβερνοασφάλειας στον αεροπορικό τομέα

Η κυβερνοασφάλεια είναι ένας διατομεακός κλάδος που καλύπτει πολιτικές, διαδικασίες, τεχνολογία και άτομα, μέσω μιας ολοκληρωμένης προσέγγισης του κύκλου ζωής των περιστατικών ασφαλείας: προστασία των αγαθών από απειλές, εντοπισμό κινδύνων, ανταπόκριση σε περιστατικά και ανάκαμψη από παραβίαση. Οι πολιτικές για την Κυβερνοασφάλεια πρέπει να καλύπτουν όλο το εύρος του οργανισμού και προϋποθέτουν την δέσμευση της Διοίκησης για την εφαρμογή τους, σε συμφωνία με το ΣΔΑΠ (ISMS) και το Σχέδιο Ασφαλείας (SMS). ΄Οπως προαναφέρθηκε, η Ευρωπαϊκή ΄Ενωση σε εκτέλεση των δύο νέων Κανονισμών της, επεξεργάζεται μέσω του EASA, την προτυποποίηση και καθοδήγηση στον τομέα αυτό, μέσω του πακέτου Part-IS.

Μιά άλλη πρόταση για την αποτίμηση της επικινδυνότητας στο πεδίο της Κυβερνοασφάλειας, που απευθύνεται εξειδικευμένα στους παρόχους υπηρεσιών αεροναυτιλίας (ANSP), είναι το

[97] EASA ESCP (European Strategic Cooperation Platform) European Strategic Coordination Platform Strategy for Cybersecurity in Aviation First Issue – September 10th , 2019
https://www.easa.europa.eu/en/downloads/103075/en
[98] IATA, Aviation Cyber Security Roundtable April 11-12, 2019 Singapore,
www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/sin_roundtable_readout.pdf
[99]UK Department of Transport: Aviation Cyber Security Strategy,2018 Aviation Cyber Security Strategy (publishing.service.gov.uk)

Πρότυπο του Οργανισμού CANSO (Standard Of Excellence in Cybersecurity, 2020). Βασίζεται στο Πλαίσιο NIST CSF για την Κυβερνοασφάλεια, στο οποίο παραπέμπει, χρησιμοποιώντας σαν αφετηρία την διάκριση σε επίπεδα (Tiers) του Πλαισίου. Αξιοποιεί παράλληλα στοιχεία από το Πρότυπο ISO 27001, ώστε να δοθεί έμφαση στη λειτουργία της ηγεσίας και της διακυβέρνησης και γενικότερα στον ανθρώπινο παράγοντα στην ασφάλεια. Στόχος του είναι η καθοδήγηση των παρόχων ώστε να αναπτύξουν μια ολιστική προσέγγιση κυβερνοασφάλειας σε περιβάλλον συστημάτων εναέριας κυκλοφορίας (ATM), επισημαίνοντας τα πιο κρίσιμα στοιχεία και τις ιδιαιτερότητες. Δεν υποκαθιστά παρόλα αυτά τα σχετικά Πρότυπα NIST και ISO, καθώς δεν παρέχει πιστοποίηση, αλλά λειτουργεί συμπληρωματικά προς αυτά.΄Έτσι ακόμα και αν το ΣΔΑΠ του οργανισμού είναι πλήρως συμβατό με τις απαιτήσεις ISO 27001, το πρότυπο προσφέρει πρόσθετη αξία, καθώς έχει σχεδιαστεί ειδικά για να ανταποκρίνεται στις ανάγκες ενός παρόχου υπηρεσιών (ANSP), ενώ το ISO 27001 είναι ανεξάρτητο κλάδου. Επιπλέον, παρέχει μια δομή για τη συνεχή βελτίωση της ωριμότητας της κυβερνοασφάλειας ενός οργανισμού, βασισμένη στην έννοια μιας προσέγγισης μοντέλου ωριμότητας για την κυβερνοασφάλεια.

Σύμφωνα με το μοντέλο ωριμότητας, οι Πάροχοι μπορούν να αξιολογήσουν τη δική τους ωριμότητα στην Κυβερνοασφάλεια, καθώς και των προμηθευτών τους. Η αξιολόγηση των προμηθευτών αφορά στα πληροφοριακά τους συστήματα και το προϊόν τους και δεν αντικαθιστά ελέγχους άλλου τύπου. Το μοντέλο ωριμότητας αποτελείται από δεκατρία στοιχεία που αντιστοιχούν σε έξι λειτουργίες, τις οποίες οφείλει να διαθέτει ο οργανισμός: Ηγεσία και διακυβέρνηση / Αναγνώριση/Προστασία/ Ανίχνευση/Απόκριση/ Ανάκαμψη. Κάθε στοιχείο περιγράφεται λεπτομερώς στο μοντέλο ωριμότητας, με πέντε διαφορετικά επίπεδα ωριμότητας που απαιτούν διαφορετική αντιμετώπιση. Η αξιολόγηση για κάθε στοιχείο πραγματοποιείται χρησιμοποιώντας ένα έντυπο βαθμολογίας που περιέχει ερευνητικά ερωτήματα, το οποίο επιτρέπει σε έναν οργανισμό και την αλυσίδα εφοδιασμού του να προσδιορίσει το τρέχον επίπεδο ωριμότητας του.

Επίπεδο ωριμότητας	*Χαρακτηρισμός*
A	΄Ατυπες διευθετήσεις (Informal Arrangements)
B	Ορισμένο (Defined)
C	Διαχειριζόμενο (Managed)
D	Διασφαλισμένο (Assured)
E	Βελτιστοποιημένο (Optimised)

Οι λειτουργίες και τα επιμέρους στοιχεία τους που ανταποκρίνονται σε ικανότητες που πρέπει να αναπτυχθούν για κάθε μία λειτουργία, προκύπτουν από το εξής παράδειγμα αποτίμησης επικινδυνότητας για τον ίδιο τον οργανισμό αεροναυτιλίας και για τους προμηθευτές του:[100]

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Ident ity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

Σχήμα 12 : Παράδειγμα αποτίμησης επικινδυνότητας παρόχου υπηρεσιών αεροναυτιλίας

4.2. Η απειλή της κυβερνοασφάλειας στους Αερολιμένες

4.2.1. Οι κυβερνοαπειλές και τα χαρακτηριστικά τους στους Αερολιμένες

Σύμφωνα με τον NIST, η απειλή στο κυβερνοχώρο ορίζεται ως οποιαδήποτε περίσταση ή γεγονός που μπορεί να επηρεάσει αρνητικά τις οργανωτικές λειτουργίες, τα περιουσιακά στοιχεία του οργανισμού, τα άτομα, τους άλλους οργανισμούς ή το Έθνος μέσω ενός συστήματος μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης πληροφοριών και/ή άρνησης παροχής υπηρεσιών.

Στην έρευνα που έγινε από τον CANSO (2023) οι πιθανές απειλές που επηρεάζουν ένα τομέα έχουν πραγματοποιήσει τεράστια εξέλιξη τα τελευταία χρόνια. Τα κράτη και οι ομάδες που λειτουργούν με την υποστήριξη των κρατών έχουν μετατραπεί σε προηγμένες διαρκείς απειλές, ενώ ο κίνδυνος από μεμονωμένους χρήστες με περιορισμένες γνώσεις στο προγραμματισμό

[100] CANSO CYBERSECURITY RISK ASSESSMENT GUIDE 2023 Edition https://canso.fra1.digitaloceanspaces.com/uploads/2023/05/CANSO-Safety_Cybersecurity-Risk-Assessment-Guide-2023.pdf

έχουν μειωθεί. Οι δράστες των απειλών αυτών έχουν γίνει όλο και πιο οργανωμένοι, υπομονετικοί και με καλύτερη χρηματοδότηση.

Ταυτόχρονα, ο τομέας της αεροπορίας αποτελεί έναν όλο και πιο συχνό στόχο για τους επιτιθέμενους, έχοντας βιώσει σταδιακή αύξηση επιθέσεων τα τελευταία χρόνια. Οι επιθέσεις εντοπίζονται κυρίως στις εταιρείες αερομεταφορών, όπου διατηρούνται προσωπικά δεδομένα, συμπεριλαμβανομένων των οικονομικών στοιχείων των πελατών. Οι κυβερνοεπιθέσεις στα συστήματα ATM (Air Traffic Management) μέχρι τώρα βρίσκονταν υπό έλεγχο, αλλά οι αερολιμένες ως κρίσιμες υποδομές παραμένουν κορυφαίος στόχος για επιθέσεις και επομένως είναι πιθανό να αυξηθούν τα περιστατικά που επηρεάζουν τα συστήματα ATM.

Τα συστήματα που διαχειρίζονται την εναέρια κυκλοφορία περνούν όλο και περισσότερο στη ψηφιοποίηση, συνδέονται με άλλους οργανισμούς, συνεπώς δημιουργούν και ανταλλάσουν περισσότερα δεδομένα από ποτέ. Παλαιότερα, τα δίκτυα ήταν απομονωμένα, χρησιμοποιώντας αποκλειστικά τηλεφωνικές υποδομές, κάτι που περιόριζε αρκετά τις εξωτερικές επιθέσεις. Με την συνδεσιμότητα του πρωτοκόλλου του Διαδικτύου (IP, Internet Protocol), αυξάνεται το ρίσκο της κυβερνοασφάλειας στο τομέα της Αεροπορίας.

Μια απειλή κυβερνοασφάλειας είναι σκόπιμη, μπορεί να είναι στοχευμένη ή όχι και μπορεί να προέρχεται από διάφορες πηγές. Κάποιες από αυτές, μπορεί να προέρχονται από έθνη που ασχολούνται με την κατασκοπεία και τον πόλεμο πληροφοριών, από εγκληματίες, χάκερ, συγγραφείς ιών, δυσαρεστημένους υπαλλήλους και εργολάβους που εργάζονται σε έναν οργανισμό. Οι απειλές μπορούν να επιδεινωθούν, ακόμη και να πραγματοποιηθούν από απρόσεκτους ή ανεπαρκώς εκπαιδευμένους υπαλλήλους. Απειλές εμφανίζονται ακόμα και από αδυναμίες στις διαδικασίες λειτουργίας/συντήρησης, αναβαθμίσεις λογισμικού και βλάβες στον εξοπλισμό που διαταράσσουν κατά λάθος τα συστήματα υπολογιστών ή αλλοιώνουν τα δεδομένα.

Οι απειλές περιλαμβάνουν τόσο στοχευμένες όσο και μη στοχευμένες επιθέσεις.Μια στοχευμένη επίθεση είναι όταν μια ομάδα ή ένα άτομο επιτίθεται ειδικά σε ένα σύστημα κρίσιμης υποδομής. Μια μη στοχευμένη επίθεση συμβαίνει όταν ο επιδιωκόμενος στόχος της επίθεσης είναι αβέβαιος, όπως όταν ένας ιός ή ένα κακόβουλο λογισμικό κυκλοφορεί στο Διαδίκτυο χωρίς συγκεκριμένο στόχο. Οι απειλές που απευθύνονται ειδικά σε μια μεμονωμένη εταιρεία ή οργανισμό, απειλές ευρύτερης εμβέλειας που αποσκοπούν στο να πλήξουν όσο το δυνατόν περισσότερες εταιρείες ή άτομα και επιθέσεις που στοχεύουν την αλυσίδα εφοδιασμού ή την υποδομή, γεγονός που καθιστά τις εταιρείες (και τα άτομα) ακούσια θύματα.

Η πιο ανησυχητική απειλή για έναν οργανισμό είναι αυτή του "εσωτερικού" του περιβάλλοντος, κάποιου που έχει εξουσιοδοτημένη και νόμιμη πρόσβαση σε ένα σύστημα ή δίκτυο. Άλλοι επιτιθέμενοι (όπως το οργανωμένο έγκλημα ή μια τρομοκρατική ομάδα) μπορούν να

χρησιμοποιήσουν τους εσωτερικούς χρήστες, για παράδειγμα, εξαναγκάζοντας έναν πρόθυμο εσωτερικό χρήστη (όπως έναν δυσαρεστημένο υπάλληλο) ή χρησιμοποιώντας έναν ασυνείδητο εσωτερικό χρήστη (π.χ. επηρεάζοντας κάποιον με εξουσιοδοτημένη πρόσβαση στο δίκτυο να τοποθετήσει ένα δίσκο που περιέχει κρυφό κώδικα). Ωστόσο, οι εσωτερικές απειλές μπορούν να να αποτραπούν με οργανωτικούς (π.χ. πολιτική), λογικούς (π.χ. πιστοποίηση ταυτότητας) και φυσικούς (π.χ. περιορισμένη πρόσβαση με κάρτα προσέγγισης) ελέγχους, καθώς και με την εκπαίδευση του προσωπικού σχετικά με τις βέλτιστες πρακτικές στον κυβερνοχώρο για την αποτροπή προσπαθειών κυβερνοεπιθέσεων (π.χ. αναγνώριση των ηλεκτρονικών μηνυμάτων phishing).

Οι επιθέσεις στον κυβερνοχώρο έχουν διάφορες μορφές, από προηγμένα botnet μέχρι πιο απλές επιθέσεις phishing. Ο πρωταρχικός στόχος είναι να παραβιάσουν τις άμυνες ασφαλείας και να δημιουργήσουν ερείσματα στο δίκτυο-στόχο.Από αυτή τη θέση διοίκησης και ελέγχου, ένας επιτιθέμενος μπορεί να κινηθεί μέσα στο δίκτυο, συλλέγοντας δεδομένα, παραβιάζοντας συστήματα και λογαριασμούς χρηστών.Αυτή η περιήγηση δεν έχει χρονικό όριο και εξαρτάται από τον επιτιθέμενο και τον τελικό του στόχο, αλλά μπορεί να περιλαμβάνει την απομόνωση δεδομένων, την ενεργοποίηση ενός ωφέλιμου φορτίου ή τη συνέχιση της κατασκοπείας.[101]

Ο ENISA (2023) στην έκθεση για τις κυριότερες απειλές στον κυβερνοχώρο υπογραμμίζει οκτώ κύριες ομάδες απειλών:

1. **Ransomware**

Είναι ένας τύπος επίθεσης που οι απειλητικοί φορείς αναλαμβάνουν τον έλεγχο των δεδομένων του στόχου και απαιτούν "λύτρα" σε αντάλλαγμα για την επιστροφή της διαθεσιμότητας των δεδομένων αυτών.

2. **Κακόβουλο λογισμικό**

Στη συγκεκριμένη κατηγορία ανήκει οποιοδήποτε λογισμικό ή υλικολογισμικό που προορίζεται να εκτελέσει μια μη εξουσιοδοτημένη διαδικασία η οποία θα έχει αρνητικό αντίκτυπο στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος. Ο κυριότερος τρόπος που εκτελείται ένα κακόβουλο λογισμικό είναι μέσω της κοινωνικής μηχανικής "Social Engineering", οπού περιλαμβάνει ένα ευρύ φάσμα δραστηριοτήτων που επιχειρούν να εκμεταλλευτούν το ανθρώπινο λάθος με στόχο τη πρόσβαση σε πληροφορίες ή υπηρεσίες. Οι χρήστες μπορεί να δελεαστούν να ανοίξουν έγγραφα, αρχεία ή μηνύματα ηλεκτρονικού ταχυδρομείου, να επισκεφθούν ιστότοπους ή να παραχωρήσουν πρόσβαση σε συστήματα ή υπηρεσίες. Παρόλο που τα τεχνάσματα που χρησιμοποιούνται μπορεί να κάνουν κατάχρηση της τεχνολογίας, βασίζονται σε ένα ανθρώπινο στοιχείο για να είναι επιτυχημένα.

[101] CANSO CYBERSECURITY RISK ASSESSMENT GUIDE 2023 Edition ό.π.

3. Απειλές κατά των δεδομένων

Η παραβίαση δεδομένων ορίζεται στον ΓΚΠΔ ως κάθε παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση ή μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε άλλη επεξεργασία (άρθρο 4.12 ΓΚΠΔ).Από τεχνική άποψη, οι απειλές κατά των δεδομένων μπορούν να ταξινομηθούν ως παραβίαση δεδομένων ή διαρροή δεδομένων και η διαφορά τους έγκειται στον τρόπο με τον οποίο συμβαίνουν.

- Παραβίαση δεδομένων : Εσκεμμένη κυβερνοεπίθεση που πραγματοποιείται από έναν εγκληματία στον κυβερνοχώρο με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης και τη δημοσιοποίηση ευαίσθητων, εμπιστευτικών ή προστατευόμενων δεδομένων.
- Διαρροή δεδομένων : Ένα γεγονός (π.χ. λανθασμένες ρυθμίσεις, ευπάθειες ή ανθρώπινα λάθη) που μπορεί να προκαλέσει την ακούσια απώλεια ή έκθεση ευαίσθητων, εμπιστευτικών ή προστατευόμενων δεδομένων (οι σκόπιμες επιθέσεις αναφέρονται μερικές φορές ως έκθεση δεδομένων).

4. Απειλές κατά της διαθεσιμότητας

- Άρνηση παροχής υπηρεσιών

Η διαθεσιμότητα αποτελεί στόχο πληθώρας απειλών και επιθέσεων, μεταξύ των οποίων ξεχωρίζει η DDoS.Η DDoS στοχεύει στη διαθεσιμότητα συστημάτων και δεδομένων και διαδραματίζει σημαντικό ρόλο στο τοπίο των απειλών για την κυβερνοασφάλεια. Ως αποτέλεσμα της επίθεσης, οι χρήστες ενός συστήματος ή μιας υπηρεσίας δεν είναι σε θέση να έχουν πρόσβαση σε σχετικά δεδομένα, υπηρεσίες ή άλλους πόρους.Αυτό μπορεί να επιτευχθεί με την εξάντληση της υπηρεσίας και των πόρων της ή με την υπερφόρτωση των στοιχείων της υποδομής του δικτύου.

- Απειλές δικτύου

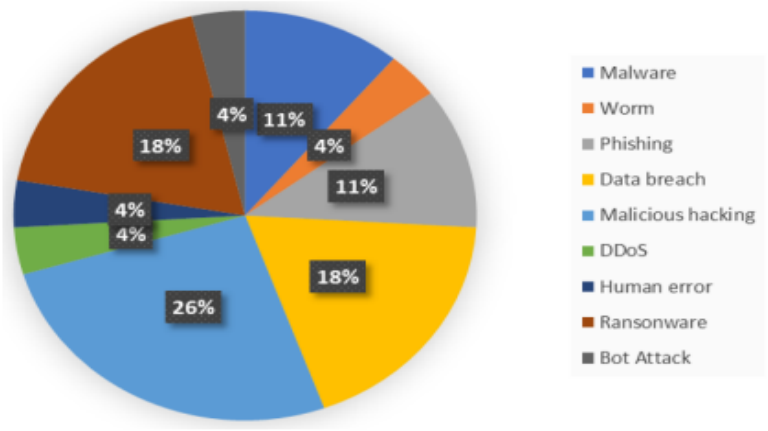
Οι απειλές κατά της διαθεσιμότητας του Διαδικτύου αναφέρονται σε εκούσιες ή ακούσιες διαταραχές του Διαδικτύου ή των ηλεκτρονικών επικοινωνιών που έχουν ως αποτέλεσμα διακοπές λειτουργίας του Διαδικτύου, διακοπές ρεύματος, διακοπή λειτουργίας κλπ.. Οι διαταραχές του Διαδικτύου μπορεί να οφείλονται σε κυβερνητικά κατευθυνόμενες διακοπές του Διαδικτύου, μαζικούς σεισμούς, διακοπές ρεύματος, διακοπές καλωδίων, κυβερνοεπιθέσεις, τεχνικά προβλήματα και στρατιωτικές ενέργειες. Αυτές οι απειλές διαφοροποιούνται και αυξάνονται ραγδαία το τελευταίο καιρό, σύμφωνα με τον ENISA, έχοντας προκαλέσει τεράστιες χρηματικές απώλειες στις εθνικές οικονομίες.

5. Χειραγώγηση πληροφοριών

Η Χειραγώγηση και Παρεμβολή Ξένων Πληροφοριών (FIMI) περιγράφει ένα ως επί το πλείστον μη παράνομο πρότυπο συμπεριφοράς που απειλεί ή έχει τη δυνατότητα να επηρεάσει αρνητικά αξίες, διαδικασίες και πολιτικές διαδικασίες. Η εν λόγω δραστηριότητα έχει χειραγωγικό χαρακτήρα και διεξάγεται με σκόπιμο και συντονισμένο τρόπο.Η FIMI μπορεί να διεξάγεται από κρατικούς ή μη κρατικούς φορείς, συμπεριλαμβανομένων των πληρεξουσίων τους εντός και εκτός της επικράτειάς τους, ενώ στην παρούσα έκθεση μελετάμε την απειλή ανεξάρτητα από την προέλευσή της.

6. Επιθέσεις κατά της εφοδιαστικής αλυσίδας

Μια επίθεση στην αλυσίδα εφοδιασμού στοχεύει στη σχέση μεταξύ των οργανισμών και των προμηθευτών τους. Μια επίθεση κατά της αλυσίδας εφοδιασμού όταν αποτελείται από συνδυασμό τουλάχιστον δύο επιθέσεων.Για να χαρακτηριστεί μια επίθεση ως επίθεση στην αλυσίδα εφοδιασμού, πρέπει τόσο ο προμηθευτής όσο και ο πελάτης να είναι στόχοι. Η επίθεση στη SolarWinds ήταν μία από τις πρώτες αυτού του είδους των επιθέσεων και έδειξε τον πιθανό αντίκτυπο των επιθέσεων στην αλυσίδα εφοδιασμού.Ουσιαστικά η επίθεση έγινε στο λογισμικό της εταιρείας πλήττοντας ένα μεγάλο αριθμό άλλων οργανισμών και εταιρειών που το χρησιμοποιούσαν. Παρατηρήθηκε ότι οι φορείς απειλών συνεχίζουν να τρέφονται από αυτή την πηγή για να διεξάγουν τις δραστηριότητές τους και να αποκτούν πρόσβαση εντός των οργανισμών, με σκοπό να επωφεληθούν από τον εκτεταμένο αντίκτυπο και τη μεγάλη βάση θυμάτων αυτών των επιθέσεων.[102]



Σχήμα 13: Συχνότητα κυβερνοαπειλών αεροδρομίων ανάλογα με τον τύπο τους[103]

[102] ENISA. (2015) Threat Landscape of Internet Infrastructure [Report/Study] https://www.enisa.europa.eu/publications/iitl

[103] Ukwandu, E.,Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends Information 2022, 13, 146, Academic Editor: Sokratis Katsikas https://doi.org/10.3390/info13030146

Η έρευνα του ENISA παρουσιάζει τις κύριες κυβερνοαπειλές και τις τάσεις όσον αφορά τη κυβερνοασφάλεια για τη περίοδο αναφοράς της έκθεσης. Συγκριτικά θα γίνει ανάλυση παρακάτω στις πιο συχνές κυβερνοαπειλές σύμφωνα με την έκθεση αναφοράς του CANSO (2023) που αναφέρεται συγκεκριμένα στις κρίσιμες υποδομές των αερολιμένων. Οι κύριες απειλές, κατανεμημένες με τη συχνότητα εμφάνισης τους στους αερολιμένες σύμφωνα με την έκθεση για τη περίοδο αναφοράς είναι ως εξής:

1. **Κακόβουλο λογισμικό**

Το κακόβουλο λογισμικό εμφανίζεται σε πολλές μορφές, όπως ransomware, worms, trojans, adware και spyware.Στόχος είναι να διεισδύσει, να κατασκοπεύσει ή να δημιουργήσει ένα τρόπο ελέγχου των συστημάτων του αερολιμένα.

2. **Phishing**

Η επίθεση αυτή συνίσταται στο να ξεγελάσει τον στόχο για να εκτελέσει μια ενέργεια.Αυτό μπορεί να είναι το άνοιγμα ενός υπερσυνδέσμου σε έναν ιστότοπο, η λήψη ενός αρχείου ή να του ζητηθεί να συμπληρώσει μια φόρμα.Το phishing μπορεί να είναι μη στοχευμένο (δηλαδή μια τυχαία προσπάθεια εξαπάτησης του οποιουδήποτε), στοχευμένο σε άτομα σε θέσεις εξουσίας (whale phishing/whaling) και στοχευμένο σε συγκεκριμένους οργανισμούς ή/και άτομα χαμηλότερου επιπέδου με ένα ηλεκτρονικό μήνυμα που φαίνεται να προέρχεται από μια γνωστή επαφή του θύματος (spear phishing). Οι στοχευμένες επιθέσεις phishing απαιτούν μια περίοδο αναγνώρισης από τον επιτιθέμενο για την πραγματοποίηση της επίθεσης.

3. **Άρνηση παροχής υπηρεσιών (DoS)**

Οι συγκεκριμένες επιθέσεις επιχειρούν να χρησιμοποιήσουν όλους τους πόρους ενός συστήματος προκαλώντας την αποτυχία του. Αυτό μπορεί να περιλαμβάνει τη συμφόρηση όλου του διαθέσιμου εύρους ζώνης του συστήματος, τη χρήση όλης της μνήμης ή των επεξεργαστών ή απλώς τη συμπλήρωση του αποθηκευτικού χώρου της συσκευής. Η κατανεμημένη άρνηση παροχής υπηρεσιών (DDoS) είναι ένας τύπος επίθεσης DoS που χρησιμοποιεί botnets, έναν αριθμό απομακρυσμένα ελεγχόμενων συστημάτων, για να φέρει το εύρος ζώνης πολλών συστημάτων στο σύστημα-στόχο που συχνά χρησιμοποιείται για να θέσει εκτός λειτουργίας ιστότοπους βομβαρδίζοντάς τους με αιτήματα.

4. **Man in the Middle**

Το επιθυμητό αποτέλεσμα αυτής της επίθεσης είναι η υποκλοπή και ενίοτε η χειραγώγηση δεδομένων μεταξύ συστημάτων. Συχνά χρησιμοποιείται για την κλοπή ή την ανακατεύθυνση πληροφοριών, συμπεριλαμβανομένης της κατεύθυνσης των θυμάτων σε ψεύτικες ιστοσελίδες και στη συνέχεια τη συλλογή των πληροφοριών τους. Οι επιθέσεις Man in the Middle είναι πιο

δύσκολο να εκτελεστούν και επομένως χρησιμοποιούνται λιγότερο συχνά από τους επιτιθέμενους.

5. **Brute Force (ωμή βία)**

Η συγκεκριμένη επίθεση περιλαμβάνει πολυάριθμες προσπάθειες για την τελική παραβίαση ενός συστήματος. Οι λίστες κωδικών πρόσβασης χρησιμοποιούνται συχνά για την εκτέλεση επιθέσεων σε λογαριασμούς με αποτέλεσμα την απόκτηση πρόσβασης σε πληροφορίες.Τέτοιες λίστες είναι εύκολα διαθέσιμες στο διαδίκτυο και χρησιμοποιούνται από τους επιτιθέμενους για την εκτέλεση μιας επίθεσης brute force σε στοχευμένα συστήματα.

6. **Structured Query Language (SQL) Injection**

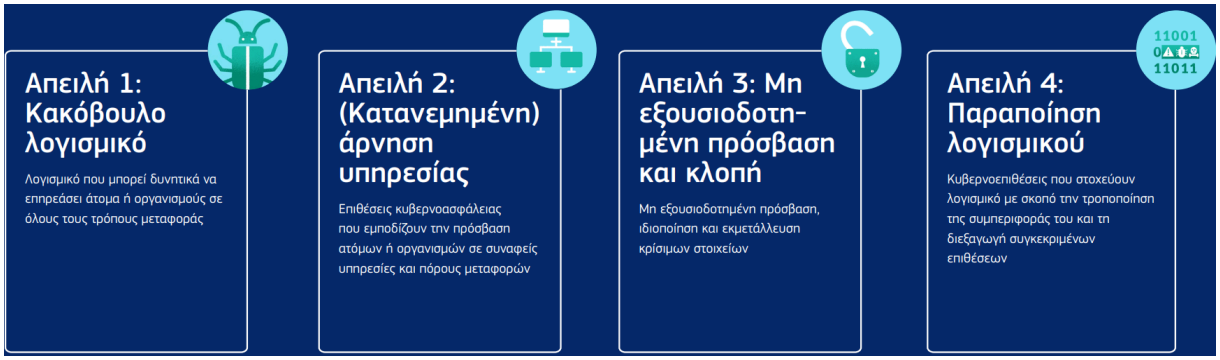
Η συγκεκριμένη επίθεση περιλαμβάνει την εισαγωγή ενός κακόβουλα μεταποιημένου ερωτήματος SQL μέσω των δεδομένων εισόδου. Μια επιτυχημένη επίθεση μπορεί να επιτρέψει την ανάγνωση ή την τροποποίηση των δεδομένων της βάσης δεδομένων ή να επιτρέψει σε έναν κακόβουλο παράγοντα να διαχειριστεί την υπηρεσία της βάσης δεδομένων. Αυτός ο τύπος επίθεσης χρησιμοποιείται συνήθως για την απόκτηση πρόσβασης σε δεδομένα.

7. **Cross-site Scripting (XSS)**

Το XSS χρησιμοποιεί διαδικτυακούς πόρους τρίτων για την εκτέλεση σεναρίων στο σύστημα του θύματος. Ο επιτιθέμενος μεταπιεί κακόβουλα έναν ευάλωτο διακομιστή ιστού και στη συνέχεια συλλέγει δεδομένα χρηστών ή κλέβει τη συνεδρία τους για να καταλάβει το λογαριασμό τους. Οι μέθοδοι επίθεσης αλλάζουν και εξελίσσονται διαρκώς με πιο σύνθετες και ποικίλες επιθέσεις να λαμβάνουν χώρα. Τα εθνικά κράτη και οι ομάδες που υποστηρίζονται από το κράτος γίνονται όλο και πιο σχολαστικοί στο σχεδιασμό και την υλοποίησή τους, πράγμα που σημαίνει ότι οι κρίσιμες υποδομές των αερολιμένων πρέπει να γίνουν πιο ανθεκτικές στην άμυνά τους.[104]

Σύμφωνα με την εργαλειοθήκη κυβερνοασφάλειας στον τομέα των μεταφορών, που κατάρτισε η Διεύθυνση MOVE της Ευρωπαϊκής Επιτροπής για τη παροχή καθοδήγησης, οι πιο πιεστικές αναδυόμενες κυβερνοαπειλές που επηρεάζουν τις μεταφορές είναι οι εξής:[105]

[104] CANSO CYBERSECURITY RISK ASSESSMENT GUIDE 2023 Edition ό.π.
[105] Ευρωπαϊκή Επιτροπή: Εργαλειοθήκη κυβερνοασφάλειας στον τομέα των μεταφορών 2021 https://transport.ec.europa.eu/document/download/7e65c691-9215-480c-9324-60727ec05d25_el?filename=cybersecurity-toolkit_el.pdf



Σχήμα 14: Συχνότερες κυβερνοαπειλές στον τομέα των μεταφορών

4.2.2. Σενάρια κυβερνοεπιθέσεων και αντιμετώπιση

Καθώς η τεχνολογία εξελίσσεται, οι επιθέσεις στον κυβερνοχώρο γίνονται πιο εξειδικευμένες και επικίνδυνες, ενώ ταυτόχρονα γίνεται η χρήση ολοένα και πιο προηγμένων τεχνικών στις επιθέσεις που απειλούν τη κυβερνοασφάλεια των οργανισμών. Για την αντιμετώπιση των απειλών οι οργανισμοί πρέπει να επενδύουν σε προηγμένα μέτρα ασφαλείας και να αναπτύσσουν εκτεταμένα σχέδια δράσης. Συνολικά, η διαχείριση των σεναρίων κυβερνοεπιθέσεων απαιτεί τη συνεργασία και τη δέσμευση όλων των επιπέδων ενός οργανισμού, από την κορυφή μέχρι τη βάση, προκειμένου να προστατευτούν οι πληροφορίες, οι υποδομές και οι λειτουργίες τους από κυβερνοεπιθέσεις.[106]

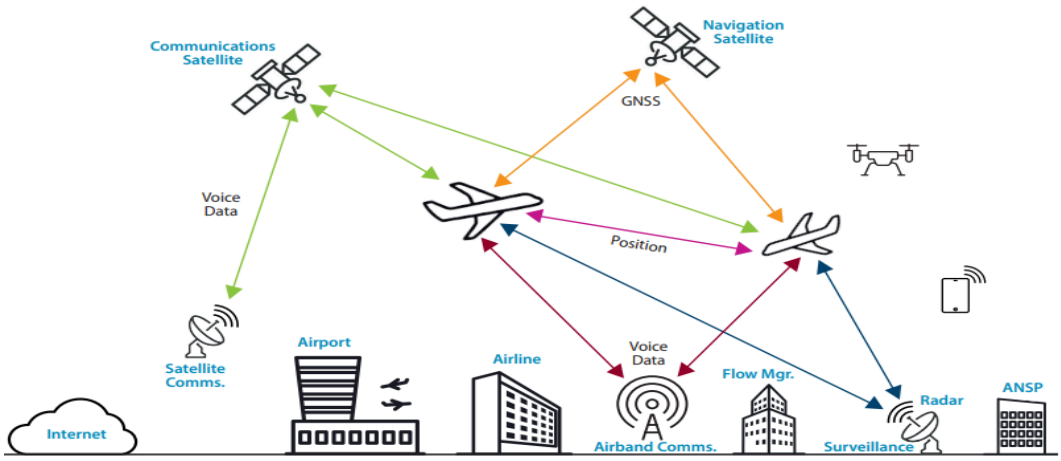
4.2.2.1 Κυβερνοεπιθέσεις στα συστήματα Ελέγχου και Διαχείρησης πτήσεων

Τα συστήματα ATM περιλαμβάνουν μια ποικιλία από φυσικά, οργανωτικά, πληροφοριακά και ανθρώπινα περιουσιακά στοιχεία, που αλληλεπιδρούν σε ένα πολύπλοκο σύστημα για την παροχή μιας ολοκληρωμένης ταξιδιωτικής εμπειρίας για τους επιβάτες. Οι ενδιαφερόμενοι φορείς περιλαμβάνουν τους παρόχους υπηρεσιών αεροναυτιλίας (ANSPs) και το διαχειριστή δικτύου EUROCONTROL (NM), που συνεργάζονται για την παροχή ροής και τη σωστή κατανομή χωρητικότητας στο τομέα της διαχείρισης εναέριας κυκλοφορίας (ATFCM).Οι στόχοι της ATM είναι η ασφαλής επιτάχυνση των πτήσεων, εξισορροπώντας τη χωρητικότητα και τη ζήτηση παρέχοντας αποτελεσματική διαχείριση της ροής για την ελαχιστοποίηση των καθυστερήσεων. Κρίσιμο κομμάτι του ATM είναι και ο περιορισμός των περιβαλλοντικών επιπτώσεων των συστημάτων ενώ παράλληλα αποδίδουν και οικονομικό κέρδος.

Ωστόσο, το σημερινό σύστημα που χρησιμοποιείται για την επίτευξη αυτού του στόχου είναι ένα συνονθύλευμα εξελισσόμενων, διασυνδεδεμένων συστημάτων, το οποίο περιλαμβάνει εξειδικευμένα παλαιά συστήματα αλλά και πιο πρόσφατα εμπορικά συστήματα (COTS), τα

[106] Top Cyber-Threats Faced by the Aviation Industry.(2022): https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

οποία συνδέονται χρησιμοποιώντας ένα συνδυασμό προτύπων. Αυτά περιλαμβάνουν επίγεια και διαστημικά συστήματα επικοινωνίας, πλοήγησης και επιτήρησης (CNS), αεροπορικά κέντρα ελέγχου της κυκλοφορίας (ATC), αεροδρόμια, πύργους ελέγχου, όπως επίσης και τις πληροφορίες που ανταλλάσσονται μεταξύ των συστημάτων ATM όταν τα αεροσκάφη αλληλεπιδρούν μέσω του ελεγχόμενου εναέριου χώρου. Αυτή η ποικιλομορφία των συστημάτων έχει σημαντικές επιπτώσεις στην ασφάλεια στον κυβερνοχώρο. [107]



Σχήμα 15: Το σύνθετο "Σύστημα Συστημάτων" της πολιτικής αεροπορίας

Οι κυβερνοεπιθέσεις στα συστήματα αυτά αποτελούν μία σοβαρή απειλή για την ασφάλεια και τη λειτουργία της αεροπορικής βιομηχανίας. Μπορούν να προκαλέσουν σοβαρές επιπτώσεις, συμπεριλαμβανομένης της διακίνησης ευαίσθητων δεδομένων πτήσης, της ανακατεύθυνσης πτήσεων, αλλά και της απώλειας ελέγχου επί των αεροσκαφών. Επιπλέον, οι επιθέσεις σε αυτά τα συστήματα μπορούν να δημιουργήσουν ανησυχίες για την ασφάλεια του επιβατικού κοινού και να προκαλέσουν σοβαρές οικονομικές απώλειες για τις αεροπορικές εταιρείες και τους αερολιμένες. Ορισμένες κυβερνοεπιθέσεις στα συστήματα ελέγχου και διαχείρισης πτήσεων περιλαμβάνουν:

1. Διακοπή ή παρεμπόδιση της λειτουργίας του συστήματος ελέγχου της εναέριας κυκλοφορίας (ATC): Μια επίθεση που εμποδίζει την επικοινωνία μεταξύ των ελεγκτών εναέριας κυκλοφορίας και των πιλότων θα μπορούσε να οδηγήσει σε σύγχυση και επικίνδυνες καταστάσεις στον εναέριο χώρο.

2. Ανεπιθύμητη παρέμβαση στο σύστημα αυτόματου πιλοτικού ελέγχου (Autopilot): Μια επίθεση που επιδιώκει να παραβιάσει το σύστημα autopilot ενός αεροσκάφους θα μπορούσε να οδηγήσει σε ανεπιθύμητες κινήσεις ή ακόμα και σε απώλεια ελέγχου.

[107] Eurocontrol "Air Traffic Management A Cybersecurity Challenge" 20 Dec2021
https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

3. Αλλοίωση των δεδομένων πτήσης: Μια επίθεση που αλλοιώνει τα δεδομένα πτήσης, όπως το ύψος, την ταχύτητα ή την πορεία ενός αεροσκάφους, θα μπορούσε να προκαλέσει σύγχυση στους ελεγκτές της εναέριας κυκλοφορίας και να οδηγήσει σε επικίνδυνες καταστάσεις.

4. Κλοπή ευαίσθητων πληροφοριών πτήσης: Μια επίθεση που κλέβει πληροφορίες πτήσης, όπως σχέδια πτήσης ή πληροφορίες επιβατών, θα μπορούσε να έχει σοβαρές επιπτώσεις στην ασφάλεια και την ιδιωτικότητα.[108]

Χαρακτηριστικά παραδείγματα κυβερνοεπιθέσεων που έχουν παρέμβει στα συστήματα ελέγχου της εναέριας κυκλοφορίας (ATM) είναι το 1997, η παραβίαση του συστήματος ελέγχου της Bell Atlantic που χρησιμοποιείται για τις επικοινωνίες εναέριας κυκλοφορίας στο αεροδρόμιο Worcester στη Μασαχουσέτη (ΗΠΑ). Η παραβίαση του συστήματος προκάλεσε τη κατάρρευση του που αχρήστευσε το τηλεφωνικό σύστημα του αεροδρομίου για έξι ώρες, διακόπτοντας τις τηλεφωνικές υπηρεσίες προς τον πύργο ελέγχου, την ασφάλεια του αεροδρομίου, την πυροσβεστική υπηρεσία του αεροδρομίου, την μετεωρολογική υπηρεσία και τους χειριστές αεροσκαφών. Η επίθεση έθεσε επίσης εκτός λειτουργίας τον κύριο ραδιοπομπό του πύργου ελέγχου, έναν πομπό για τον έλεγχο των φώτων του διαδρόμου και έναν εκτυπωτή που χρησιμοποιούν οι ελεγκτές για την παρακολούθηση της προόδου των πτήσεων. Ακόμα, οι τηλεφωνικές υπηρεσίες σε 600 σπίτια στην περιοχή διακόπηκαν.

Ένα από τα πρώτα ευρέως τεκμηριωμένα περιστατικά στον τομέα του ATC σημειώθηκε σε σύστημα της Ομοσπονδιακής Διοίκησης της Αεροπορίας των ΗΠΑ (Federal Aviation Administration, FAA) στην Αλάσκα το 2006. Το σύστημα έπρεπε να τεθεί εκτός λειτουργίας όταν η ακεραιότητά του τέθηκε σε κίνδυνο από μια ιογενή επίθεση που εξαπλώθηκε από τα διοικητικά δίκτυα, γεγονός που υπογραμμίζει τη σημασία της απομόνωσης των λειτουργικών συστημάτων.

Στη κατηγορία της παρέμβασης του αυτόματου πιλότου και της αλλοίωσης των δεδομένων πτήσης εμπίπτει η περίπτωση του αεροσκάφους A320 της Lufthansa όπου το 2015 έχασε απροσδόκητα ύψος αφού τα αυτοματοποιημένα συστήματα του παρερμήνευσαν σημαντικά δεδομένα. Σύμφωνα με το γερμανικό Ομοσπονδιακό Γραφείο Διερεύνησης Αεροπορικών Ατυχημάτων στην περίπτωση αυτή, το αεροπλάνο πετούσε με αυτόματο πιλότο όταν ο πιλότος παρατήρησε ότι μία από τις ενδείξεις αυξανόταν ασυνήθιστα γρήγορα. Η οθόνη ανέφερε τις πληροφορίες για τη γωνία προσβολής του αεροπλάνου, οι οποίες αφορούν την ευθυγράμμιση της γραμμής των πτερύγων και την πορεία της πτήσης. Ωστόσο, οι αισθητήρες έδιναν λανθασμένα δεδομένα. Τα λανθασμένα αυτά δεδομένα προκάλεσαν την ενεργοποίηση του συστήματος "Alpha Protection" του αεροσκάφους, το οποίο συνήθως αποτρέπει την ακινητοποίηση και τις επιπτώσεις της ανεμοθραύσης. Όταν αυτό συνδυάστηκε με άλλες τεχνικές

[108] De Zan, Tommaso & Camillo, Federica & d'Amore, Fabrizio. (2015). The Defence of Civilian Air Traffic Systems from Cyber Threats https://www.researchgate.net/publication/324759427_The_Defence_of_Civilian_Air_Traffic_Systems_from_Cyber_Threats

πληροφορίες, το αεροπλάνο ανταποκρίθηκε διατάσσοντας αυτόματα μια κλίση με τη μύτη προς τα κάτω. Η Airbus, έπειτα εξέδωσε ένα επιχειρησιακό τεχνικό δελτίο, το οποίο είναι μια προσωρινή ειδοποίηση ταχείας αντίδρασης που αποστέλλεται από τον κατασκευαστή στους χρήστες ενός αεροσκάφους. Η έκθεση σημείωνε ότι ο πιλότος προσπάθησε να μεταδώσει μια κλήση mayday προς τον έλεγχο εναέριας κυκλοφορίας, αλλά δεν ελήφθη επειδή ο ασύρματος είχε επίσης χάσει την ισχύ του. Στην περίπτωση αυτή, οι πιλότοι κατάφεραν να πραγματοποιήσουν επανεκκίνηση των συστημάτων και το αεροπλάνο συνέχισε το ταξίδι του. Σχετικά με τη παρέμβαση στο σύστημα του αυτόματου πιλότου δεν υπήρξε κάποια εξήγηση ως προς το τί πραγματικά επηρέασε και αλλοίωσε τις ενδείξεις του συστήματος του αεροσκάφους.[109]

Όσον αφορά την επίθεση κλοπής ευαίσθητων πληροφοριών πτήσης, σημαντική είναι η αναφορά σε κάποιους οργανισμούς που καθιστούν προσιτή και εύκολα προσβάσιμη τη διαδικασία εντοπισμού ενός αεροσκάφους. Με την έλευση των προσιτών ραδιοσυχνοτήτων καθορισμένου λογισμικού (SDR), έχει γίνει διαθέσιμη στο κοινό η λήψη μηνυμάτων ADS-B για τον εντοπισμό θέσης πολλών αεροσκαφών. Ένας προσωπικός δέκτης SDR μπορεί να παρέχει εμβέλεια ακτίνας έως και 600 χιλιομέτρων, ενώ εμπορικοί και μη κερδοσκοπικοί οργανισμοί, όπως οι Flightradar24, PlaneFinder, FlightAware, ADSBexchange, Radarbox25 και OpenSky, συγκεντρώνουν τα δεδομένα και τα καθιστούν διαθέσιμα στο διαδίκτυο, προσθέτοντας μια παγκόσμια διάσταση στον εντοπισμό των αεροσκαφών. Ωστόσο, μπορεί να αποκλείει αεροσκάφη που θεωρούνται ευαίσθητα, όπως αυτά που ανήκουν σε κυβερνήσεις ή εταιρείες. Παρόλα αυτά, τα μη φιλτραρισμένα δεδομένα ADS-B, τα οποία λαμβάνονται εύκολα από διάφορες πηγές, μπορούν να επηρεάσουν την ιδιωτική ζωή των χρηστών της αεροπλοΐας όταν χρησιμοποιούνται σε συνδυασμό με δημόσια διαθέσιμα μεταδεδομένα αεροσκαφών. Υπάρχουν αρκετά τεκμηριωμένα παραδείγματα που αποδεικνύουν την ευκολία με την οποία με την οποία οι πληροφορίες αυτές μπορούν να προσπελαστούν και να αναλυθούν για την αποκάλυψη εμπιστευτικών πληροφοριών. Ένα χαρακτηριστικό παράδειγμα αποτελούν οι δημοσιογράφοι-ερευνητές που χρησιμοποίησαν τα δεδομένα αυτά για να αποκαλύψουν τις πτήσεις της CIA που πραγματοποιήθηκαν κατά τη διάρκεια του "πολέμου κατά της τρομοκρατίας". Ομοίως, τα δεδομένα αυτά έχουν χρησιμοποιηθεί για την αποκάλυψη συναντήσεων μεταξύ στελεχών επιχειρήσεων, παρέχοντας ενδείξεις για μελλοντικές συγχωνεύσεις και εξαγορές και για την εξαγωγή συμπερασμάτων από συναντήσεις μεταξύ κυβερνήσεων. Συνεπώς, η εκμετάλλευση τέτοιων δεδομένων μπορεί δυνητικά να χρησιμοποιηθεί για την εξαγωγή συμπερασμάτων για εμπιστευτικές πληροφορίες σε διάφορους τομείς, όπως η εθνική ασφάλεια, η διπλωματία και η ανταγωνιστικότητα των επιχειρήσεων. Προστασία της ιδιωτικής ζωής των μη εμπορικών χρηστών της αεροπορίας στο μέλλον μπορεί να απαιτήσει περαιτέρω ρυθμιστικές και τεχνικές εξελίξεις.[110]

[109] The Guardian, 2015:
https://www.theguardian.com/world/2015/mar/25/germanwings-plane-crash-attention-airbus-safety
[110] Eurocontrol “Air Traffic Management A Cybersecurity Challenge” 20 Dec2021
https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

4.2.2.2 Κυβερνοεπιθέσεις με στόχο τη διαρροή προσωπικών δεδομένων επιβατών

Οι κυβερνοεπιθέσεις που στοχεύουν στη διαρροή προσωπικών δεδομένων επιβατών αντιπροσωπεύουν μια σοβαρή απειλή για την αεροπορική βιομηχανία και την ιδιωτικότητα των επιβατών. Μπορούν να οδηγήσουν στη διαρροή ευαίσθητων πληροφοριών, όπως προσωπικά δεδομένα, δεδομένα ταξιδίου και πληροφορίες πιστωτικών καρτών, με αποτέλεσμα σοβαρές επιπτώσεις στην ασφάλεια και την ιδιωτικότητα των επιβατών. Αυτές οι επιθέσεις μπορούν να προκαλέσουν ανησυχία σε επιβάτες, αεροπορικές εταιρείες και αρχές ελέγχου, και να υπονομεύσουν την εμπιστοσύνη στα συστήματα που διαχειρίζονται τα προσωπικά δεδομένα των επιβατών. Συνολικά, απαιτούνται αποτελεσματικά μέτρα ασφαλείας και προστασίας δεδομένων για την αντιμετώπισή τους και την εξασφάλιση της ιδιωτικότητας των επιβατών.

Το 2018, ένα τρίτο μέρος που διενεργούσε υποχρεωτικό έλεγχο του ιστορικού των εργαζομένων στα αεροδρόμια για την αυστραλιανή κυβέρνηση υπέστη πειρατεία , με αποτέλεσμα την έκθεση των προσωπικών στοιχείων εκατοντάδων εργαζομένων στις αερομεταφορές, προκαλώντας ανησυχία όσον αφορά την παραβίαση της ιδιωτικής ζωής των εργαζομένων, την πιθανή κακόβουλη χρήση των πληροφοριών από εγκληματίες και την ευπάθεια του συστήματος αερομεταφορών. Μια ακόμα πολύ γνωστή περίπτωση κυβερνοεπίθεσης με στόχο τη διαρροή προσωπικών δεδομένων συνέβει το 2020. Η British Airways (BA) τιμωρήθηκε με πρόστιμο ύψους 20 εκατ. λιρών επειδή δεν κατάφερε να προστατεύσει τα προσωπικά και οικονομικά στοιχεία περισσότερων από 400.000 πελατών της, στα οποία είχε πρόσβαση μέσω κυβερνοεπίθεσης που προέκυψε από την αποτυχία της να διασφαλίσει επαρκώς τα επιχειρησιακά της συστήματα. Το πρόστιμο επιβλήθηκε ως αποτέλεσμα της παραβίασε τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) , έναν νόμο της Ευρωπαϊκής Ένωσης που απαιτεί από τους οργανισμούς να διασφαλίζουν τα προσωπικά δεδομένα και να προασπίζουν τα δικαιώματα ιδιωτικότητας οποιουδήποτε βρίσκεται στην επικράτεια της ΕΕ. Ακόμα, το 2018 θύμα κυβερνοεπίθεσης που ως αποτέλεσμα είχε τη διαρροή προσωπικών δεδομένων ήταν η Cathay Pacific. Η αεροπορική εταιρία του Χονγκ Κονγκ ήταν ο στόχος μιας επίθεσης που παραβίασε τα προσωπικά δεδομένα των πελατών της. Πιο συγκεκριμένα, προκάλεσε τη διαρροή περισσότερων από 9 εκατομμυρίων προσωπικών δεδομένων.[111] Επιπλέον, το 2020 η αεροπορική εταιρεία EasyJet δέχθηκε κυβερνοεπίθεση και παρόλο που απέφυγε τη μη εξουσιοδοτημένη πρόσβαση, στο πλαίσιο της έρευνας που διεξήγαγε για την επίθεση, διαπιστώθηκε ότι κλάπηκαν διευθύνσεις ηλεκτρονικού ταχυδρομείου και στοιχεία ταξιδιών περίπου 9 εκατομμυρίων πελατών, αλλά και στοιχεία πιστωτικών καρτών περισσότερων από 2.000 πελατών.[112]

Οι πληροφορίες από την Ευρωπαϊκή Ομάδα Αντιμετώπισης Εκτάκτων Αναγκών σε Θέματα Υπολογιστών ATM της EUROCONTROL (EATM-CERT) παρέχουν μια εικόνα για ένα ευρύ

[111] Cathay Pacific Airways (2018)
https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data
[112] BBC(2020): https://www.bbc.com/news/technology-52722626

φάσμα περιστατικών ασφάλειας που αναφέρθηκαν από τους ενδιαφερόμενους φορείς της αεροπορίας το 2019, εκ των οποίων το 20% είχε ως στόχο τους παρόχους υπηρεσιών αεροπορικών μεταφορών. Όσον αφορά τη σοβαρότητα του συμβάντος, το 80% ταξινομήθηκε ως χαμηλό, το 20% ως μέτριο και, ευτυχώς, κανένα δεν ήταν υψηλό. Οι συνέπειες των επιθέσεων ήταν κυρίως η διαρροή ευαίσθητων εγγράφων (47%) και η κλοπή δεδομένων (35%), συμπεριλαμβανομένων των σχημάτων δικτύου και των διαπιστευτηρίων χρηστών για ευαίσθητα συστήματα. Οι δράστες των απειλών ήταν γενικά εγκληματίες του κυβερνοχώρου και ομάδες που υποστηρίζονται από κράτη, με κύρια κίνητρα τη στόχευση χρήστες του εναέριου χώρου για οικονομικό κέρδος και/ή απόκτηση πνευματικής ιδιοκτησίας των κατασκευαστών εξοπλισμού. Η έκθεση υπογραμμίζει τη σημασία μιας ολιστικής προσέγγισης της ασφάλειας, υποδεικνύοντας ότι η υπερβολική εστίαση στους τεχνικούς ελέγχους σε βάρος των ανθρώπων και των διαδικασιών μπορεί να εκθέσει τρωτά σημεία που μπορούν να αξιοποιηθούν. Η έκθεση υπογραμμίζει επίσης τη σημασία της ασφαλούς ανταλλαγής ανώνυμων πληροφοριών σχετικά με περιστατικά ασφαλείας, καθώς αυτό επιτρέπει σε άλλους να βελτιώσουν τη στάση ασφαλείας τους. Οι επιτιθέμενοι προσαρμόζονται στις μεταβαλλόμενες συνθήκες. Το έτος 2020 είδαν εγκληματικές ομάδες να αναπτύσσουν δολώματα με θέμα το COVID-19 για σκοπούς phishing. Υπάρχουν επίσης ενδείξεις ότι η εξ αποστάσεως εργασία, η οποία αυξήθηκε μαζικά για πολλούς υπαλλήλους κατά τη διάρκεια της πανδημίας, αυξάνει σημαντικά τον κίνδυνο επιτυχούς επίθεσης, λόγω των ασθενέστερων ελέγχων που υπάρχουν στα οικιακά δίκτυα και συστήματα ΤΠ.[113]

4.3. Προκλήσεις και τάσεις στο τομέα της Κυβερνοασφάλειας των Αεροδρομίων

4.3.1. Η ανάπτυξη της τεχνολογίας στον αεροπορικό τομέα

Η ανάπτυξη της τεχνολογίας στον αεροπορικό τομέα έχει φέρει σημαντικές και καινοτόμες αλλαγές τα τελευταία χρόνια παγκοσμίως στο τομέα των μεταφορών, επηρεάζοντας τόσο τη λειτουργία των αεροπορικών επιχειρήσεων όσο και την εμπειρία των επιβατών. Ο ENISA το 2016 εισήγαγε τον όρο “Smart Airports”, αποσκοπώντας στην καθιέρωση μιας ολιστικής τεχνολογικής εικόνας για τη λειτουργία των κρίσιμων υποδομών των αερολιμένων.

Οι έξυπνοι αερολιμένες εξασφαλίζουν μια καλύτερη ταξιδιωτική εμπειρία και στοχεύουν στα υψηλότερα επίπεδα ασφάλειας των επιβατών και των φορέων εκμετάλλευσης τους. Η βάση του ορισμού των έξυπνων αερολιμένων είναι η δικτύωση και συνεργασία όλων των τεχνολογικων συστημάτων πληροφοριών έτσι ώστε να επιτευχθεί η βέλτιστη χρήση των δεδομένων των πτήσεων, των επιβατών και των παροχών του αερολιμένα συνδυαστικά. Τα αεροδρόμια αυτά εφαρμόζουν νέα “έξυπνα” στοιχεία για να προσφέρουν στους επιβάτες ένα συνδυασμό υπηρεσιών που εκτείνεται από το αυτόματο check-in, τον έλεγχο αποσκευών και εγγράφων, τη

[113] Eurocontrol “Air Traffic Management A Cybersecurity Challenge” 20 Dec2021 https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

διαχείριση κρατήσεων πτήσεων και τις υπηρεσίες εύρεσης τρόπου πρόσβασης έως τον αυτοματοποιημένο συνοριακό έλεγχο και τον έλεγχο ασφαλείας. Ως έξυπνο στοιχείο μπορεί να οριστεί κάθε τεχνολογικό σύστημα που έχει δυνατότητα επεξεργασίας δεδομένων, από τη συγκέντρωση απλών δεδομένων έως την εξαγωγή συμπερασμάτων για την υποστήριξη ανθρώπινων αποφάσεων ή/και την ενεργοποίηση μιας αυτοματοποιημένης απόκρισης. Τα στοιχεία αυτά, ενώ βελτιώνουν την εμπειρία του χρήστη, ανοίγουν επίσης το δρόμο για νέους φορείς επίθεσης και εκθέτουν σε μεγαλύτερο βαθμό τα περιουσιακά στοιχεία του αεροδρομίου. Ως εκ τούτου, οι αερολιμένες πρέπει να αναγνωρίσουν τις απειλές που αναδύονται από τα έξυπνα στοιχεία που ενσωματώνουν, να αυξήσουν την ευαισθητοποίησή τους σχετικά με τις απειλές της ασφάλειας και να βελτιώσουν την ασφάλεια των υποδομών τους, προκειμένου να ενισχύσουν την ασφάλεια των επιβατών και όλων των ενδιαφερομένων μερών του αεροδρομίου.[114]

Η τεχνολογική ανάπτυξη του αεροπορικού τομέα τα τελευταία χρόνια περιλαμβάνει αλλαγές που αφορούν τη ψηφιοποίηση διαδικασιών της υποδομής του αερολιμένα για τη βελτίωση της εξυπηρέτησης των επιβατών όπως τη διαδικασία κρατήσεων εισιτηρίων, τον έλεγχο επιβίβασης και την αναζήτηση πληροφοριών για τις πτήσεις. Ακόμα, η ανάπτυξη των IoT συσκευών συνίσταται στη χρήση αισθητήρων και συσκευών συνδεδεμένων στο διαδίκτυο για τη καλύτερη ανίχνευση, συλλογή, αναγνώριση και παρουσίαση πληροφοριών και δεδομένων στους επιβάτες και τους άμεσα ενδιαφερόμενους φορείς της υποδομής του αερολιμένα. Η τεχνολογία IoT παράδειγμα επιτρέπει στις αεροπορικές εταιρείες να συλλέγουν δεδομένα για την αποτελεσματικότητα της συντήρησης των αεροσκαφών και την παρακολούθηση της ασφάλειας των πτήσεων.[115]

Με την εξέλιξη της τεχνολογίας ενθαρρύνεται και ο αυτοματισμός λειτουργιών και διαδικασιών στους αερολιμένες. Έτσι οι επιχειρησιακές και λειτουργικές ανάγκες ενός αεροδρομίου σταδιακά θα βελτιώνονται προκειμένου να επιτευχθεί η βέλτιστη και γρήγορη εξυπηρέτηση των επιβατών. Ο αυτοματισμός των υποδομών των αερολιμένων δίνει χώρο στην ανάπτυξη της Τεχνητής νοημοσύνης, η οποία μπορεί να χρησιμοποιηθεί για την ανάλυση δεδομένων και την πρόβλεψη προβλημάτων στη λειτουργία των αεροδρομίων και των αεροσκαφών αλλά και στην αναγνώριση μοτίβων των συμπεριφορών και των αναγκων των επιβατών.

Μια επιπλέον προέκταση της τεχνολογικής εξέλιξης για τους αερολιμένες είναι τα Αυτόνομα αεροσκάφη και η ανάπτυξη των μη επανδρωμένων αεροσκαφών (drones). Η έρευνα στον τομέα των αυτόνομων αεροσκαφών έχει ως κύριο στόχο τη μείωση της εκπομπής αερίων του θερμοκηπίου και των καυσίμων και την ανάπτυξη πιο βιώσιμων τεχνολογιών. Τα μη επανδρωμένα αεροσκάφη χρησιμοποιούνται για εργασίες επιθεώρησης, παρακολούθησης και

[114] ENISA. (2016). Securing Smart Airports [Report/Study] ό.π.
[115] Dragos Popa, Andrei Popa, MIrela-Maria Codescu. (2016). Smart Airport-Structure and Elements: https://www.agir.ro/buletine/2812.pdf

παράδοσης εμπορευμάτων, βελτιώνοντας την αποδοτικότητα και μειώνοντας το κόστος λειτουργίας.[116]

Είναι σαφές ότι η ψηφιακή τεχνολογία έχει να διαδραματίσει σημαντικό ρόλο στα αεροδρόμια του μέλλοντος, καθώς οι αλλαγές που φέρνει είναι αναπόφευκτες και θα πρέπει να είναι ευπρόσδεκτες στην αεροδρομιακή κοινότητα. Η κινητικότητα στα αεροδρόμια συνεχίζει να αυξάνεται εκθετικά, με τις ανάγκες και τις προσδοκίες των επιβατών και των αεροπορικών εταιρειών να αυξάνονται ακόμη περισσότερο σε όρους ποιότητας και ποσότητας. Τα αεροδρόμια δεν μπορούν πλέον να ικανοποιούν αυτές τις προσδοκίες χρησιμοποιώντας παραδοσιακές προσεγγίσεις. Πολύ σημαντικά θέματα για τη λειτουργία του αερολιμένα, τις αεροπορικές εταιρείες και τους επιβάτες κρίνεται η ενίσχυση των ροών των επιβατών και η ενίσχυση της απόδοσης εντός του χρόνου άφιξης της πτήσης. Αντιμέτωποι με την προοπτική έργων επέκτασης εντάσεως κεφαλαίου που απαιτούν χρόνια για να υλοποιηθούν, οι ψηφιακές τεχνολογίες μπορούν να χρησιμοποιηθούν με τέτοιο τρόπο έτσι ώστε να βοηθήσουν τα αεροδρόμια να ανταπεξέλθουν στις ανάγκες της εποχής και να αποσπάσουν τη μέγιστη αξία από τα υπάρχοντα περιουσιακά τους στοιχεία. Ωστόσο, αυτό που είναι επίσης σαφές είναι ότι προκειμένου να αποκομίσουν πλήρη οφέλη αυτών των νέων τεχνολογιών στο μέλλον, τα αεροδρόμια πρέπει να συνεχίσουν να εξελίσσονται καθημερινά.[117]

4.3.2. Ο ρόλος της Τεχνητής Νοημοσύνης στην τεχνολογική εξέλιξη των πληροφοριακών συστημάτων των Αεροδρομίων

Η τεχνητή νοημοσύνη (ΤΝ) έρχεται με ταχείς ρυθμούς και υιοθετείται ευρέως, μεταξύ άλλων και στον τομέα των αερομεταφορών. Ενώ η έννοια της τεχνητής νοημοσύνης υπάρχει από τη δεκαετία του 1950, η ανάπτυξή της έχει επιταχυνθεί σημαντικά την τελευταία δεκαετία λόγω τριών παραγόντων:

- Ικανότητα συλλογής και αποθήκευσης τεράστιων ποσοτήτων δεδομένων,
- Αύξηση της υπολογιστικής ισχύος
- Ανάπτυξη ολοένα και ισχυρότερων αλγορίθμων και αρχιτεκτονικών.

Η τεχνητή νοημοσύνη είναι ένας ευρύς όρος και ο ορισμός της έχει εξελιχθεί με την ανάπτυξη της τεχνολογίας. Ως εκ τούτου, ο οργανισμός EASA επέλεξε ένα ευρύ φάσμα ορισμού που είναι "κάθε τεχνολογία που φαίνεται να μιμείται τις επιδόσεις ενός ανθρώπου".

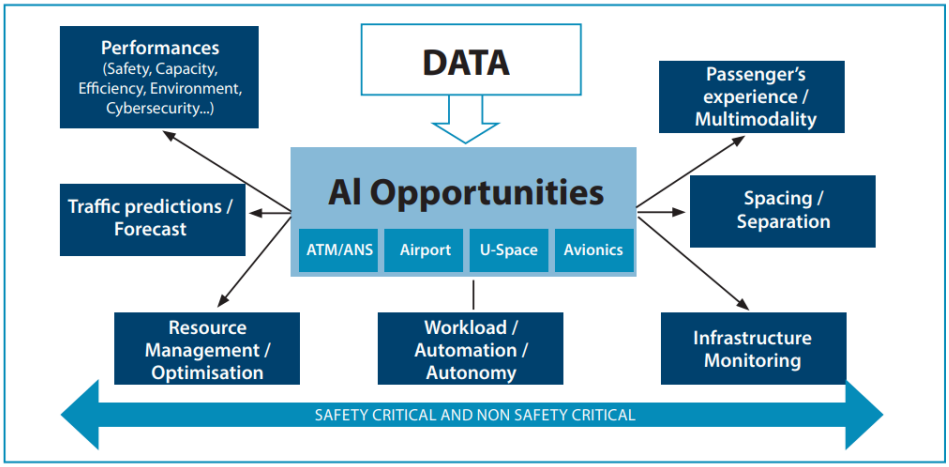
Τα συστήματα τεχνητής νοημοσύνης έχουν ήδη ενσωματωθεί σε καθημερινές τεχνολογίες όπως τα smartphones και οι προσωπικοί βοηθοί. Είναι επακόλουθο ότι το αεροπορικό σύστημα αρχίζει

[116] Cisco, 2009. Smart Airports: Transforming Passenger Experience To Thrive in the New Economy:https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf
[117] Arthur D. Little: Airports Digital Transformation.(2018). https://amadeus.com/documents/en/airports/research-report/airports-digital-transformation.pdf

ήδη να επηρεάζεται από αυτή την τεχνολογική επανάσταση. Όσον αφορά τον τομέα των αερομεταφορών, η τεχνητή νοημοσύνη δεν θα επηρεάσει μόνο τα προϊόντα και τις υπηρεσίες που παρέχει ο κλάδος αλλά θα θα προκαλέσει επίσης την εμφάνιση νέων επιχειρηματικών μοντέλων. Οι βασικές διαδικασίες ενός Οργανισμού (πιστοποίηση, θέσπιση κανόνων, εγκρίσεις οργανισμών και τυποποίηση) θα επηρεαστούν. Αυτό με τη σειρά του θα επηρεάσει το πλαίσιο ικανοτήτων και του προσωπικού του Οργανισμού.[118]

Η προσφορά της τεχνητής νοημοσύνης σε εφαρμογές είναι κυρίως η αυτοματοποίηση και αυτονομία πάνω στην επίλυση πολύπλοκων προβλημάτων σε διάφορους κλάδους. Η αεροπορία δεν αποτελεί εξαίρεση. Τα τελευταία χρόνια η τεχνητή νοημοσύνη έχει γίνει μια μετασχηματιστική τεχνολογία χάρη στις εκθετικές εξελίξεις της υπολογιστικής ισχύος, της διαθεσιμότητας δεδομένων και των εκτεταμένων δικτύων συσκευών.Ο κλάδος δείχνει έντονο ενδιαφέρον για τις δυνατότητες της τεχνητής νοημοσύνης και των κατηγοριών που εμπεριέχονται σε αυτή όπως μηχανική μάθηση (Machine Learning) και βαθιά μάθηση (Deep Learning), για την ανάπτυξη ευφυούς συντήρησης, μηχανικής και προγνωστικών εργαλείων, εφαρμογών για τον εξορθολογισμό των επιχειρηματικών διαδικασιών, των αλυσίδων εφοδιασμού, τις υπηρεσίες εξυπηρέτησης πελατών, και πολλά άλλα. Η διαχείριση της εναέριας κυκλοφορίας (ATM) είναι είναι από τους βασικούς τομείς που θα επηρεαστούν και θα ενισχυθούν μέσω της ΤΝ για μεγαλύτερη αυτοματοποίηση. Με τις επαναλαμβανόμενες διαδικασίες που παράγουν τεράστιες ποσότητες δεδομένων, οι αερομεταφορές και η ATM μπορούν να κάνουν χρήση της ΤΝ και υψηλότερων επιπέδων αυτοματοποίησης για να βελτιώσουν την αποτελεσματικότητα των λειτουργιών τους με πολλούς τρόπους και να επιτρέψουν στους ανθρώπινους χειριστές να επικεντρωθούν σε κρίσιμα για την ασφάλεια καθήκοντα. Μέσω της μηχανικής μάθησης μπορούν να εξορυχθούν τεράστιες ποσότητες ιστορικών δεδομένων για να υποστηρίξουν τους ανθρώπινους χειριστές στη λήψη των καλύτερων δυνατών αποφάσεων. Ακόμα, οι αυτοματοποιημένες αγορές μπορούν να βοηθήσουν τις αεροπορικές εταιρείες να καθορίσουν την κατανομή των πτήσεων χωρίς να αποκαλύπτουν προσωπικά δεδομένα τιμολόγησης μιας εμπορικής πτήσης.

[118]EASA Artificial Intelligence Roadmap- A human-centric approach to AI in aviation, 07 Feb 2020
https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-10



Σχήμα 16: Δυνατότητες για εφαρμογή ΤΝ στον αεροπορικό τομέα[119]

Αναλυτικότερα, οι λειτουργίες που θα εξελιχθούν μέσω της αυτοματοποίησης της ΤΝ, σύμφωνα με έρευνα που πραγματοποιήθηκε για τον αεροπορικό τομέα στις ευρωπαϊκές χώρες, περιλαμβάνουν :

1. **Μείωση του κόστους (και των καθυστερήσεων) στα αεροδρόμια με τη κατανομή πτήσεων μέσω της χρήσης προγνωστικής τεχνητής νοημοσύνης**

Η συγκέντρωση και η κοινή χρήση ευαίσθητων δεδομένων από τις αεροπορικές εταιρείες θα μπορούσε να βοηθήσει την υπηρεσία αεροναυτιλίας και τους παρόχους υπηρεσιών αεροναυτιλίας να προβλέπουν και να προγραμματίζουν καλύτερα την κατανομή των πτήσεων. Παράλληλα όμως πρέπει να εγγυάται η ασφάλεια στον κυβερνοχώρο και η προστασία της ιδιωτικής ζωής των δεδομένων.

2. **Βοήθεια μέσω της ΤΝ στους ελεγκτές εναέριας κυκλοφορίας να διατηρούν επίγνωση της κατάστασης**

Η αυτοματοποίηση στη διαχείριση της εναέριας κυκλοφορίας μπορεί να βελτιώσει την αποτελεσματικότητα με εργαλεία μηχανικής μάθησης που είναι πλήρως αξιόπιστα και συμπληρώνουν το έργο των ελεγκτών. Ο τομέας της διαχείρισης της εναέριας κυκλοφορίας (ATM) εξετάζει τρόπους εφαρμογής της αυτοματοποίησης για τη διαχείριση του φόρτου εργασίας, και να απελευθερώσει τη νοητική ικανότητα των ελεγκτών ώστε να μπορούν να να χειρίζονται περισσότερα αεροσκάφη και να επικεντρώνονται σε κρίσιμα για την ασφάλεια καθήκοντα, όπως η ανίχνευση συγκρούσεων.

[119] EUROCONTROL EUROPEAN AVIATION ARTIFICIAL INTELLIGENCE HIGH LEVEL GROUP The FLY AI Report Demystifying and Accelerating AI in Aviation/ATM 5th March 2020 www.eurocontrol.int/sites/default/files/2020-03/eurocontrol-fly-ai-report-032020.pdf

3. **Σχεδιασμός ασφαλούς διαδρομής μέσα από επικίνδυνες διαδρομές**

Ένα πρωτότυπο σύστημα τεχνητής νοημοσύνης που προσφέρει ακριβείς πληροφορίες για τις φυσικές καταστροφές και τα γεγονότα, όπως καταιγίδες και σύννεφα ηφαιστειακής τέφρας, θα μπορούσε να βοηθήσει τα αεροσκάφη να αποφύγουν τον κίνδυνο και τις διαταραχές.

4. **Αξιολόγηση των επιπτώσεων των αλλαγών στα συστήματα ATM στην ασφάλεια και την ανθεκτικότητα**

Ενώ η αυτοματοποίηση προσφέρει λύσεις για καλύτερη διαχείριση της ολοένα και πιο αυξημένης εναέριας κίνησης, φέρνει επίσης κινδύνους. Ο μεγάλος αριθμός ανθρώπων που ταξιδεύουν αεροπορικώς, σε συνδυασμό με μια διευρυμένη γκάμα μη συμβατικών αεροσκαφών, συμπεριλαμβανομένων διαφόρων μη επανδρωμένων οχημάτων, καθιστά πρόκληση για τη διαχείρισή της κυκλοφορίας. Οι αλλαγές στο περιβάλλον λειτουργίας των ATM, όπως τεχνολογικές αναβαθμίσεις και διαδικαστικές αλλαγές, μπορεί να έχουν ακούσιες, ενίοτε επικίνδυνες, συνέπειες. Εάν οι φορείς εκμετάλλευσης θα μπορούσαν να αξιολογήσουν εκ των προτέρων τις πιθανές επιπτώσεις των αλλαγών, θα θα μπορούσαν να τις μετριάσουν.

Το FARO (saFety And Resilience guidelines for aviatiOn) χρηματοδοτήθηκε στο πλαίσιο του κοινού προγράμματος SESAR που συστάθηκε για τον εκσυγχρονισμό της διαχείρισης της εναέριας κυκλοφορίας στην Ευρώπη. Συγκεκριμένα, εντοπίζει χαρακτηριστικά όπως ο φόρτος εργασίας, ο καιρός, οι συνθήκες και ο αριθμός των αεροσκαφών με καθυστέρηση, μετρήσεις που είναι σημαντικές για τη μοντελοποίηση της ασφάλειας και της ανθεκτικότητας από τεχνικής, οργανωτικής και ανθρώπινης προσέγγισης.

5. **Αυτόματη αναγνώριση ομιλίας για ασφαλέστερο έλεγχο εναέριας κυκλοφορίας**

Η αποτελεσματική επικοινωνία μεταξύ πιλότων και ελεγκτών είναι ζωτικής σημασίας για την ασφάλεια. Η αναγνώριση ομιλίας ανάμεσα σε ελεγκτές εναέριας κυκλοφορίας και των πιλότους παραμένει πρόκληση λόγω της τυποποιημένης φρασεολογίας, των διαφορετικών προφορών, διαφορετικών ταχυτήτων ομιλίας και τα θορυβώδη κανάλια. Δημιουργήθηκε το HAAWAII (Highly Automated Air Traffic Controller Workstations with Artificial Intelligence Integration) ως λογισμικό αναγνώρισης. Με μία ώρα χειροκίνητης μεταγραφής δεδομένων, η αναγνώριση λέξεων βελτιώθηκε διπλάσια. Μετά την εκπαίδευσή του σε όλα τα μεταγραμμένα και μη μεταγραμμένα δεδομένα, το ποσοστό αναγνώρισης λέξεων ήταν πάνω από 95 % για τους ελεγκτές και πάνω από 90 % για τους πιλότους.

6. **Θέτοντας τον επιβάτη στο επίκεντρο της πολυτροπικής κινητικότητας**

Καθώς τα αεροδρόμια εξελίσσονται σε κόμβους μεταφορών, η τεχνητή νοημοσύνη μπορεί να βοηθήσει στη χαρτογράφηση του ταξιδιού των επιβατών, τοποθετώντας τις βάσεις για ολοκληρωμένη ταξιδιωτική εμπειρία.

7. **Ενσωμάτωση της προγνωστικής ΤΝ στις ροές διαχείρισης της εναέριας κυκλοφορίας και Μέθοδοι μηχανικής μάθησης για τη μοντελοποίηση των πολυσύχναστων διαδρομών**

Η υπολογιστική ισχύς που απαιτείται για τη μοντελοποίηση της εναέριας κυκλοφορίας και τη διαχείριση των ροών αυξάνεται. Το χρηματοδοτούμενο από την ΕΕ και τη βιομηχανία έργο SIMBAD (Combining Simulation Models and Big Data Analytics for ATM Performance Analysis) έχει αναπτύξει ισχυρά συστήματα που βασίζονται σε τεχνητή νοημοσύνη με μοντέλα προσομοίωσης που καθιστούν πολύ πιο εύκολη την αξιολόγηση νέων σεναρίων εναέριας κυκλοφορίας. Έχουν αναπτυχθεί σύγχρονες τεχνικές μοντελοποίησης με βάση την τεχνητή νοημοσύνη, χρησιμοποιώντας νέες προσεγγίσεις μηχανικής μάθησης για τη βελτίωση των σημερινών προσομοιώσεων της εναέριας κυκλοφορίας.

8. **Λογισμικό τεχνητής νοημοσύνης που υπερασπίζεται τα αεροναυτικά συστήματα από κυβερνοεπιθέσεις**

Οι διαταραχές στα δίκτυα αεροπορικών επικοινωνιών αποτελούν σοβαρή απειλή για την ασφάλεια και την την αποτελεσματικότητα. Ένα λογισμικό τεχνητής νοημοσύνης μπορεί να προβλέψει και να αποτρέψει αυτόν τον κίνδυνο. Όπως κάθε ψηφιακό δίκτυο, τα συστήματα αεροναυτικών επικοινωνιών είναι ευάλωτα σε προσωρινές ή μόνιμες διαταραχές. Αυτές μπορούν να προκληθούν από τοπικές συνθήκες, όπως ένας μεγάλος αριθμός αεροσκαφών που προσπαθούν να στείλουν ή να λάβουν δεδομένα με φορείς εκμετάλλευσης εδάφους, ή με την έλλειψη κάλυψης μεταξύ αεροσκαφών και επίγειων κέντρων. Αυτά τα συστήματα είναι επίσης ευάλωτα σε επιθέσεις στον κυβερνοχώρο.

Σύμφωνα με τεχνικούς, στην πιο ακραία περίπτωση, χρειάζονται έξι λεπτά για μια διαταραχή να επιβεβαιωθεί, μια περίοδος κατά την οποία οι εντολές των ελεγκτών δεν μπορούν να να εκτελεστούν από τους πιλότους. Οποιαδήποτε διαταραχή σε ένα αεροσκάφος έχει έμμεσες επιπτώσεις σε άλλα αεροσκάφη που βρίσκονται κοντά, καθώς η χωρητικότητα του εναέριου χώρου υποβαθμίζεται και τα αεροπλάνα μπορεί να καθυστερήσουν ή να αναδρομολογηθούν. Κατα συνέπεια οποιαδήποτε πρόβλεψη ενός προβλήματος στο δίκτυο επικοινωνιών συμβάλλει στη μείωση του αντίκτυπού τους στις συνολική κυκλοφορία.

Το έργο SINAPSE (Software defined networking architecture επαυξημένο με τεχνητή νοημοσύνη για τη βελτίωση των αεροναυτικών επικοινωνιών, την ασφάλεια και την αποδοτικότητα), που χρηματοδοτείται στο πλαίσιο της κοινής επιχείρησης SESAR για τον εκσυγχρονισμό του ευρωπαϊκού συστήματος διαχείρισης της εναέριας κυκλοφορίας, έχει δημιουργήσει ένα νέο λογισμικό που χρησιμοποιεί ΤΝ για την πρόβλεψη τέτοιων διακοπών. Βασίζεται στη δικτύωση που καθορίζεται από το λογισμικό (SDN), μια κατανεμημένη αρχιτεκτονική λογισμικού που επιτρέπει αυξημένη διαμόρφωση του δικτύου, πάντα με παρακολούθηση από έναν κεντρικό ελεγκτή. Στα παραδοσιακά συστήματα,η έννοια του ελεγκτή βασίζεται σε ανθρώπους, αλλά το SINAPSE εισήγαγε την τεχνητή νοημοσύνη ως ελεγκτή, για

την αποτελεσματικότερη διαχείριση του συστήματος. Ελέγχει αυτόματα για σφάλματα στα δίκτυα, και χρησιμοποιώντας προγνωστικές πληροφορίες μπορεί να ρυθμίσει προληπτικά το σύστημα και να εκτελεί συντήρηση.

Το SINAPSE χρησιμοποιεί επιχειρησιακά δεδομένα σε πραγματικό χρόνο και παρακολουθεί το δικτύου για την πρόβλεψη βλαβών επικοινωνίας. Κατά τη διάρκεια του έργου, η ομάδα SINAPSE αξιολόγησε την τεχνολογία με τον ελεγκτή Pilot Data Link Communications (CPDLC), τα οποία καταγράφονται σε πραγματικό χρόνο από το επιχειρησιακό δίκτυο αεροναυτικών τηλεπικοινωνιών (ATN), ένα παγκόσμιο σύστημα αεροπορικών επικοινωνιών.

Μια στοχευμένη περίπτωση χρήσης έδειξε ότι το SINAPSE θα μπορούσε να προβλέπει συμβάντα διαταραχής 10 λεπτά προτού συμβούν. Αυτές οι πληροφορίες θα μπορούσαν να είναι πολύ χρήσιμες και θα μπορούσε τελικά να αποτρέψει γεγονότα απώλειας επικοινωνίας σε διάφορες καταστάσεις.

9. Τεχνητή νοημοσύνη για αυξημένη εμπιστοσύνη στο λογισμικό διαχείρισης εναέριας κυκλοφορίας

Ενώ η τεχνητή νοημοσύνη χρησιμοποιείται στη διαχείριση της εναέριας κυκλοφορίας (ATM), όπως η ανάλυση μετά από συμβάντα ή η πρόβλεψη, δεν έχει ακόμη ενσωματωθεί πλήρως σε όλες τις λειτουργίες της. Η τεχνητή νοημοσύνη δεν εντάσσεται στους παραδοσιακούς κύκλους εργασίας της μηχανικής, οι οποίοι ευνοούν τα γραμμικά βήματα με προβλέψιμα αποτελέσματα. Αυτό είναι και ο λόγος που κρίνεται ιδιαίτερα δύσκολο στις εθνικές αρχές να την επικυρώσουν και να την πιστοποιήσουν για κρίσιμες για την ασφάλεια λειτουργίες.

Οι τεχνικές τεχνητής νοημοσύνης συχνά δεν είναι εύκολα κατανοητές στον άνθρωπο. Ο αυτόνομος σχεδιασμός των περισσότερων ΤΝ σημαίνει ότι οι χρήστες συνήθως δεν καταλαβαίνουν γιατί λήφθηκε μια απόφαση έναντι μιας άλλης, καθιστώντας δύσκολη την αντίστροφη μηχανική ενός επιτυχημένου ή αποτυχημένου αποτέλεσματος. Πρέπει να αυξηθεί η επεξηγηματικότητα της τεχνητής νοημοσύνης, δηλαδή να μετατραπεί το εσωτερικό, οι λειτουργίες της, οι κανόνες, οι ικανότητες και οι περιορισμοί της πιο διαφανείς στους δυνητικούς χρήστες.

Σε όλους τους κλάδους, η αυξημένη χρήση της τεχνητής νοημοσύνης φέρνει μαζί της σοβαρά ηθικά ζητήματα. Επειδή οι αερομεταφορές είναι κρίσιμες για την ασφάλεια και επικεντρώνονται στον άνθρωπο, είναι σημαντικό οι λύσεις ΤΝ σε αυτόν τον χώρο να είναι κατανοητές και αξιόπιστες. Η ηθική προσέγγιση της τεχνητής νοημοσύνης είναι σημαντική για την ενίσχυση της εμπιστοσύνης των πολιτών στην ψηφιακή ανάπτυξη και για την οικοδόμηση ενός ανταγωνιστικού πλεονεκτήματος για τις εταιρείες. [120]

[120] European Commission, Sesar Joint Undertaking " AI in air traffic management- Bringing intelligent and trustworthy automation to Europe's aviation sector- A thematic collection of innovative EU-funded research result,

4.3.3 Ο ρόλος της IT/OT τεχνολογίας στη κυβερνοασφάλεια των Αεροδρομίων.

Οι τεχνολογίες IT/OT αναφέρονται συγκεκριμένα στη σύγκλιση των Πληροφοριακών Τεχνολογιών (IT) και των Τεχνολογιών Επιχειρησιακής Λειτουργίας (OT). Η Πληροφοριακή Τεχνολογία (IT) αφορά στην τεχνολογία που συνδέεται με την επεξεργασία, αποθήκευση και διακίνηση δεδομένων και πληροφοριών. Αυτό περιλαμβάνει τους υπολογιστές, το διαδίκτυο, το λογισμικό, την αποθήκευση δεδομένων και άλλες σχετικές τεχνολογίες. Από την άλλη πλευρά, οι Επιχειρησιακές Τεχνολογίες (OT) αναφέρονται στις τεχνολογίες που σχετίζονται με τη λειτουργία και τον έλεγχο φυσικών διαδικασιών και εγκαταστάσεων. Αυτό περιλαμβάνει τους αισθητήρες, τα προγράμματα ελέγχου, τις βιομηχανικές μηχανές και άλλα συστατικά που χρησιμοποιούνται σε βιομηχανικές και ενεργειακές εγκαταστάσεις. Η έννοια της σύγκλισης IT/OT αναφέρεται στην ολοκληρωμένη χρήση των τεχνολογιών τόσο της Πληροφοριακής Τεχνολογίας όσο και των Επιχειρησιακών Τεχνολογιών για τη βελτίωση της αποτελεσματικότητας, της ασφάλειας και της αυτοματοποίησης της βιομηχανίας των αεροπορικών μεταφορών. Αυτή η σύγκλιση επιτρέπει την αλληλεπίδραση μεταξύ των ψηφιακών και φυσικών κόσμων, δημιουργώντας έτσι ένα ολοκληρωμένο περιβάλλον όπου οι διαδικασίες μπορούν να αυτοματοποιηθούν και να βελτιστοποιηθούν για καλύτερη απόδοση και αποτελέσματα.[121]

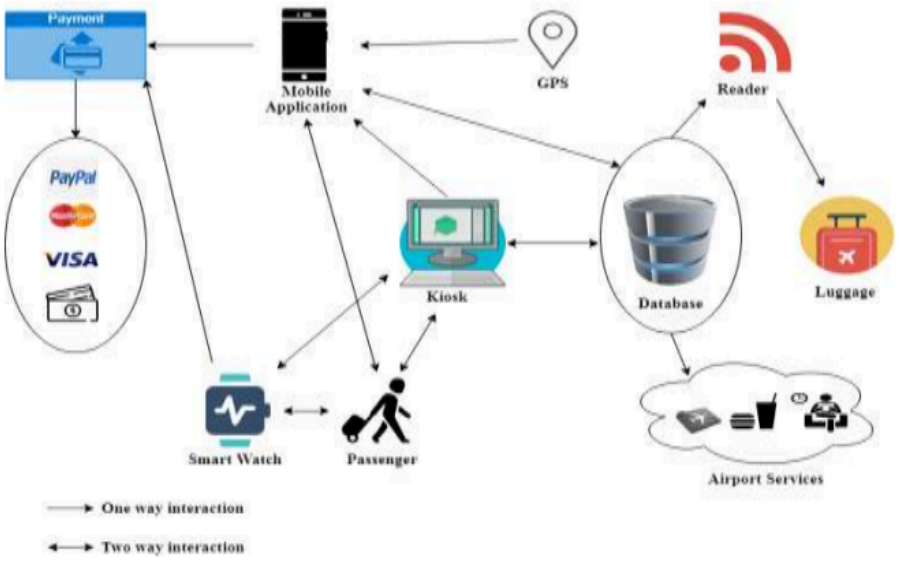
Η πληροφορική και οι επικοινωνίες έχουν υποστεί αξιοσημείωτες αλλαγές τις τελευταίες δεκαετίες. Η εμπορική αεροπορία καλύπτει πολλούς τομείς, την επιχειρηματική αεροπορία, την προσωπική αεροπορία, τις εμπορευματικές μεταφορές. Υπάρχουν πολλοί παράγοντες που εμπλέκονται στη λειτουργία και τη συντήρηση αυτών των τομέων. Σήμερα υπάρχουν τεράστιες ευκαιρίες για την ανάπτυξη του IoT στην εμπορική αεροπορία. Οι ευκαιρίες αυτές καλύπτουν τόσο τη λειτουργική αποδοτικότητα των εμπορικών αεροσκαφών όσο και τις ευκαιρίες αξιοποίησης των δεδομένων των συσκευών σε πραγματικό χρόνο για την παροχή ολοκληρωμένης προληπτικής συντήρησης και νοημοσύνης που συνδέεται με την προηγμένη διαχείριση. Λόγω του μεγάλου αριθμού χρηστών στο ασύρματο περιβάλλον, το παράδειγμα επικοινωνίας έχει επίσης μετατοπιστεί στην έννοια των γνωστικών ραδιοδικτύων για την καλύτερη αξιοποίηση του ασύρματου φάσματος. Είναι περιττό να πούμε ότι η εξέλιξη του φορητού εξοπλισμού και η τεράστια δημοτικότητα των κινητών εφαρμογών οδηγεί στην ανάγκη έγκαιρης ανάλυσης και παροχής ασφάλειας στο περιβάλλον επικοινωνίας.

Οι συσκευές IoT παρέχουν στους χρήστες αρκετές σημαντικές δυνατότητες, όπως ευκολία στη χρήση, μικρές διαστάσεις και ασύρματη συνδεσιμότητα. Οι συσκευές αυτές αποτελούνται από αισθητήρες όπως η θερμοκρασία, η υγρασία και ο ήχος και συνήθως αποτελούν μέρος ενός

Oct. 2022
https://www.sesarju.eu/sites/default/files/documents/AI%20in%20air%20traffic%20management%20brochure.pdf

[121] Arthur D. Little: Airports Digital Transformation(2018) ό.π.

δικτύου που επιτρέπει τον έλεγχο μέσω μιας κεντρικής συσκευής όπως ένα smartphone ή ένας υπολογιστής. Καθώς τα εμπορικά αεροδρόμια συνδέονται περισσότερο ψηφιακά, το IoT μπορεί να ανοίξει έναν κόσμο ευκαιριών. Πολύ περισσότερο από την απλή βελτίωση της αποδοτικότητας, το IoT μπορεί να μεταμορφώσει την εμπειρία των επιβατών. "Πράγματα" που αντιλαμβάνονται και συλλέγουν δεδομένα και τα στέλνουν στο διαδίκτυο. Το IoT είναι το δίκτυο των συνδεδεμένων στο διαδίκτυο συσκευών, δρόμων, αεροσκαφών, αεροδρομίων, πληρώματος, επιβατών και άλλων πραγμάτων με λογισμικό, αισθητήρες, ηλεκτρονικά και συνδεσιμότητα δικτύου που επιτρέπει σε αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν πληροφορίες. Υπάρχουν πολλές προκλήσεις και κίνδυνοι στον κυβερνοχώρο για την εφαρμογή υπηρεσιών που βασίζονται στο IoT στην εμπορική αεροπορία.[122]



Σχήμα 17: Αλληλεπίδραση μεταξύ "πραγμάτων" σε περιβάλλον αεροδρομίου

Τα συστήματα αυτοματισμού και ελέγχου, όπως το SCADA (Supervisory Control and Data Acquisition), το DCS (Distributed Control Systems) αναφέρονται ως επιχειρησιακή τεχνολογία (OT). Τα συστήματα αυτά χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο κρίσιμων υποδομών, όπως η ηλεκτρική ενέργεια, οι αγωγοί, η διανομή νερού, τα συστήματα αποχέτευσης και ο έλεγχος της παραγωγής. Παραδοσιακά, αυτά τα συστήματα OT είχαν ένα βαθμό φυσικού διαχωρισμού από τις υποδομές τεχνολογίας πληροφοριών (ΤΠ). Με τις μεταβαλλόμενες τεχνολογίες και την τάση για λειτουργία με βάση τα δεδομένα και από απόσταση, τα δύο τεχνολογικά περιβάλλοντα αρχίζουν να συγκλίνουν.

[122] Aboti, Chiragkumar (2019).Survey on IoT: Challenges and cyber risks in commercial aviation. 6. 970. 10.1729/Journal.22604 https://www.researchgate.net/publication/337485708_Survey_on_IoT_Challenges_and_cyber_risks_in_commercial_aviation

Η τεχνολογία IT/OT παίζει έναν σημαντικό ρόλο στην κυβερνοασφάλεια των αεροδρομίων, παρέχοντας εργαλεία και λύσεις για την προστασία των συστημάτων και των δικτύων τους από διάφορες απειλές κυβερνοασφάλειας. Οι τεχνολογίες IT/OT χρησιμοποιούνται για την παρακολούθηση, τη διαχείριση και την προστασία των λειτουργικών συστημάτων, των δικτύων επικοινωνίας, των αισθητήρων ασφαλείας, των συστημάτων ανίχνευσης και άλλων κρίσιμων υποδομών. Χρησιμοποιούνται επίσης για την ανίχνευση και αποτροπή επιθέσεων, την προστασία από κακόβουλο λογισμικό, τον περιορισμό της πρόσβασης σε ευαίσθητα δεδομένα και την αντιμετώπιση πιθανών απειλών κυβερνοασφάλειας. Επιπλέον, συμβάλλει στην ανάπτυξη και εφαρμογή συστημάτων αυτοματισμού και ελέγχου, τα οποία μπορούν να βελτιώσουν την αποτελεσματικότητα και την ασφάλεια των διαδικασιών στα αεροδρόμια. Οι εφαρμογές IT/OT μπορούν να βοηθήσουν στην αυτοματοποίηση της διαχείρισης της κίνησης των αεροσκαφών, τη διαχείριση των αποσκευών, την ασφάλεια των πτήσεων και άλλων λειτουργιών στα αεροδρόμια.Με αυτή τη σύγκλιση των τεχνολογιών IT/OT, αυτό που ήταν ένα σχετικά αυτόνομο, ασφαλές και απομονωμένο περιβάλλον είναι πλέον συνδεδεμένο και προσβάσιμο μέσω του Διαδικτύου/υπολογιστικού νέφους. Με αυτή τη διασύνδεση έρχονται οι προκλήσεις της ασφάλειας στον κυβερνοχώρο που συνήθως συνδέονται μόνο με τις υποδομές των Τεχνολογιών της Πληροφορίας. Τα δεδομένα OT που είναι στη συνέχεια προσβάσιμα από αυτά τα περιβάλλοντα θα μπορούσαν να περιλαμβάνουν κρίσιμες πληροφορίες όπως πιέσεις, θερμοκρασίες, επίπεδα εγγύτητας, σήματα ελέγχου και άλλα σήματα αισθητήρων. Η υιοθέτηση του ψηφιακού μετασχηματισμού από τον αεροπορικό τομέα αποσκοπεί στην αύξηση της αποτελεσματικότητας και τη μείωση του κόστους λειτουργίας του. Ωστόσο, μπορεί να δημιουργήσει νέους κινδύνους, καθώς αυξάνει την πιθανότητα περιστατικών κυβερνοεπιθέσεων στις υποδομές των αερολιμένων, ιδίως στα λειτουργικά τους στοιχεία (OT). Έτσι, όσο πιο ψηφιακά συνδεδεμένη γίνεται η αεροπορική βιομηχανία , τα δεδομένα OT και οι σχετικοί μηχανισμοί ελέγχου είναι πλέον σημαντικά ευάλωτα σε κυβερνοεπιθέσεις.[123]

Η φράση “OT air gap” αναφέρεται στην απομόνωση των Επιχειρησιακών τεχνολογιών (OT) από τα δίκτυα Πληροφορικής (IT). Συγκεκριμένα, στον τομέα των κρίσιμων υποδομών, δηλαδή στις υποδομές αερολιμένων, οι συσκευές και τα συστήματα που ελέγχουν τις φυσικές διεργασίες (δηλ. Συστήματα SCADA όπως αισθητήρες, ελεγκτές, αυτόματο σύστημα διαχείρισης αποσκευών) συνήθως λειτουργούν σε ξεχωριστά δίκτυα από αυτά που χρησιμοποιούνται για τα συστήματα πληροφορικής και επικοινωνιών. Τα συστήματα OT σχεδιάστηκαν για να ενσωματώνουν συστήματα απόκτησης δεδομένων, συστήματα συλλογής/μετάδοσης δεδομένων και συστήματα διεπαφής ανθρώπου-μηχανής (HMI) για τη δημιουργία μιας κεντρικής λύσης ελέγχου και παρακολούθησης. Έτσι, επιτρέποντας σε έναν χειριστή να ερμηνεύει οπτικά την κατάσταση της εγκατάστασης για σκοπούς ελέγχου και παρακολούθησης. Η δημιουργία αυτού του διαχωρισμού δικτύων (air-gapped networks) έχει ως στόχο να μειώσει τον κίνδυνο κυβερνοεπιθέσεων, καθώς με την απομόνωση των OT συστημάτων από το διαδίκτυο με τα εξωτερικά δίκτυα μειώνονται οι πιθανότητες εισβολής και κακόβουλων επιθέσεων. Για τους

[123] Glenn Murray, Michael N. Johnstone, Craig Valli (2017). The convergence of IT and OT in critical Infrastructures: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1217&context=ism

περισσότερους οργανισμούς το “OT air gap” βοηθούσε αλλά και παρεμπόδιζε την ασφάλεια. Ο διαχωρισμός αυτός οδεύει ουσιαστικά προς την εξαφανιση, οδηγώντας σε αυξημένες ανησυχίες που πρέπει να αντιμετωπιστούν όπως η στοχοποίηση της υποδομής OT για κακόβουλο λογισμικό, επιθέσεις phishing.[124]

4.3.4.Κίνδυνοι των νέων τεχνολογιών και ευαλωτότητες των συστημάτων

4.3.4.1 Κίνδυνοι της τεχνολογίας IT/OT στον Αεροπορικό τομέα

Η ασφάλεια στις παγκόσμιες αερομεταφορές εξαρτάται όλο και περισσότερο από τα τρωτά σημεία της τεχνολογίας των πληροφοριών (IT) και της επιχειρησιακής τεχνολογίας (OT).Ένα πρόσφατο άρθρο που αναμεταδόθηκε από το Κέντρο Ανταλλαγής και Ανάλυσης Πληροφοριών Αεροπορίας των ΗΠΑ (A-ISAC) εστιάζει στα τρωτά σημεία των αεροδρομίων και συγκεκριμένα των δικτύων επιχειρησιακής τεχνολογίας (OT). Τα κρίσιμα συστήματα αεροδρομίων που κάνουν χρήση OT περιλαμβάνουν τον έλεγχο αποσκευών, τα φώτα διαδρόμου, τον εναέριο κλιματισμό και την ηλεκτρική ενέργεια, και η διαχείρισή τους γίνεται μέσω ψηφιακών ελεγκτών συνδεδεμένων σε δίκτυο. Σύμφωνα με το άρθρο, είναι πολύ λιγότερο οργανωμένα από τα συμβατικά δίκτυα IT. Παρακολουθούνται σπάνια όσον αφορά τη λειτουργία τους και συχνά μένουν ανέγγιχτα για χρόνια. Πρόκειται για μια αναδυόμενη απειλή που έχει προκαλέσει την προσοχή δεκάδων υπεύθυνων ασφάλειας πληροφοριών αεροδρομίων. Συγκεκριμένα, έχουν εντοπιστεί περισσότερα από εκατό μοναδικές ευαλωτότητες στη Επιχειρησιακή τεχνολογία των συστημάτων των αεροδρομίων. Οι τέσσερις σημαντικοί φορείς κινδύνου που έχουν εντοπιστεί πιο συγκεκριμένα είναι:

Απειλή 1:Διαχείριση αποσκευών

Τα συστήματα αυτά αποτελούν εξαιρετικά ελκυστικούς στόχους για μια επίθεση, επειδή μπορούν να εκτελεστούν εξ αποστάσεως- ο επιτιθέμενος δεν θα χρειαζόταν καν να επιβιβαστεί στο αεροπλάνο. Το μόνο που απαιτείται είναι ένα μόνο άτομο να πέσει στην παγίδα ενός απλού phishing email και ο επιτιθέμενος μπορεί να εισάγει κακόβουλο λογισμικό ειδικά για OT στο δίκτυο του αεροδρομίου. Αυτό το κακόβουλο λογισμικό θα ενσωματωθεί στο σύστημα διαχείρισης αποσκευών για να εκτελέσει την επίθεση.

Απειλή 2:Ρυμουλκά αεροσκαφών

Οι επιτιθέμενοι θα μπορούσαν δυνητικά να καταλάβουν τους αισθητήρες βάρους ενός ρυμουλκού και να ρίξουν ένα μεγάλο αεροσκάφος σε μια πύλη με την ταχύτητα που χρησιμοποιείται για ένα μικρό αεροπλάνο, προκαλώντας τη συντριβή του στον τοίχο του αεροδρομίου.

[124] Fortinet(2021): State of Operational Technology Security in Transportation and logistics: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-ot-transportation-and-logistics.pdf

Απειλή 3: Συστήματα αποπαγοποίησης

Τα υγρά χημικά που χρησιμοποιούνται για την αποπαγοποίηση αποθηκεύονται στις εγκαταστάσεις του αεροδρομίου. Οι εγκαταστάσεις αυτές χρησιμοποιούν συσκευές OT για τη ρύθμιση και τη διατήρηση της σύνθεσης των χημικών ουσιών αποπάγωσης. Εάν τα συστήματα αυτά δεχθούν επίθεση και η σύνθεση του διαλύματος αλλάξει, αυτό θα μπορούσε εύκολα να προκαλέσει το σχηματισμό πάγου στο σώμα ενός αεροπλάνου. Η αλλοίωση της αεροδυναμικής ενός αεροπλάνου με την παραβίαση των συστημάτων αποπάγωσης είναι ένας τρόπος να προκληθεί συντριβή του χωρίς τη φόρτωση εκρηκτικών υλών σε αυτό, και αυτός είναι πιθανόν ο λόγος για τον οποίο τα συστήματα αποπάγωσης, όσο ασαφής και αν είναι ο φορέας κινδύνου, είναι συχνά ένα από τα πρώτα συστήματα OT που παρακολουθούν τα αεροδρόμια.

Απειλή 4: Αντλίες καυσίμων

Ένας επιτιθέμενος θα μπορούσε, για παράδειγμα, να εισβάλει σε μια αποθήκη καυσίμων, προκαλώντας την άντληση καυσίμων λανθασμένου τύπου ή μίγματος σε ένα αεροπλάνο, με αποτέλεσμα από προβλήματα στον κινητήρα μέχρι έκρηξη. [125]

Τα πιθανά αποτελέσματα που θα μπορούσαν να προκύψουν από μια κυβερνοεπίθεση OT περιλαμβάνουν:

- Καθυστέρηση στις πληροφορίες που διαβιβάζονται σε ένα ICS/DCS/SCADA Master από μια απομακρυσμένη τερματική μονάδα (RTU). Αυτή η καθυστέρηση θα μπορούσε να οδηγήσει σε ένα καταστροφικό συμβάν, καθώς οι πληροφορίες θα μπορούσαν να αφορούν τον αισθητήρα στάθμης, τον αισθητήρα συναγερμού ή τους ενεργοποιητές.
- Διακοπή της σύνδεσης μεταξύ ενός ICS/DCS/SCADA Master για την ενεργοποίηση ενός συμβάντος μέσω ενός συστήματος ασφαλείας.
- Αλλαγή των τιμών που λαμβάνονται από ένα ICS/DCS/SCADA Master. Αυτό θα μπορούσε είτε να έχει μια αυτόματη αντίδραση, όπως να κλείσει ένα τμήμα μιας εγκατάστασης, είτε να οδηγήσει σε ανθρώπινη αντίδραση, η οποία θα μπορούσε να οδηγήσει σε ακατάλληλη ενέργεια.
- Τιμές σημείου ρύθμισης των RTU. Ένα παράδειγμα θα ήταν η αλλαγή του σημείου ρύθμισης συναγερμού για έναν αισθητήρα στάθμης σε ένα δοχείο. Ως εκ τούτου, προκαλείται υπερχείλιση του δοχείου.
- Αλλαγή/τροποποίηση της λειτουργίας των συστημάτων προστασίας του εξοπλισμού, π.χ. επιτάχυνση μιας τουρμπίνας σε ένα εργοστάσιο με αποτέλεσμα την καταστροφή των πτερυγίων.

[125] CERT-EU(2019): Airports & Operational Technology: 4 Attack-Scenarios: https://cow-prod-www-v3.azurewebsites.net/publications/threat-intelligence/threat-memo-190404-2/pdf

Λαμβάνοντας υπόψη το ευρύ φάσμα των ευάλωτων πρωτοκόλλων που χρησιμοποιούνται στο IT/OT και το υψηλό κόστος των παραβιάσεων δεδομένων (π.χ. κόστος επανεκκίνησης εγκαταστάσεων, μείωση της τιμής των μετοχών), είναι απαραίτητη η περαιτέρω έρευνα για τη μείωση του κινδύνου για τις κρίσιμες υποδομές.[126]

Σύμφωνα με την έρευνα της Fortinet (2021), το 43% των οργανισμών μεταφοράς και logistics αντιμετώπισαν τέσσερις ή περισσότερες επιθέσεις στην κυβερνοασφάλεια των λειτουργικών τους τεχνολογιών (OT). Το 56% ανησυχούν περισσότερο για πιθανές μελλοντικές παραβιάσεις σε αυτόν τον τομέα σε σχέση με το παρελθόν. Επίσης αναφέρεται ότι το 80% των οργανισμών θεωρούν ότι οι εσωτερικοί παράγοντες τους είναι αυτοί που αποτελούν τον μεγαλύτερο κίνδυνο για την κυβερνοασφάλεια των επιχειρησιακών τους τεχνολογιών (OT).

Οι δύο κύριες τεχνολογίες για θέματα ασφάλειας OT έχουν ήδη αρχίσει να αναπτύσσονται σε οργανισμούς μεταφορών και logistics. Οι οργανισμοί αυτοί εστιάζουν στη διαχείριση των τρωτών σημείων και τη τμηματοποίηση του δικτύου. Παρόλα αυτά, η ενσωμάτωση της επιχειρησιακής τεχνολογίας (OT) στα δίκτυα πληροφορικής (IT) είναι αναπόφευκτη, καθώς τα συστήματα OT, τα οποία στο παρελθόν ήταν ανενεργά, τώρα είναι στη πλειοψηφία τους συνδεδεμένα στο διαδίκτυο και ευάλωτα σε κυβερνο-επιθέσεις.

Οι πρακτικές που πρέπει να ενσωματωθούν από τους οργανισμούς που κάνουν χρήση συστημάτων OT για την ασφάλεια τους:

1. **Τμηματοποίηση του δικτύου**

Όσο "μικραίνει" το OT air gap, μια καλή πρακτική αποτελεί η τμηματοποίηση του δικτύου σε λειτουργικά τμήματα, που κι αυτά θα έχουν τη δυνατότητα περαιτέρω τμηματοποίησης. Έτσι θα εξασφαλίζεται η πρόσβαση μόνο σε εξουσιοδοτημένες συσκευές, εφαρμογές και χρήστες.

2. **Έλεγχος ταυτότητας και διαχείρισης πρόσβασης**

Ένας μεγάλος αριθμός κυβερνοεπιθέσεων OT είναι αποτέλεσμα διαρροής διαπιστευτηρίων πρόσβασης σε συστήματα μέσω της τεχνικής phishing. Η συγκεκριμένη πρακτική ασφαλείας συχνα αγνοείται από τους περισσότερους οργανισμούς, ενώ θα έπρεπε να αποτελεί προτεραιότητα.

3. **Προσδιορισμός των περιουσιακών στοιχείων**

Ως καλή πρακτική θεωρείται η ταξινόμηση και ιεράρχηση της αξίας των περιουσιακών στοιχείων μιας κρίσιμης υποδομής, έτσι ώστε να δοθεί προτεραιότητα στην ασφάλεια των περιουσιακών στοιχείων που ο οργανισμός θα πρέπει να επικεντρωθεί.

[126] Glenn Murray, Michael N. Johnstone, Craig Valli (2017). The convergence of IT and OT in critical Infrastructures ό.π.

4. **Ανάλυση της κίνησης σχετικά με τις απειλές στα τρωτά σημεία του οργανισμού**

Με τη τμηματοποίηση του δικτύου σε μικρότερες μονάδες, που αναφέρθηκε παραπάνω, οι κινήσεις που θα εμφανίζονται στο διαιρεμένο δίκτυο IT/OT θα πρέπει να εξεταστούν για γνωστές αλλά και άγνωστες απειλές.

5. **Προστασία ενσύρματης και ασύρματης πρόσβασης**

Στο περιβάλλον OT, οι περισσότερες κυβερνοεπιθέσεις γίνονται μέσω των μεταγωγέων δικτύου (network switches) και των ασύρματων σημείων σύνδεσης (WAP). Η λύση για την ασφάλεια των ενσύρματων και ασύρματων δικτύων είναι η διαχείριση τους μέσω μιας κεντρικής διεπαφής αντί μεμονωμένων διαφορετικών διεπαφών. Με αυτό το τρόπο γίνεται καλύτερη εστίαση στη διαχείριση της απειλής και μειώνεται το ρίσκο μιας επίθεσης. Επιπλέον βελτιώνεται η δυνατότητα πρόβλεψης του οργανισμού των κινδύνων και μειώνεται ο χρόνος επίλυσης του προβλήματος από τις ομάδες ασφαλείας του οργανισμού.[127]

4.3.4.2 Κίνδυνοι της Τεχνητής Νοημοσύνης για τον Αεροπορικό τομέα

Στον τομέα της αεροπορίας, οι εφαρμογές της τεχνητής νοημοσύνης έχουν φέρει επαναστατικές αλλαγές, βελτιώνοντας την ασφάλεια, την απόδοση και την εμπειρία των επιβατών. Ωστόσο, με την αυξανόμενη χρήση της τεχνητής νοημοσύνης στον αεροπορικό τομέα, εμφανίζονται και ορισμένοι κίνδυνοι που απαιτούν προσεκτική αντιμετώπιση.

Η ενσωμάτωση της τεχνητής νοημοσύνης σε επιχειρησιακές λειτουργίες, αεροπορικά συστήματα ελέγχου, πλοήγησης και συντήρησης αποφέρει οφέλη όπως η αυτοματοποίηση και η βελτίωση της απόδοσης. Παράλληλα, όμως, οι τεχνολογικές αυτές εξελίξεις συνοδεύονται από πιθανούς κινδύνους, όπως:

- Η έλλειψη της εμπιστευτικότητας των δεδομένων που επεξεργάζονται και εξάγονται από την TN
- Η αυξημένη ευπάθεια σε κυβερνοεπιθέσεις
- Η ανθρώπινη αναποτελεσματικότητα λόγω υπερβολικής εμπιστοσύνης στην τεχνολογία

Ένα μεγάλο κεφάλαιο της TN είναι τα δεδομένα εκπαίδευσης των αλγορίθμων για τη διεξαγωγή αποφάσεων. Η δύναμη της μηχανικής μάθησης (Machine Learning - ML) έγκειται στη δυνατότητα ενός συστήματος να μαθαίνει από ένα σύνολο δεδομένων αντί να απαιτεί την ανάπτυξη και προγραμματισμό κάθε απαραίτητης διαδρομής για τη λήψη απόφασης σε ένα λογισμικό. Η αεροπορική βιομηχανία λοιπόν έρχεται αντιμέτωπη με έναν αριθμό προκλήσεων όσον αφορά την αξιοπιστία του λογισμικού ML/DL(Deep Learning), καθώς μπορεί κλονιστεί η

[127]Fortinet(2021): State of Operational Technology Security in Transportation and logistics: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-ot-transportation-and-logistics.pdf

προστασία της ιδιωτικότητας και η αξιοπιστία των δεδομένων που διαχειρίζονται τα συστήματα ΤΝ.

- **Τα παραδοσιακά πλαίσια διασφάλισης της ανάπτυξης δεν είναι προσαρμοσμένα στη μηχανική μάθηση.**

Το ML δίνει πρόσθετη έμφαση σε άλλα μέρη της διαδικασίας, δηλαδή στην προετοιμασία των δεδομένων, στην αρχιτεκτονική, στην επιλογή αλγορίθμων, στη ρύθμιση υπερ-παραμέτρων, κ.λπ. Υπάρχει ανάγκη για αλλαγή παραδείγματος για την ανάπτυξη ειδικών μεθοδολογιών διασφάλισης για την αντιμετώπιση των διαδικασιών μάθησης.

- **Υπάρχουν δυσκολίες στη διατήρηση μιας ολοκληρωμένης περιγραφής της επιδιωκόμενης λειτουργίας της μάθησης.**

Όταν πρόκειται για διαδικασίες μάθησης, η συμπεριφορά περιέχεται εκ φύσεως στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του αλγορίθμου και εξαρτάται επίσης από την ίδια τη διαδικασία μάθησης. Μπορεί να γίνει πιο δύσκολο να διατηρηθεί μια σύνδεση με απαιτήσεις υψηλότερου επιπέδου και να διασφαλιστεί η πληρότητα και η ορθότητα του συνόλου δεδομένων. Επιπλέον, η ποιότητα του συνόλου δεδομένων έχει μεγάλη σημασία, καθώς τα ελλιπή ή εσφαλμένα δεδομένα θα μπορούσαν να επηρεάσουν τη συμπεριφορά του μοντέλου εκπαίδευσης.

- **Έλλειψη προβλεψιμότητας και επεξηγηματικότητας της συμπεριφοράς της εφαρμογής ML**

Οι εφαρμογές ML είναι από τη φύση τους πιθανοτικές. Ακόμη και αν ένα μοντέλο ML είναι ντετερμινιστικό από μαθηματική άποψη, για κάθε νέα είσοδο, η έξοδος θα εξαρτάται από τη συσχέτιση μεταξύ αυτής της εισόδου και του συνόλου δεδομένων που χρησιμοποιήθηκε για τη διαδικασία εκπαίδευσης. Αυτό μπορεί να οδηγήσει σε απρόβλεπτες εξόδους που μπορεί να είναι δύσκολο να εξηγηθούν. Αυτό συχνά συγχέεται με την έλλειψη ντετερμινισμού του αλγορίθμου, οπότε είναι σαφέστερο να μιλάμε για απρόβλεπτη εφαρμογή ML. Κατά συνέπεια, υπάρχει ανάγκη να αυξηθεί η ικανότητα να γίνονται πιο κατανοητές οι συνθήκες που οδήγησαν σε μια δεδομένη έξοδο.

- **Έλλειψη εγγύησης της ευρωστίας (robustness).**

Λόγω της στατιστικής φύσης των εφαρμογών ML, υπόκεινται σε μεταβλητότητα στην έξοδό τους για μικρές παραλλαγές στην είσοδό τους (που μπορεί να είναι ακόμη και ανεπαίσθητες από τον άνθρωπο). Υπάρχει ανάγκη διερεύνησης νέων μεθόδων για την επαλήθευση της ανθεκτικότητας των εφαρμογών ML/DL, καθώς και για την αξιολόγηση της πληρότητας της επαλήθευσης.

- **Έλλειψη τυποποιημένων μεθόδων για την αξιολόγηση των λειτουργικών επιδόσεων των εφαρμογών ML/DL**

Πρέπει να διερευνηθούν οι ακριβείς τιμές αναφοράς ή το ποσοστό σφάλματος μιας εφαρμογής ML/DL και στη συνέχεια να καθιερωθούν.

- **Ζήτημα προκατάληψης (bias) και διακύμανσης (variance) στις εφαρμογές ML**

Στο πλαίσιο της μηχανικής μάθησης , οι όροι "bias" και "variance" αναφέρονται σε δύο τύπους σφαλμάτων που μπορούν να επηρεάσουν την απόδοση ενός προγνωστικού μοντέλου:

Bias (Προκατάληψη): Η προκατάληψη αναφέρεται στο σφάλμα που προκύπτει από την προσέγγιση ενός πραγματικού προβλήματος με ένα απλοποιημένο μοντέλο. Αντιπροσωπεύει τη διαφορά μεταξύ της προβλεπόμενης έξοδου του μοντέλου και της πραγματικής εξόδου. Μια υψηλή προκατάληψη σημαίνει ότι το μοντέλο είναι υπερβολικά απλό και αποτυγχάνει να αιχμαλωτίσει τα υποκείμενα πρότυπα στα δεδομένα, οδηγώντας σε υποπροσαρμογή. Τα μοντέλα με υψηλή προκατάληψη τείνουν να έχουν χαμηλή ακρίβεια τόσο στα δεδομένα εκπαίδευσης όσο και στα δεδομένα ελέγχου.

Variance (Διακύμανση): Η διακύμανση μετρά την ευαισθησία των προβλέψεων του μοντέλου σε αλλαγές στα σύνολα δεδομένων εκπαίδευσης. Αντιπροσωπεύει το πόσο θα μεταβάλλονταν οι προβλέψεις του μοντέλου αν εκπαιδευόταν σε διαφορετικά υποσύνολα δεδομένων εκπαίδευσης. Η υψηλή διακύμανση υποδηλώνει ότι το μοντέλο είναι υπερβολικά ευαίσθητο στο “θόρυβο” των δεδομένων εκπαίδευσης και αιχμαλωτίζει τις τυχαίες διακυμάνσεις αντί των υποκείμενων προτύπων, οδηγώντας σε υπερπροσαρμογή. Τα μοντέλα με υψηλή διακύμανση επιτυγχάνουν καλή απόδοση στα δεδομένα εκπαίδευσης, αλλά κακή στα δεδομένα που δεν έχουν χρησιμοποιηθεί για την εκπαίδευσή τους.

Η εύρεση της κατάλληλης ισορροπίας μεταξύ προκατάληψης και διακύμανσης είναι κρίσιμη για την ανάπτυξη ενός αξιόπιστου προγνωστικού μοντέλου. Μία από τις πιο δύσκολες πτυχές κατά τη συλλογή, προετοιμασία ή χρήση δεδομένων είναι η ικανότητα εντοπισμού, ανίχνευσης και, τέλος, επαρκούς μετριασμού οποιασδήποτε προκατάληψης ή διακύμανσης που θα μπορούσε να έχει εισαχθεί σε οποιαδήποτε κατά τη διάρκεια της διαχείρισης των δεδομένων και/ή των διαδικασιών κατάρτισης.

- **Πολυπλοκότητα αρχιτεκτονικών και αλγορίθμων**

Τα διαδραστικά νευρωνικά δίκτυα (CNNs) θα χρησιμοποιηθούν ευρέως στον τομέα της όρασης υπολογιστών. Ακόμα κι αν είναι πιο σύνθετα από αρχιτεκτονική άποψη, εφόσον περιοριστούν σωστά, αναμένεται να είναι διαχειρίσιμα σαν τα κλασσικά τεχνητά νευρωνικά δίκτυα (ANNs).

Από την άλλη πλευρά, τα αναδρομικά νευρωνικά δίκτυα (RNNs) εγείρουν πιο σύνθετα ζητήματα (π.χ. χρήση βρόχων ανάδρασης) και μπορεί να χρειαστούν ειδική καθοδήγηση και όρια.

Τα δίκτυα γενετικής αντιπαράθεσης (GANs) θα μπορούσαν φαινομενικά να χρησιμοποιηθούν για να βελτιώσουν την εκπαίδευση ή να συμπληρώσουν το σύνολο επαλήθευσης για την μηχανική μάθηση/βαθιά μάθηση. Ωστόσο, είναι αποτέλεσμα αρκετά πρόσφατης έρευνας και εγείρουν πολλά ερωτήματα σχετικά με την ερμηνευσιμότητα της εξόδού τους.

➢ **Διαδικασίες προσαρμοστικής μάθησης**

Η μάθηση σε πραγματικό χρόνο στις επιχειρήσεις είναι μια παράμετρος που θα εισάγει μεγάλη πολυπλοκότητα στην ικανότητα παροχής διασφάλισης στο συνεχώς μεταβαλλόμενο λογισμικό. Αυτό είναι ασύμβατο με την τρέχουσα πιστοποίηση διαδικασίες και θα απαιτήσει μεγάλες αλλαγές στους ισχύοντες κανονισμούς και οδηγίες. [128]

Όσον αφορά τον τομέα της κυβερνοασφάλειας για την ΤΝ, περιλαμβάνει τρεις κύριους φορείς:

- ❖ Το σύστημα/οργανισμός που έχει ευπάθειες που οδηγούν στον κίνδυνο εκμετάλλευσης και προκαλούν επιχειρησιακές επιπτώσεις
- ❖ Την απειλή (π.χ. ένα κακόβουλο λογισμικό) η οποία θα μπορούσε να προκαλέσει ζημία σε ένα σύστημα ή έναν οργανισμό εκμεταλλευόμενη τις ευπάθειές του
- ❖ Τον έλεγχο ασφάλειας/το αντίμετρο, το οποίο μετριάζει έναν ή περισσότερους κινδύνους ασφάλειας.

Η ανάδυση της χρήσης της ΤΝ θα επηρεάσει και τους τρεις παράγοντες. Με την τεχνητή νοημοσύνη, ένα σύστημα μπορεί να βελτιώσει την αποτελεσματικότητά του, αλλά μπορεί επίσης να περιλαμβάνει νέα είδη τρωτών σημείων για κυβερνοεπιθέσεις. Αυτοί οι νέοι τύποι ευπαθειών πρέπει να γίνουν καλύτερα κατανοητοί (π.χ. δηλητηρίαση δεδομένων) και πρέπει να καθοριστούν ειδικοί έλεγχοι ασφαλείας (τεχνικοί ή οργανωτικοί) για αυτές.

Από την πλευρά των απειλών, σήμερα, τα κακόβουλα προγράμματα μεταλλάσσονται ήδη (δηλαδή προσαρμόζουν τη συμπεριφορά τους ανάλογα με το περιβάλλον εκτέλεσης). Η τεχνητή νοημοσύνη (ΤΝ) μπορεί να χρησιμοποιηθεί σε κυβερνοεπιθέσεις με διάφορους τρόπους λόγω των εξελιγμένων δυνατοτήτων της. Η ΤΝ μπορεί να χρησιμοποιηθεί:

- Για την ανάλυση μεγάλου όγκου δεδομένων για την εντοπισμό ευάλωτων σημείων σε φυσικά συστήματα (όπως ενεργειακά δίκτυα ή μεταφορικά δίκτυα) και για τη διεξαγωγή πιο αποτελεσματικών επιθέσεων, όπως αντιμετώπισης του ηλεκτρικού δικτύου ή καταστροφής υποδομών.

[128] EASA Artificial Intelligence Roadmap- A human-centric approach to AI in aviation,07 Feb 2020 ό.π.

- Για τη δημιουργία κυβερνοεπιθέσεων όπως malware με εξελιγμένες τεχνικές κρυπτογράφησης και αυτοματοποιημένης επιλογής στόχων, έξυπνη ανίχνευση ευπαθειών σε δίκτυα ή εφαρμογές, και ακόμα και τη δημιουργία deepfakes για προωθητικούς ή κατασκευασμένους σκοπούς.
- Για την ανάλυση μεγάλου όγκου δεδομένων από κοινωνικά δίκτυα, email, και άλλες πηγές για τη δημιουργία στοχοθετημένων επιθέσεων ή κοινωνικών επιθέσεων.

Οι προσεκτικά σχεδιασμένες επιθέσεις που χρησιμοποιούν την ΤΝ μπορούν να είναι δύσκολο να ανιχνευθούν και να αντιμετωπιστούν, καθιστώντας τις πολύ αποτελεσματικές σε πολλές περιπτώσεις. Ωστόσο, η επίδρασή τους μπορεί να είναι ιδιαίτερα επιζήμια και να προκαλέσει σημαντικές ζημιές σε κρίσιμες υποδομές ή οργανισμούς. Επιπλέον, οι ερευνητές έχουν αποδείξει τη δυνατότητα δημιουργίας μιας νέας κατηγορίας κακόβουλου λογισμικού με τεχνητή νοημοσύνη (π.χ. DeepLocker).[129]

Το "DeepLocker" είναι ένα προηγμένο είδος κακόβουλου λογισμικού που χρησιμοποιεί τεχνητή νοημοσύνη (AI) για να εκτελέσει επιθέσεις με στόχο συγκεκριμένους χρήστες ή συστήματα. Το DeepLocker αναπτύχθηκε από ερευνητές της IBM και παρουσιάστηκε στο συνέδριο Black Hat το 2018. Η ιδιαιτερότητα του DeepLocker είναι ότι χρησιμοποιεί τεχνητή νοημοσύνη για να κρύψει το κακόβουλο περιεχόμενο του και να το καθιστά δραστικά δυσεύρετο από τα συστήματα ασφαλείας. Για παράδειγμα, μπορεί να ενσωματώσει το κακόβουλο πρόγραμμά του σε ένα απλό παιχνίδι ή ένα βίντεο που δεν παρουσιάζει εμφανώς κάποια κακόβουλη ενέργεια κατά τη λειτουργία του. Όταν το DeepLocker ενεργοποιηθεί, αναζητά τον στόχο του μέσω τεχνικών όπως η αναγνώριση προσώπων ή η αναγνώριση φωνής και στη συνέχεια εκτελεί την επίθεσή του. Το DeepLocker αντιπροσωπεύει μια πρωτοποριακή μορφή επιθέσεων που χρησιμοποιεί την τεχνητή νοημοσύνη για να κρύψει και να παρακολουθεί το κακόβουλο περιεχόμενο και συνήθως αποσκοπεί σε στοχευμένη επίθεση.[130]

Η χρήση της ΤΝ για κυβερνοεπιθέσεις θα βελτιώσει σίγουρα την αποτελεσματικότητα των απειλών, αναπτύσσοντας την ικανότητα παράκαμψης των συμβατικών συστημάτων ανίχνευσης βάσει κανόνων και καθιστώντας τελικά τις κυβερνοεπιθέσεις προσαρμοστικές και αυτόνομες. Οι επιθέσεις με τεχνητή νοημοσύνη μπορεί να αναπτυχθούν σύντομα και να είναι σημαντικό να προσδιοριστούν κατάλληλα αντίμετρα.Συνεπώς, είναι ζωτικής σημασίας να αντιμετωπιστούν οι πιθανοί κίνδυνοι της τεχνητής νοημοσύνης στον αεροπορικό τομέα με στρατηγικές που θα συνδυάζουν την καινοτομία και την ασφάλεια. Απαιτείται η ανάπτυξη κατάλληλων πρωτοκόλλων ασφαλείας και προστασίας δεδομένων, η εκπαίδευση του προσωπικού για τη σωστή χρήση και επίβλεψη των συστημάτων τεχνητής νοημοσύνης, καθώς και η συνεχής επικοινωνία και ανταλλαγή γνώσεων με τον ευρύτερο κοινό και τους ειδικούς του τομέα,

[129] EASA Artificial Intelligence Roadmap- A human-centric approach to AI in aviation,07 Feb 2020 ό.π.
[130] Marc Ph. Stoecklin,Jiyong Jang,Dhilung Kirat (2018): DeepLocker: How AI can power a stealthy new breed of Malware https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

προκειμένου να διασφαλιστεί η ομαλή και ασφαλής ενσωμάτωση της τεχνολογίας στην αεροπορική βιομηχανία.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

Διανύουμε μια περίοδο καθοριστικών αλλαγών σε κάθε πτυχή της ανθρώπινης δραστηριότητας, σαν επακόλουθο της ανάδυσης τεχνολογιών με εντελώς διαφορετικά χαρακτηριστικά, όπως η τεχνητή νοημοσύνη. Στη ψηφιοποιημένη νέα εποχή, η πληροφορία και τα δεδομένα, βρίσκονται στο επίκεντρο της τεχνολογικής εξέλιξης, με επιτακτική την ανάγκη της διασφάλισής τους. Η χρήση Προτύπων και Πλαισίων για την υποστήριξη των πολιτικών ασφαλείας πληροφοριών ενός οργανισμού, όπως εκφράζεται μέσα από ένα ολοκληρωμένο σύστημα διαχείρισης, αποτελεί την αποτελεσματικότερη λύση. Μέσω των βημάτων των Προτύπων, θέτονται με σαφήνεια οι απαιτήσεις και ελέγχεται η συμμόρφωση, ενώ παράλληλα εμπεδώνονται οι βέλτιστες πρακτικές και διαμορφώνεται μια κουλτούρα ασφάλειας στον οργανισμό.

Στις νέες εκδόσεις των Προτύπων, βλέπουμε την ασφάλεια πληροφοριών να αποκτά αυξημένη βαρύτητα και να εντάσσεται στο συνολικό οργανωσιακό πλαίσιο του οργανισμού, ξεφεύγοντας από το στενό πλαίσιο της τεχνικής διαχείρισης. Η ασφάλεια πληροφοριών και πληροφοριακών συστημάτων γίνεται ένα ευρύτερο ζήτημα, που απασχολεί όλες τις δομές του οργανισμού, οι οποίες επικοινωνούν μεταξύ τους και διαβουλεύονται, ώστε να υπάρχει συνεχής παρακολούθηση των κινδύνων και επικαιροποίηση του συστήματος ασφαλείας. Από την άλλη πλευρά, η ασφάλεια πληροφοριών ενός οργανισμού, είναι μια υπόθεση που αφορά τις σχέσεις του με άλλους οργανισμούς. Η ανάπτυξη της διαλειτουργικότητας, εξασφαλίζει την ύπαρξη ενός κοινού υπόβαθρου κατανόησης για τη συμμόρφωση στις απαιτήσεις προτύπων και κανονιστικών πλαισίων, με στόχο την διευκόλυνση της συνεργασίας των οργανισμών σε παγκόσμιο επίπεδο.

Η διεργασία της αποτίμησης επικινδυνότητας, είναι αυτή στην οποία εστιάζουν τα πρότυπα και οι μεθοδολογίες, προκειμένου να αξιοποιηθούν τα αποτελέσματά της στη λήψη των κατάλληλων μέτρων, που θα προστατεύσουν τα πληροφοριακά συστήματα. Στον τομέα αυτό, παρατηρούμε τα τελευταία χρόνια μια αλλαγή παραδείγματος, που υπαγορεύεται από την πραγματικότητα του ρευστού και μεταβαλλόμενου τοπίου των απειλών. Η έννοια της προστασίας υποχωρεί μπροστά στην έννοια της ανθεκτικότητας, που σαν στόχο θέτει τη διασφάλιση της συνέχειας της λειτουργίας των συστημάτων, μετά την εκδήλωση περιστατικών ασφαλείας και παραβιάσεων.

Η σημασία της ανθεκτικότητας φαίνεται στη περίπτωση των οργανισμών που παρέχουν κρίσιμες υπηρεσίες και αγαθά ζωτικής σημασίας, καθώς η αδιατάρακτη παροχή τους, αποτελεί κοινωνικό αίτημα, αλλά και παράγοντα οικονομικής σταθερότητας. Για τον λόγο αυτό, η προστασία των

κρίσιμων υποδομών είναι στο κέντρο του ενδιαφέροντος των φορέων κρατικής εξουσίας, που επεμβαίνουν με ρυθμίσεις είτε ενδοτικού, είτε κανονιστικού χαρακτήρα. Στην Ευρωπαϊκή Ένωση, η ασάφεια των κριτηρίων καθορισμού των κρίσιμων υποδομών που χαρακτήριζε το ευρωπαϊκό θεσμικό πλαίσιο, φαίνεται να λειτούργησε ανασταλτικά για την προστασία τους. Γεωπολιτικές αναταραχές και επιθέσεις σε κρίσιμες υποδομές στον ευρωπαϊκό χώρο, έστρεψαν την Ευρωπαϊκή Ένωση στην υιοθέτηση μιας νέας πολιτικής, που εστιάζει στην ανθεκτικότητα των οργανισμών που διαχειρίζονται τις κρίσιμες υποδομές, η οποία πρόκειται να εφαρμοστεί μέσα στο έτος που διανύουμε. Σημαντικός παράγοντας για την αντιμετώπιση των προκλήσεων στο πεδίο της ανθεκτικότητας, είναι η ολιστική θεώρηση των κινδύνων που απειλούν τις κρίσιμες υποδομές, οι οποίες λειτουργούν πλέον σαν ένα σύστημα ψηφιοποιημένων συστημάτων με πολύπλοκες αλληλεξαρτήσεις. Αντίστοιχα, η μεθοδολογική προσέγγιση της διαχείρισης επικινδυνότητας στις κρίσιμες υποδομές, για να είναι αποτελεσματική, πρέπει να ενσωματώνει τις ιδιαιτερότητες αυτές.

Ο αεροπορικός τομέας, είναι η κρίσιμη υποδομή μεταφορών, που ανταποκρίνεται στους γρήγορους ρυθμούς της σύγχρονης ζωής. Το διακύβευμα για τους κρατικούς φορείς, τους φορείς προστασίας της και τους παρόχους, είναι η διαφύλαξη της αξιοπιστίας της απέναντι στο κοινωνικό σύνολο, καθώς οι πυκνές αλληλεξαρτήσεις με άλλους τομείς κρίσιμων υποδομών, μεγιστοποιούν τις συνέπειες μιας ενδεχόμενης διατάραξης της λειτουργίας της. Σαν πολύπλοκο σύστημα συστημάτων, με παγκόσμια διασύνδεση, η πολιτική αεροπορία χρησιμοποιεί όλες τις τεχνολογίες αιχμής για να αναπτυχθεί, με επακόλουθο την έκθεσή της στο δυναμικά εξελισσόμενο και συχνά απρόβλεπτο τοπίο των κυβερνοαπειλών. Φυσικές απειλές και κυβερνοαπειλές συμπλέκονται λόγω της ψηφιοποίησης των συστημάτων και των αλληλεξαρτήσεων μεταξύ τους. Στο επίκεντρο βρίσκεται η θωράκιση του Συστήματος Διαχείρισης Εναέριας Κυκλοφορίας (ATM), στη προστασία του οποίου έχουν εστιάσει οι οργανισμοί προστασίας της διεθνούς αεροναυτιλίας.

Η εφαρμογή Πλαισίων για την κυβερνοασφάλεια από τους παρόχους υπηρεσιών και η συμμόρφωση με διεθνή Πρότυπα διοίκησης πληροφοριών, αποτελούν τις πρακτικές που θα λειτουργήσουν σαν δίχτυ προστασίας στις αερομεταφορές σε παγκόσμιο επίπεδο. Ωστόσο η συμμόρφωση στα Πρότυπα, χωρίς μηχανισμούς διαμοιρασμού πληροφοριών για τα περιστατικά κυβερνοασφάλειας και συνεργασίας μεταξύ των μελών της αεροπορικής κοινότητας, μπορεί να δημιουργήσει επικίνδυνο εφησυχασμό. Για την ενίσχυση της ανθεκτικότητας στην αεροναυτιλία, απαιτείται η χάραξη μιας ολιστικής στρατηγικής, που θα στηρίζεται στη συνεχή συλλογική προσπάθεια για την αναθεώρηση των Προτύπων, σύμφωνα με τα νέα δεδομένα που προκύπτουν, την εκπαίδευση σε σταθερή βάση του προσωπικού των παρόχων και κυρίως την ευαισθητοποίηση όλων των εμπλεκομένων για την διατήρηση υψηλού επιπέδου κυβερνοασφάλειας στην αεροναυτιλία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α) Βιβλία

Κάτσικας Σωκράτης "Διαχείριση της ασφάλειας πληροφοριών" εκδ. Πεδίο 2014

Κάτσικας Σ., Γκρίτζαλης Σ., Λαμπρινουδάκης Κ (επιμ.) "Ασφάλεια πληροφοριών και συστημάτων στον Κυβερνοχώρο" , εκδ. Νέες Τεχνολογίες 2021

Sutton David " Information risk management, A practitioner's guide" BCS Learning and Development Ltd 2021

Β) ΄Άρθρα

Aboti, Chiragkumar. (2019). Survey on IoT: Challenges and cyber risks in commercial aviation. 6. 970. 10.1729/Journal.22604
https://www.researchgate.net/publication/337485708_Survey_on_IoT_Challenges_and_cyber_risks_in_commercial_aviation

Argyroudis S. et al. "Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets" 2020- ScienceDirect
https://doi.org/10.1016/j.scitotenv.2020.136854

De Zan, Tommaso & Camillo, Federica & d'Amore, Fabrizio. (2015). The Defence of Civilian Air Traffic Systems from Cyber Threats
https://www.researchgate.net/publication/324759427_The_Defence_of_Civilian_Air_Traffic_Systems_from_Cyber_Threats

Giannopoulos G, Filippini R, Schimmer M. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. EUR 25286 EN. Luxembourg Publications Office of the European Union; 2012, JRC70046
https://publications.jrc.ec.europa.eu/repository/handle/JRC70046

Giannopoulos G. et al. " Risk Assessment Methodology for Critical Infrastructure Protection" 2013 European Commission Joint Research Centre Risk Assessment Methodology for Critical Infrastructure JRC Publications Repository https://publications.jrc.ec.europa.eu › JRC78292

Γκρίτζαλης Δ,Μήτρου Ν.,Σκουλαρίδου Β. (Επιμ.) Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης: Στρατηγικός Σχεδιασμός, eGov Forum-CICIP-D1-v2.3/29.09.2008
https://www.infosec.aueb.gr/CIS_Reviews/reviews/1580eGovFor_CICIP.pdf

Γκρίτζαλης Δ, Κοτζανικολάου Π. κ.α. "Ολιστική Προστασία Κρίσιμων Υποδομών" Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών, Ιούνιος 2016
https://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo3_version_020616_2.pdf

Καρατράντος Τ. "Από τις κρίσιμες υποδομές στις κρίσιμες οντότητες: μία σύνθετη διαδικασία ασφάλειας" ΕΛΙΑΜΕΠ Μάρτιος 2023
www.eliamep.gr/wp-content/uploads/2023/03/Policy-brief-177-Karatrantos-EL.pdf

Koroniotis N. et al. "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports" January 2020, IEEE
https://www.researchgate.net/publication/347832747_A_Holistic_Review_of_Cybersecurity_and_Reliability_Perspectives_in_Smart_Airports

Kotzanikolaou P., Theoharidou M..& Gritzalis D. "Assessing n-order dependencies between critical infrastructures" Int. J. of Critical Infrastructures, 2013
https://www.researchgate.net/publication/264815932_Assessing_n-order_dependencies_between_critical_infrastructures/link/5407089e0cf2bba34c1e8415/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Little Arthur D. Airports Digital Transformation(2018)
https://amadeus.com/documents/en/airports/research-report/airports-digital-transformation.pdf

Lykou, G. "Developing Resilience and Cyber-Physical Protection Capabilities in Critical Aviation Infrastructures" Εθνικό Αρχείο Διδακτορικών Διατριβών,
https://www.didaktorika.gr/eadd/handle/10442/49706

Lykou, G., Iakovakis, G., Gritzalis, D. (2019). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer, Cham. (PDF) Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies (researchgate.net)

Murray Glenn, Johnstone Michael N. , Valli Craig (2017). The convergence of IT and OT in critical Infrastructures: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1217&context=ism

Petersen L., D. Lange , M. Theocharidou "Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators"2020
https://doi.org/10.1016/j.ress.2020.106872

Petit Frederic, “Analysis of Critical Infrastructure Dependencies and Interdependencies” Argonne June 2015
https://www.researchgate.net/publication/299525808_Analysis_of_Critical_Infrastructure_Dependencies_and_Interdependencies

Petrakos, N., Kotzanikolaou, P. (2019). Methodologies and Strategies for Critical Infrastructure Protection, pp 17-33 In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer https://doi.org/10.1007/978-3-030-00024-0_2

Popa Dragos , Popa Andrei, Codescu Mirela-Maria(2016). Smart Airport-Structure and Elements: https://www.agir.ro/buletine/2812.pdf

Pursiainen C.& Kytömaa E. (2023) From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and Resilient Infrastructure, 8:sup1, 85-101 https://doi.org/10.1080/23789689.2022.2128562

Rehak David et al. “Critical Entities Resilience Failure Indication” Nov.2023
https://www.sciencedirect.com/science/article/pii/S0925753523003132

Rehak David et al. “Complex Approach to Assessing Resilience of Critical Infrastructure Elements”,March 2019,International Journal of Critical Infrastructure Protection 25
https://www.researchgate.net/publication/332084463_Complex_Approach_to_Assessing_Resilience_of_Critical_Infrastructure_Elements

Stergiopoulos G., Vasilellis R., Lykou G, Kotzanikolaou P., Gritzalis D. “Classification and Comparison of Critical Infrastructure Protection Tools” 10th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2016, Arlington, VA, USA pp.239-255,
https://inria.hal.science/hal-01614869

Stoecklin Marc Ph. ,Jiyong Jang,Dhilung Kirat (2018): DeepLocker: How AI can power a stealthy new breed of Malware
https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

Theoharidou M., Kotzanikolaou P., Gritzalis D., A multi-layer Criticality Assessment methodology based on interdependencies, 2010
https://www.sciencedirect.com/science/article/abs/pii/S0167404810000210

Theocharidou, M., Galbusera, L., & Giannopoulos, G. (2018). Resilience of critical infrastructure systems: Policy, research projects and tools. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems. Lausanne, CH: EPFL International Risk Governance Center.
*Theocharidou-et-al-for-IRGC-Resilience-Guide-Vol-2-2018.pdf

Theocharidou M, Giannopoulos G. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. EUR 27332. Luxembourg (Luxembourg): Publications Office of the European Union; 2015. JRC96623 https://dx.doi.org/10.2788/621843

Witte G., Connecting COBIT 2019 to the NIST Cybersecurity Framework Connecting COBIT 2019 to the NIST Cybersecurity Framework (isaca.org)

White Richard "Risk Analysis for Critical Infrastructure Protection"Methodologies and Strategies for Critical Infrastructure Protection, pp 35-54 In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer https://doi.org/10.1007/978-3-030-00024-0_2

Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information 2022, 13, 146, Academic Editor: Sokratis Katsikas https://doi.org/10.3390/info13030146

Γ) Ιστοσελίδες

- ***Airports Council International (ACI)***

  ACI Airport Excellence in Security https://aci.aero/wp-content/uploads

- ***Αρχή Πολιτικής Αεροπορίας (ΑΠΑ)***

Ιστοσελίδα ΑΠΑ https://hcaa.gov.gr/el/aeroporiki-asfaleia

- ***BBC***

BBC EasyJet admits data of nine million hacked 19-5-2020
https://www.bbc.com/news/technology-52722626

- ***Cathay Pacific Airways***

Cathay Pacific Airways, 2018, Cathay Pacific announces data security event affecting passenger data
https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data

- ***Cisco***

Cisco, 2009. Smart Airports: Transforming Passenger Experience To Thrive in the New Economy

https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf

- ***Civil Air Navigation Services Organization (CANSO)***

CANSO CYBERSECURITY RISK ASSESSMENT GUIDE 2023 Edition
https://canso.fra1.digitaloceanspaces.com/uploads/2023/05/CANSO-Safety_Cybersecurity-Risk-Assessment-Guide-2023.pdf

CANSO Protecting ATM systems https://canso.org/protecting-atm-systems/
/2021/08/APEX-in-Security.pdf

- ***Cybersecurity Agency of Singapore (CSA)***

CSA Singapore Guide to conducting cybersecurity risk assessment for critical infrastructure, Feb.2021
https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_ttps://data.europa.eu/doi/10.2788/621843

- ***Cybersecurity & Infrastructure Security Agency (CISA)***

Critical Infrastructure Sectors
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CISA Presidential Policy Directive (PPD)21: Critical Infrastructure Security and Resilience
https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

CISA National Critical Functions Set, April 2019
https://www.cisa.gov/sites/default/files/publications/national-critical-functions-set-508.pdf

CISA SECURING INDUSTRIAL CONTROL SYSTEMS: A UNIFIED INITIATIVE FY 2019—2023
https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

CISA NIPP 2013 Partnering for Critical Infrastructure Security and Resilience
https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

CISA Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects
https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Incorporating-Resilience-into-CI-Projects-508.pdf

- ***European Union***

Commission of the European Communities (2005), “Green Paper on a European Programme for Critical Infrastructure Protection” Annex 2
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=pl

Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, της 6 Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (Οδηγία NIS) 32016L1148 - EN - EUR-Lex

ΕΕ -ΚΑΝΟΝΙΣΜΟΣ 2019/1583 της 25 Σεπτ 2019 για την τροποποίηση του εκτελεστικού κανονισμού 2015/1998 σχετικά με τον καθορισμό λεπτομερών μέτρων εφαρμογής των κοινών βασικών προτύπων ασφάλειας των αερομεταφορών από έκνομες ενέργειες, όσον αφορά τα μέτρα ασφάλειας στον κυβερνοχώρο
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R1583

CERT-EU(2019): Airports & Operational Technology: 4 Attack-Scenarios:
https://cow-prod-www-v3.azurewebsites.net/publications/threat-intelligence/threat-memo-190404-2/pdf

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/1645 της 14 Ιουλίου 2022 και ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2023/203 της 27 Οκτ 2022 για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις απαιτήσεις για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj
https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj

European Commission, Sesar Joint Undertaking “ AI in air traffic management- Bringing intelligent and trustworthy automation to Europe’s aviation sector- A thematic collection of innovative EU-funded research result, October 2022
https://www.sesarju.eu/sites/default/files/documents/AI%20in%20air%20traffic%20management%20brochure.pdf

European Commission, Press Release 18-10-22 “Critical Infrastructure : Commission accelerates work to build up European resilience”
https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 14 Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) 32022L2555 - EN - EUR-Lex

Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 14 Δεκεμβρίου 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (οδηγία CER) 32022L2557 - EN - EUR-Lex

Ευρωπαϊκή Επιτροπή, Δνση MOVE: Εργαλειοθήκη κυβερνοασφάλειας στον τομέα των μεταφορών 2021

https://transport.ec.europa.eu/document/download/7e65c691-9215-480c-9324-60727ec05d25_el?filename=cybersecurity-toolkit_el.pdf

- ***European Union Agency for Cybersecurity (ENISA)***

ENISA Methodologies for the identification of Critical Information Infrastructure assets and services, 2015
https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

ENISA Threat Landscape of Internet Infrastructure [Report/Study], 2015
https://www.enisa.europa.eu/publications

ENISA, Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, 2015
https://www.enisa.europa.eu/publications/maturity-levels/iitl

ENISA, Communication network dependencies for ICS/SCADA Systems, 2016
www.enisa.europa.eu/publications/ics-scada-dependencies

ENISA Securing Smart Airports [Report/Study], 2016
https://www.enisa.europa.eu/publications/securing-smart-airportshttps://

ENISA Guidelines on assessing DSP and OES compliance to the NISD security requirements Information Security Audit and Self – Assessment/ Management Frameworks, Nov.2018
https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

ENISA Compendium of Risk Management Frameworks with potential Interoperability, 2022
https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

ENISA Interoperable EU Risk Management Framework, 2022
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

ENISA Interoperable EU Risk Management Toolbox, 2023
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox

ENISA NIS Investments Report 2023, Nov.16,2023
https://www.enisa.europa.eu/publications/nis-investments-2023

ENISA Threat Landscape, 2023
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA Transport Threat Landscape,2023
https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

- ***European Union Aviation Safety Agency (EASA)***

EASA Artificial Intelligence Roadmap- A human-centric approach to AI in aviation,07 Feb 2020 https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-10

EASA Opinion 03/2021 Management of information security risks, June 2021 https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

EASA Information Security (Part-IS) https://www.easa.europa.eu/en/the-agency/faqs/information-security-part#category-delegation-of-tasks

EASA ESCP (European Strategic Cooperation Platform) European Strategic Coordination Platform Strategy for Cybersecurity in Aviation First Issue – September 10th , 2019 https://www.easa.europa.eu/en/downloads/103075/en

Cybersecyrity EASA https://www.easa.europa.eu/en/domains/cyber-security

- ***Eurocontrol***

EUROCONTROL EUROPEAN AVIATION ARTIFICIAL INTELLIGENCE HIGH LEVEL GROUP The FLY AI Report Demystifying and Accelerating AI in Aviation/ATM 5th March 2020 www.eurocontrol.int/sites/default/files/2020-03/eurocontrol-fly-ai-report-032020.pdf

Eurocontrol “Air Traffic Management A Cybersecurity Challenge” 20 Dec2021 https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

Eurocontrol : ATM: navigating the challenging cybersecurity landscape, March 2023 https://www.eurocontrol.int/article/atm-navigating-challenging-cybersecurity-landscape

Eurocontrol : Aviation as a critical infrastructure: challenges and opportunities for a more resilient sector, March 2023 https://www.eurocontrol.int/article/aviation-critical-infrastructure-challenges-and-opportunities-more-resilient-sector

Eurocontrol Cybersecurity https://www.eurocontrol.int/cybersecurity

- ***Federal Aviation Administration (FAA)***

FAA Cybersecurity Risk (CyRM Modelling) https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cas/cytf/cytf.pdf

- ***FORTINET***

Fortinet(2021): State of Operational Technology Security in Transportation and logistics: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-ot-transportation-and-logistics.pdf

Fortinet(2021): State of Operational Technology Security in Transportation and logistics: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-ot-transportation-and-logistics.pdf

- ***International Air Transport Association (IATA)***

The Security Management System (SemS) manual
https://www.iata.org/en/publications/store/security-management-system-manual/

IATA - Categories of Aviation Security Occurrences SeMS Edition 5 (iata.or g)

IATA, 2023:IATA - What You Need to Know About Aviation Security

IATA, Aviation Cyber Security Roundtable April 11-12, 2019 Singapore,
www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/sin_roundtable_readout.pdf

- ***International Civil Aviation Organization (ICAO)***

ICAO Strategic Objectives
https://www.icao.int/about-icao/Council/Pages/Strategic-Objectives.aspx

ICAO Aviation Cybersecurity Strategy , October 2019
www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf

ICAO Cybersecurity Policy Guidance, Published by authority of the Secretary General January 2022
www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf

ICAO (2011) Manual on Threat Assesment and Risk Management Methodology
https://www.icao.int/SAM/Documents/2012/ICAOLACACAVSECRG2/Manual%20on%20Threat%20Assessment%20and%20Risk%20Management%20Methology%20NoLogos.pdf

- ***International Organisation for Standardization (ISO)***

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection-Information security management systems,Requirements https://www.iso.org/standard/27001

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls https://www.iso.org/standard/75652.html

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks https://www.iso.org/standard/75652.html

- ***ISACA***

ISACA Implementation Guide ISO/IEC 27001:2022 Practical guide for the implementation of an information security management system (ISMS) according to ISO/IEC 27001:2022 ISACA Germany

https://isaca.de/publikationen/publikationen/leitfaeden/implementierungsleitfaden-iso-iec-27001-2022.html

ISACA COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

ISACA COBIT Focus Area: Information Security Using COBIT 2019, ISACA 2020 https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ku2gEAC

ISACA COBIT 2019 and COBIT 5 Comparison, Harisaiprasad K.,27 April 2020 www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

ISACA The Risk IT Framework 2nd edition 2020 https://www.isaca.org/resources/it-risk

- ***National Institute of Standards and Technology (NIST)***

NIST SP 800-39 "Managing Information Security Risk: Organization, Mission, and Information System View"Date Published: March 2011 https://csrc.nist.gov/pubs/sp/800/39/final

NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018 https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, September 2020 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security, September 2023 /https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

The NIST Cybersecurity Framework (CSF) 2.0 National Institute of Standards and Technology, Feb 26, 2024 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST Releases Version 2.0 of Landmark Cybersecurity Framework, Feb 26, 2024 https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

- ***SOCRadar***

SOCRadar Top Cyber-Threats Faced by the Aviation Industry 2022 https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

- ***The Guardian***

The Guardian, 2015: Germanwings crash calls attention to Airbus safety historyhttps://www.theguardian.com/world/2015/mar/25/germanwings-plane-crash-attention-airbus-safety

- ***UK Department of Transport***

UK Department of Transport: Aviation Cyber Security Strategy,2018 Aviation Cyber Security Strategy (publishing.service.gov.uk)