ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

ΠΜΣ «Ψηφιακός Πολιτισμός, Έξυπνες Πόλεις, IoT και Προηγμένες Ψηφιακές Τεχνολογίες»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής:	**Ασφάλεια και Ιδιωτικότητα σε Περιβάλλοντα Ναυτιλίας** **Security and Privacy in Maritime Environments**
Ονοματεπώνυμο φοιτητή:	ΣΤΕΦΑΝΟΣ ΤΣΟΥΝΤΑΣ
Πατρώνυμο:	ΚΩΝΣΤΑΝΤΙΝΟΣ
Αριθμός Μητρώου:	ΨΠΟΛ19064
Επιβλέπων:	**ΧΡΗΣΤΟΣ ΔΟΥΛΙΓΕΡΗΣ, ΚΑΘΗΓΗΤΗΣ**

Ημερομηνία Παράδοσης **Ιούλιος 2022**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Ιωάννης Αναγνωστόπουλος Καθηγητής	Κοτσιφάκος Δημήτριος Διδάσκων

Στους γονείς μου

Ευχαριστίες

Για τη διεκπεραίωση της παρούσας Μεταπτυχιακής Διατριβής, θα ήθελα να ευχαριστήσω τον επιβλέποντα, καθηγητή Χρήστο Δουληγέρη, για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωσή της.

Περίληψη

Το αντικείμενο της παρούσας μεταπτυχιακής διατριβής είναι η παρουσίαση και ανάλυση της ιδιωτικότητας στη Ναυτιλία, κυρίως υπό το πρίσμα της πληροφορικής και της τεχνολογίας. Εξετάζονται σημεία όπως ποιες είναι οι ευαίσθητες πληροφορίες που διατηρούνται σε μια ναυτιλιακή εταιρεία, πώς αυτές συλλέγονται και πώς προστατεύονται με τεχνικά μέσα. Παρουσιάζονται επίσης οι σχετικές νομοθεσίες που προστατεύουν την ιδιωτικότητα του πληρώματος, καθώς και οι ναυτιλιακοί κανονισμοί που διέπουν την υποχρέωση τήρησης και προστασίας πληροφοριών, χάριν της εύρυθμης λειτουργίας. Επιπρόσθετα, παρατίθενται παραδείγματα περιστατικών διαρροής πληροφοριών και οικονομικών επιπτώσεων απώλειας δεδομένων. Η παρούσα εργασία υπάρχει και ως ιστοσελίδα στον σύνδεσμο https://stmaritimesecurity.000webhostapp. com/index.html.

Abstract

This masters thesis presents and analyzes privacy issues in the Maritime business, mostly from under the information technology’s point of view. The main points being examined are which types of information maintained within a marine company are sensitive, how this info is collected and how it is technically protected. Furthermore, relevant privacy legislation is presented, along with marine-specific regulations focusing on data collection and security matters. We, also, refer to data-breach incidents, and how they have impacted financially the organizations. The present thesis can be found on a website at the link "https://stmaritimesecurity.000webhostapp.com/index.

html

Περιεχόμενα

1 ΝΑΥΤΙΛΙΑ-ΑΣΦΑΛΕΙΑ ΓΕΝΙΚΑ 11

1.1: ΝΑΥΤΙΛΙΑ 11
1.1.1: Κατηγορίες πλοίων με βάση το φορτίο 11
1.1.2: Κατηγορίες φορτηγών πλοίων με βάση το μέγεθος 11
1.2: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ 12
1.3: ΠΡΟΤΥΠΑ-ΦΟΡΕΙΣ 12
1.3.1: Διεθνής ναυτιλιακός οργανισμός 13
1.3.2: Διεθνής οργανισμός τυποποίησης 14
1.3.3: Διεθνής Συνθήκη Περί Ασφάλειας Ανθρώπινης Ζωής Εν Θαλάσση 14
1.4: ΣΥΝΟΨΗ 15
1.5: ΒΙΒΛΙΟΓΡΑΦΙΑ 15

2 ΓΕΝΙΚΗ ΑΝΑΦΟΡΑ ΣΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ 16

2.1: ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΝΑΥΤΙΛΙΑ 18
2.2: ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΠΛΗΡΩΜΑΤΟΣ 20
2.3: ΣΥΝΟΨΗ 21
2.4: ΒΙΒΛΙΟΓΡΑΦΙΑ 21

3 ΝΑΥΤΙΛΙΑΚΑ ΠΡΟΤΥΠΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 23

3.1: ΔΙΕΘΝΗΣ ΚΩΔΙΚΑΣ ΑΣΦΑΛΕΙΑΣ ΠΛΟΙΩΝ ΚΑΙ ΛΙΜΕΝΙΚΩΝ ΕΓΚΑΤΑΣΤΑΣΕΩΝ 23
3.2: ΤΟ ΒΑΛΤΙΚΟ ΚΑΙ ΔΙΕΘΝΕΣ ΝΑΥΤΙΛΙΑΚΟ ΣΥΜΒΟΥΛΙΟ 24
3.3: ΣΥΝΟΨΗ 24
3.4: ΒΙΒΛΙΟΓΡΑΦΙΑ 24

4 ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΗ ΝΑΥΤΙΛΙΑ 25

4.1: ΤΕΧΝΟΛΟΓΙΑ ΠΛΗΡΟΦΟΡΙΩΝ 25
4.2: ΛΕΙΤΟΥΡΓΙΚΗ ΤΕΧΝΟΛΟΓΙΑ 27
4.3 : ΠΡΟΤΥΠΑ – ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ 29
4.3.1: ISO 27001 29
4.3.2: ISO 22301 29
4.3.3: Control Objectives for Information and Related Technology 30
4.3.4: Information Technology Infrastructure Library 30
4.4: ΣΥΝΟΨΗ 30
4.5: ΒΙΒΛΙΟΓΡΑΦΙΑ 31

5 ΠΕΡΙΣΤΑΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΝΑΥΤΙΛΙΑ 32

5.1: ΠΕΡΙΣΤΑΤΙΚΟ MAERSK 32
5.2: ΠΕΡΙΣΤΑΤΙΚΟ CHINA OCEAN SHIPPING COMPANY 32
5.3: ΠΕΡΙΣΤΑΤΙΚΟ AUSTAL 33
5.4: ΣΥΝΟΨΗ 33
5.5: ΒΙΒΛΙΟΓΡΑΦΙΑ 33

6 ΙΔΙΩΤΙΚΟΤΗΤΑ ΜΕΣΑ ΑΠΟ ΤΟ ΠΡΙΣΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ 35

6.1: ΑΠΟΡΡΗΤΟ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ 35
6.2: ΔΕΔΟΜΕΝΑ “IN TRANSIT” 35
6.3: ΔΕΔΟΜΕΝΑ “AT REST” 36
6.4: ΕΡΓΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ 36
6.5: ΣΥΝΟΨΗ 37
6.6: ΒΙΒΛΙΟΓΡΑΦΙΑ 37

7 ΣΥΓΧΡΟΝΕΣ ΕΡΕΥΝΗΤΙΚΕΣ ΤΑΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΝΑΥΤΙΛΙΑΣ 39

7.1: ΜΟΝΤΕΛΟ HYBRID SITUATIONAL AWARENESS 39
7.2: ΦΥΣΙΚΗ ΚΑΙ ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ – ΚΡΙΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ 40

7.3: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΗΝ ΑΛΥΣΙΔΑ ΕΦΟΔΙΑΣΜΟΥ....42
7.4: ΣΥΝΟΨΗ....42
7.5 ΒΙΒΛΙΟΓΡΑΦΙΑ....42
8 ΣΥΜΠΕΡΑΣΜΑΤΑ....44

Κατάλογος εικόνων

ΕΙΚΟΝΑ 4.1: ΤΥΠΙΚΟ ΕΤΑΙΡΙΚΟ ΔΙΚΤΥΟ 26
ΕΙΚΟΝΑ 4.2: ΤΥΠΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΦΑΡΜΟΓΩΝ 27
ΕΙΚΟΝΑ 7.1: ΜΕΘΟΔΟΛΟΓΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ - ΦΥΣΙΚΗ ΚΑΙ ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ ΕΝΟΣ ΛΙΜΕΝΑ 40

Κατάλογος Συντομογραφιών

AIS……Automatic identification system
ARPA……Automatic radar plotting aid
BCMS ……...Business Continuity Management System
BIMCO……Baltic and International Maritime Council
COBIT……Control Objectives for Information and Related Technology
COSCO……China Ocean Shipping Company
CRAMM……Central Communication and Telecommunication Agency. Risk Analysis and Management Method
EBIOS……Expression des Besoins et Identification des Objectifs de Sécurité
ECDIS……Electronic Chart Display and Information System
ECE……Event Correlation Engine
EPAS……Emergency Population Alert System
CSA……Cyber Situational Awareness
GDPR……General Data Protection Regulation
GPS……Global Positioning System
HSA……Hybrid Situational Awareness
ICT……Information and Communication Technology
IEC……International Electrotechnical Commission
IMO……International Maritime Organization
ISACA……Information Systems Audit and Control Association
ISAMM……Information Security Assessment & Monitoring Method
ISO……International Organization for Standardization
ISPS……International Ship and Port Facility Security Code
IT……Information technology
ITIL……Information Technology Infrastructure Library
KPI……Key Performance Indicator
MEHARI……MEthod for Harmonized Analysis of RIsk
MITIGATE……Multidimensional integrated risk assessment framework and dynamic collaborative Risk Management tools for critical information infrastructures
OT……Operational Technology
PSA……Physical Situational Awareness
SOLAS……Safety Of Life At Sea
STORM……Strategic, Tactical & Operational Risk Management
TPE……Threat Protagonist Engine
VDR……Voyage Data Recorder
ΥΠΔ……Υπεύθυνο Προστασίας Δεδομένων
ΑΠΔ……Αρχή Προστασίας Δεδομένων
ΓΚΠΔ……Γενικός κανονισμός για την προστασία δεδομένων
ΕΕ……Ευρωπαϊκή Ένωση
ΗΠΑ……Ηνωμένες Πολιτείες της Αμερικής
ΠΑΑΖΕΘ ……Περί Ασφάλειας Ανθρώπινης Ζωής Εν Θαλάσση

ΦΕΚ……Φύλλα Εφημερίδας της Κυβέρνησης

Εισαγωγή

Η ναυτιλία αποτελεί για την Ελλάδα, αλλά και παγκοσμίως, έναν από τους πιο κρίσιμους τομείς επιχειρηματικής δραστηριότητας. Η εφοδιαστική κρίση που παρατηρείται κατά την εποχή της συγγραφής της παρούσας μεταπτυχιακής διατριβής (2021-2022) επιβεβαιώνει το γεγονός ότι η μεταφορά αγαθών και προϊόντων πετρελαίου από και προς όλα τα σημεία του πλανήτη, αποτελεί έναν από τους πιο σημαντικούς δείκτες ανάπτυξης.

Η ασφάλεια πληροφοριών, ομοίως, είναι ένας ταχύτατα αναπτυσσόμενος κλάδος της τεχνολογίας, και η ευαισθησία των κρατών, των οργανισμών και των προσώπων απέναντι σε ζητήματα ιδιωτικότητας και διαρροών δεδομένων αυξάνεται κατά τα τελευταία χρόνια, και θωρακίζεται από σχετικές νομοθεσίες όπως ο Γενικός Κανονισμός για την Προστασία των Δεδομένων ή General Data Protection Regulation (GDPR). Στα παρακάτω κεφάλαια θα μελετηθούν από κοινού τα ζητήματα ιδιωτικότητας στο χώρο της Ναυτιλίας και, υπό το πρίσμα της πληροφορικής και της τεχνολογίας, θα γίνει προσπάθεια αποτύπωσης της τρέχουσας κατάστασης στα ζητήματα που αφορούν από κοινού τη Ναυτιλία και την ασφάλεια πληροφοριών. Εκτός από τις συνήθεις αρχιτεκτονικές υποδομών και εφαρμογών που διαθέτουν οι συνήθεις Οργανισμοί, ένας ναυτιλιακός Οργανισμός περιλαμβάνει, επιπρόσθετα, τα συστήματα αλλά και τους ανθρώπους που βρίσκονται εν πλω, κάτι το οποίο συνιστά από μόνο του μια σημαντική ιδιαιτερότητα. Για παράδειγμα, τα προσωπικά δεδομένα ενός ναυτικού τηρούνται, εκτός από το πλοίο και την εταιρεία του, σε πολλές λιμενικές και προξενικές αρχές. Επίσης ο εξοπλισμός τεχνολογίας των σύγχρονων πλοίων διαφοροποιείται σημαντικά από τη λογική ενός μέσου πληροφοριακού συστήματος. Έτσι, η προστασία των δεδομένων στη Ναυτιλία έχει περισσότερες προκλήσεις λόγω της φύσης της εν λόγω δραστηριότητας.

Στο κεφάλαιο 1 γίνεται περιγραφή των βασικών εννοιών και των κυριότερων κανονισμών που διέπουν τη ναυτιλία γενικότερα. Το κεφάλαιο 2 αναλύει από νομικής άποψης τα δικαιώματα του πληρώματος και τη σχετική νομοθεσία. Επιπλέον, παρουσιάζεται το General Data Protection Regulation. Στο 3ο κεφάλαιο παρατίθενται τα τρέχοντα ναυτιλιακά πρότυπα για την ασφάλεια της πληροφορίας. Το 4ο κεφάλαιο είναι πιο τεχνικό και παρουσιάζει τα συστήματα Information Technology των Ναυτιλιακών εταιρειών και τα κυριότερα συστήματα Operational Technology των πλοίων. Το κεφάλαιο 5 αναφέρει περιστατικά διαρροών δεδομένων και αναλύει τις οικονομικές επιπτώσεις που αυτά προκάλεσαν. Στο 6ο κεφάλαιο παρουσιάζονται από κοινού τα χαρακτηριστικά της ασφάλειας πληροφορίας που αφορούν τη ναυτιλία και αναφέρονται τεχνικοί τρόποι προστασίας της ιδιωτικότητας.

1 Ναυτιλία-Ασφάλεια γενικά

Στο κεφάλαιο αυτό, δίνονται οι γενικοί ορισμοί και έννοιες που χαρακτηρίζουν την ασφάλεια υπό το πρίσμα των ναυτιλιακών δραστηριοτήτων. Περιγράφονται οι συνιστώσες της ναυτιλίας και πως η ασφάλεια πληροφοριών συσχετίζεται με τις ναυτιλιακές διαδικασίες. Αναφέρονται επίσης τα πρότυπα και οι φορείς που διέπουν κανονιστικά την ναυτιλιακή δραστηριότητα.

1.1: Ναυτιλία

Με τον όρο ναυτιλία αναφερόμαστε στις ασφαλείς δραστηριότητες που συμβαίνουν στην θάλασσα, από την μεταφορά ανθρώπων ως και την μεταφορά αγαθών υγρής ή στερεάς μορφής. Αναλύονται τα πλοία μεταφοράς αγαθών όπως και αναφέρονται και άλλα είδη πλοίων με βάση το φορτίο τους. Στην συνέχεια διαχωρίζονται οι κατηγορίες των πλοίων με βάση το μέγεθός τους, παρουσιάζονται οι ονομασίες αυτών και λεπτομέρειες τους.

1.1.1: Κατηγορίες πλοίων με βάση το φορτίο

Οι βασικές κατηγορίες των πλοίων με βάση το φορτίο το οποίο μεταφέρουν, σύμφωνα με την (e-nautilia, 2021), είναι οι ακόλουθες:

- Φορτηγά Πλοία: είναι τα πλοία τα οποία μεταφέρουν κάθε είδους φορτίου.
- Επιβατικά Πλοία: είναι τα πλοία τα οποία μεταφέρουν επιβάτες και υπό προϋποθέσεις φορτία και οχήματα.
- Πλοία Ειδικού Προορισμού: είναι τα πλοία τα οποία δημιουργήθηκαν για την κάλυψη αναγκών γρήγορης μεταφοράς ή λόγω της εξέλιξης της τεχνολογίας οδηγηθήκαμε στην κατασκευή τους.
- Πλοία Βοηθητικής Ναυτιλίας: είναι τα πλοία τα οποία δεν μεταφέρουν φορτίο ή επιβάτες αλλά συμβάλουν και βοηθούν στην ομαλή και ασφαλή διέλευση των υπολοίπων πλοίων.

1.1.2: Κατηγορίες φορτηγών πλοίων με βάση το μέγεθος

Οι κατηγορίες των φορτηγών πλοίων ανάλογα με το μέγεθος τους, σύμφωνα με την (e-nautilia, 2020),είναι οι εξής:

- Handysize: Μικρά δεξαμενόπλοια με μεταφορική ικανότητα 15,000 – 35,000 τόνων. Μεταφέρουν φορτία πετρελαίου στην τελική του μορφή και αποτελούν την πλειοψηφία των ποντοπόρων πλοίων παγκοσμίως.
- Seawaymax: Είναι τα μεγαλύτερα πλοία που μπορούν να διασχίσουν τις δεξαμενές του ST. Lawrence Seaway. Οι διαστάσεις των πλοίων αυτών είναι 225,6 μ. μήκος 35,5 μ. πλάτος και βύθισμα 7,92 μ.
- Handymax / Supramax: Είναι μικρά φορτηγά πλοία με μεταφορική ικανότητα 60,000 τόνων και είναι ικανά να εισέρχονται σε μικρά λιμάνια τα οποία έχουν περιορισμούς στο μήκος και στο βύθισμα.
- Panamax και New Panamax: Είναι πλοία τα οποία διέρχονται στην διώρυγα του Παναμά και έχουν μέση μεταφορική ικανότητα τους 65,000 τόνους. Τα Panamax είναι πλοία τα οποία δεν ξεπερνούν σε διαστάσεις τα 294,13 μ. μήκος, σε πλάτος τα 32,31 μ. και σε βύθισμα τα 12,04 μ. Το New Panamax ονομάστηκε έτσι λόγω της επέκτασης της διώρυγας του Παναμά και το μέγεθος του φτάνει τα 427 μ. σε μήκος, τα 55μ. σε πλάτος και σε βύθισμα τα 18,30 μ.

- Aframax: Είναι πλοία με μεταφορική ικανότητα 120,000 τόνων. Τα αρχικά AFRA σημαίνουν Average Freight Rate Assessment. Είναι ιδανικά για μικρές και μεσαίες αποστάσεις και χρησιμοποιούνται συνήθως σε λιμάνια στα οποία δεν μπορούν να διέλθουν μεγαλύτερα πλοία.
- Suezmax: Είναι πλοία μεσαίου μεγέθους με μεταφορική ικανότητα 200,000 τόνων. Το όνομα τους πάρθηκε από την διώρυγα του Σουέζ καθώς είναι τα μόνα που πληρούν τους περιορισμούς για να διέλθουν από αυτήν.
- Qatar-Max: Είναι τα μεγαλύτερα πλοία μεταφοράς Υγροποιημένου Φυσικού Αέριου που μπορούν να δέσουν στο Κατάρ σε τερματικούς σταθμούς υγροποιημένου φυσικού αερίου. Η μεταφορική του ικανότητα είναι 266,000 κυβικά μέτρα φυσικού αερίου. Οι διαστάσεις του πλοίου είναι 345 μ. μήκος, 34,7 μ. πλάτος και βύθισμα 12 μ.
- Malaccamax: Είναι τα πλοία που πληρούν τους περιορισμούς για να μπορέσουν να διασχίσουν το στενό Malacca στην Σιγκαπούρη. Οι διαστάσεις τους φτάνουν τα 400 μ. μήκους, 59 μ. πλάτους και το βύθισμα τους τα 14,5 μ.
- Capesize: Είναι πολύ μεγάλα πλοία με μεταφορική ικανότητα μέχρι και 400,000 τόνους. Η κύρια χρήση τους είναι η μεταφορά άνθρακα και σιδήρου. Λόγω του μεγάλου μεγέθους του πλοίου η διέλευση του περιορίζεται σε μικρό αριθμό λιμανιών.
- Very Large Crude Carriers & Ultra Large Crude Carriers: Τα Very Large Crude Carriers έχουν μέγιστη μεταφορική ικανότητα 320,000 τόνων. Τα Ultra Large Crude Carriers είναι τα μεγαλύτερα πλοία με την μεταφορική τους ικανότητα να υπερβαίνει τους 320,000 τόνους. Τα Ultra Large Crude Carriers χρησιμοποιούνται για την μεταφορά αργού πετρελαίου από την Μέση Ανατολή προς Ευρώπη, Ασία και Αμερική.

1.2: Ασφάλεια πληροφοριών

Με τον όρο πληροφορία εννοούμε τον συνδυασμό δεδομένων που συνιστούν μια αληθή απεικόνιση της πραγματικότητας. Σύμφωνα με (Νότης Ηλιόπουλος, 2008), στον τομέα της τεχνολογίας, η πληροφορία εξάγεται από την επεξεργασία ψηφιακά αποθηκευμένων δεδομένων σε πληροφοριακά συστήματα, όπου μπορούν να έχουν πρόσβαση πολλοί χρήστες. Σε ένα τέτοιο περιβάλλον η πληροφορία βρίσκεται εκτεθειμένη σε διαφόρων ειδών κίνδυνους με αποτέλεσμα η ασφάλεια της πληροφορίας να κρίνεται αναγκαία. Η ασφάλεια πληροφοριών συνίσταται από την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα.

- Με τον όρο εμπιστευτικότητα εννοούμε, την απόκρυψη εμπιστευτικών πληροφοριών από μη εξουσιοδοτημένους χρήστες. Επιτυγχάνεται με την καθιέρωση ειδικών μηχανισμών και συγκεκριμένων διαδικασιών.
- Η ακεραιότητα της πληροφορίας έρχεται ως αποτέλεσμα της πληρότητας, της ακρίβειας και της εγκυρότητας. Η εξασφάλιση προστασίας από τροποποίηση της πληροφορίας υλοποιείται από μηχανισμούς και διαδικασίες.
- Μέσω της διαθεσιμότητας εξασφαλίζεται η γρήγορη και συνεχή απόκριση των πληροφοριακών συστημάτων. Πραγματοποιείται με διαδικασίες και μηχανισμούς οι οποίοι ως σκοπό έχουν την αύξηση της διαθεσιμότητας των πληροφοριών και προβλέπουν την ανάκτηση των πληροφοριών αυτών σε περίπτωση βλάβης.

1.3: Πρότυπα-Φορείς

Η ασφάλεια στην ναυτιλία καθορίζονται, μεταξύ άλλων, από θεσμικούς φορείς. Οι σημαντικότεροι σε θέματα ασφάλειας πληροφοριών στην ναυτιλία είναι, ο International Maritime Organization, ο International Organization for Standardization και το Safety of Life at Sea. Στις παρακάτω παραγράφους αναλύουμε αντίστοιχα τον ρόλο των φορέων αυτών.

1.3.1: Διεθνής ναυτιλιακός οργανισμός

Ο Διεθνής Ναυτιλιακός Οργανισμός (International Maritime Organization, IMO) με βάση την (Ελληνική Δημοκρατία Υπουργείο Εξωτερικών, 2020) αποτελεί εξειδικευμένο Οργανισμό των Ηνωμένων Εθνών με σκοπό την ασφάλεια και προστασία της διεθνούς ναυτιλίας και την αποφυγή της θαλάσσιας ρύπανσης που προκαλείται από τα πλοία. Παράλληλα ασχολείται και με την διευκόλυνση της διεθνούς θαλάσσιας κυκλοφορίας καθώς και με τα νομικά ζητήματα της διεθνούς ναυτιλίας, συμπεριλαμβανομένων ζητημάτων ευθύνης και αποζημίωσης από ναυτικές απαιτήσεις. Έχει 174 Κράτη Μέλη και 3 Συνδεδεμένα Μέλη. 63 Διακυβερνητικοί Οργανισμοί συνεργάζονται με το IMO και 80 Μη Κυβερνητικές Οργανώσεις έχουν συμβουλευτικό καθεστώς. Αποτελείται από την Συνέλευση, το Συμβούλιο και 5 Επιτροπές: Επιτροπή Ναυτικής Ασφαλείας, Επιτροπή Προστασίας Θαλασσιού Περιβάλλοντος, Νομική Επιτροπή, Επιτροπή Τεχνικής Συνεργασίας και την Επιτροπή Διευκόλυνσης. Επίσης, υπάρχει ένας σημαντικός αριθμός υποεπιτροπών, που υποστηρίζουν το έργο των κύριων τεχνικών επιτροπών.

Το ανώτατο διοικητικό όργανο του Οργανισμού είναι η Συνέλευση η οποία συνεδριάζει μια φορά κάθε 2 χρόνια σε τακτικές συνόδους αλλά γίνεται να συνεδριάσει και εκτάκτως. Οι αρμοδιότητες της είναι η έγκριση του προγράμματος εργασίας, η ψήφιση του προϋπολογισμού, ο καθορισμός των χρηματοδοτικών αναγκών καθώς και η εκλογή του Συμβούλιου του Οργανισμού. Το Συμβούλιο έχει διετή θητεία και είναι το εκτελεστικό όργανο του IMO, που εποπτεύει το έργο του Οργανισμού. Μεταξύ των συνόδων της Συνέλευσης, το Συμβούλιο εκτελεί όλα τα καθήκοντα της Συνέλευσης, εκτός αυτού της διενέργειας συστάσεων προς τα Κράτη Μέλη του Οργανισμού σχετικά με την ασφάλεια στη θάλασσα και την πρόληψη της ρύπανσης. Οι αρμοδιότητες του Συμβουλίου είναι οι εξής:

1) Συντονισμός των δράσεων των Οργάνων του IMO
2) Κατάρτιση σχεδίου προγράμματος εργασιών και προβλέψεων του προϋπολογισμού του Οργανισμού, τα οποία υποβάλει στη Συνέλευση
3) Λήψη εκθέσεων και προτάσεων των Επιτροπών και άλλων Οργάνων και την υποβολή τους στη Συνέλευση, με σχόλια και συστάσεις, ανάλογα με την περίπτωση
4) Διορισμός του Γενικού Γραμματέα του Οργανισμού, με την επιφύλαξη της έγκρισης της Συνέλευσης και 5) Σύναψη συμφωνιών ή έτερων ρυθμίσεων σχετικά με τη σχέση του Οργανισμού με άλλους οργανισμούς, με την επιφύλαξη έγκρισης από τη Συνέλευση.

Τα μέλη του Συμβουλίου για την περίοδο 2020-2021 χωρίζονται σε τρείς κατηγορίες:

1) Κατηγορία Α. 10 κράτη με το μεγαλύτερο ενδιαφέρον για την παροχή διεθνών ναυτιλιακών υπηρεσιών
2) Κατηγορία Β. 10 κράτη με το ενδιαφέρον για το διεθνές θαλάσσιο εμπόριο και
3) Κατηγορία Γ. 20 κράτη, που έχουν ιδιαίτερα συμφέροντα για τη θαλάσσια μεταφορά ή τη ναυσιπλοΐα και των οποίων η εκλογή στο Συμβούλιο εξασφαλίζει την εκπροσώπηση όλων των μεγάλων γεωγραφικών περιοχών του κόσμου.

Η Επιτροπή Ναυτικής Ασφάλειας είναι το ανώτατο τεχνικό όργανο του IMO. Είναι αρμόδια για την εξέταση όλων των ζητημάτων που εμπίπτουν στο πεδίο εφαρμογής του Οργανισμού και επηρεάζουν άμεσα την ασφάλεια στη θάλασσα. Η Επιτροπή Προστασίας Θαλάσσιου Περιβάλλοντος είναι αρμόδια να εξετάζει κάθε ζήτημα που εμπίπτει στο πεδίο εφαρμογής του Οργανισμού και σχετίζεται με την πρόληψη και τον έλεγχο της ρύπανσης από τα πλοία. Η Νομική Επιτροπή είναι το αρμόδιο τεχνικό όργανο για την εξέταση κάθε ζητήματος που εμπίπτει στο πεδίο εφαρμογής του Οργανισμού με νομικές προεκτάσεις. Η Επιτροπή Τεχνικής Συνεργασίας είναι το αρμόδιο τεχνικό όργανο για την εξέταση κάθε ζητήματος που εμπίπτει στο πεδίο εφαρμογής του Οργανισμού, που σχετίζεται με την υλοποίηση σχεδίων τεχνικής συνεργασίας για τα οποία ο Οργανισμός ενεργεί ως εκτελεστικός ή συνεργαζόμενος οργανισμός. Η Επιτροπή Διευκόλυνσης είναι το αρμόδιο τεχνικό όργανο για την εξέταση κάθε ζητήματος που εμπίπτει στο πεδίο εφαρμογής του Οργανισμού, που σχετίζεται με την εξάλειψη περιττών διατυπώσεων και μείωσης του διοικητικού άχθους στη διεθνή ναυτιλία.

1.3.2: Διεθνής οργανισμός τυποποίησης

Ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO), σύμφωνα με τον (Loshin, 2021), είναι δίκτυο Εθνικών Φορέων Τυποποίησης που επί του παρόντος περιλαμβάνει 147 μέλη, ένα από κάθε χώρα. Ο στόχος του ISO είναι να προωθήσει την ανάπτυξη της Τυποποίησης και των σχετικών με αυτή δραστηριοτήτων στον κόσμο, έτσι ώστε να διευκολύνεται η διεθνής ανταλλαγή αγαθών και υπηρεσιών καθώς επίσης και η ανάπτυξη συνεργασίας σε δραστηριότητες πνευματικού, επιστημονικού, τεχνολογικού και οικονομικού ενδιαφέροντος. Ο ISO ενώνει τα συμφέροντα των παραγωγών, των χρηστών, των κυβερνήσεων και της Επιστημονικής Κοινότητας κατά την προετοιμασία των Διεθνών Προτύπων. Οι δραστηριότητες του Οργανισμού πραγματοποιούνται σε περιφερειακό επίπεδο από τις Τεχνικές Επιτροπές και τις Υποεπιτροπές, οι οποίες οργανώνονται και υποστηρίζονται από Τεχνικές Γραμματείες που ανατίθενται στις χώρες μέλη. Τα αποτελέσματα του Τεχνικού Έργου του ISO εκδίδονται υπό την μορφή των Διεθνών Προτύπων.

Σε ό,τι αφορά την ναυτιλία ο ISO ορίζει μεταξύ άλλων το ISO/TC8, “Ships and Marine Technology”, με σκοπό την τυποποίηση σχεδιασμού, κατασκευής, εκπαίδευσης, δομικών στοιχείων, εξαρτημάτων εξαρτημάτων, εξοπλισμού, μεθόδων και τεχνολογίας και θαλάσσιων περιβαλλοντικών θεμάτων, που χρησιμοποιούνται στη ναυπηγική βιομηχανία, που περιλαμβάνουν θαλάσσια πλοία, πλοία εσωτερικής ναυσιπλοΐας, υπεράκτιες κατασκευές, διεπαφή ship-to-shore, τη λειτουργία πλοίων, θαλάσσιων κατασκευών που υπόκεινται σε απαιτήσεις του IMO και την παρατήρηση και εξερεύνηση της θάλασσας.

1.3.3: Διεθνής Συνθήκη Περί Ασφάλειας Ανθρώπινης Ζωής Εν Θαλάσση

Σύμφωνα με τον (International Maritime Organization, 2020) και την (www.e-nomothesia.gr, 2018), Η Διεθνής Συνθήκη Περί Ασφάλειας Ανθρώπινης Ζωής Εν Θαλάσση (ΠΑΑΖΕΘ, SOLAS) 74 με τις διαδοχικές μορφές της είναι η πιο σημαντική από όλες τις διεθνείς συνθήκες που αφορούν την ασφάλεια των πλοίων και κατ’ επέκταση την ασφάλεια της ανθρώπινης ζωής στην θάλασσα. Αφορμή για την έκδοση της SOLAS ήταν το ναυάγιο του υπερωκεάνιου Ε/Γ «ΤΙΤΑΝΙΚΟΣ», το 1912, το όποιο κόστισε 1500 ζωές. Με αφορμή και αυτό το συμβάν, η διεθνής ναυτιλιακή επιτροπή συνέταξε και εξέδωσε την πρώτη Διεθνή Σύμβαση για την Ασφάλεια της Ανθρώπινης Ζωής στην Θάλασσα το 1914.Από τότε μέχρι σήμερα έχουν υπάρξει αρκετές ανανεωμένες εκδόσεις της SOLAS με κορύφωση τη σύμβαση η όποια υιοθετήθηκε το 1974, τέθηκε σε ισχύ την 25η Μαΐου 1980 και κυρώθηκε με το νόμο 1045/1980 ΦΕΚ 95/Α/25-4-1980.

Σκοπός της ΠΑΑΖΕΘ-SOLAS (International Maritime Organization, 2020) είναι ο καθορισμός των ελαχίστων απαιτήσεων που αφορούν στην κατασκευή, τον εξοπλισμό και την λειτουργία των πλοίων. Περιλαμβάνει άρθρα, στα οποία καθορίζονται οι γενικές υποχρεώσεις των πλοίων καθώς και η διαδικασία τροποποιήσεων. Η σύμβαση ΠΑΑΖΕΘ-SOLAS 74 είναι ιδιαίτερα χρήσιμη στα στελέχη του Λιμενικού Σώματος, Επιθεωρητές πλοίων, σπουδαστές των ναυτικών ακαδημιών, τον Ελληνικό Νηογνώμονα για την έκδοση πιστοποιήσεων των πλοίων και τους ναυτικούς μας γενικότερα. Στην σημερινή μορφή της η SOLAS αποτελείται από 15 κεφάλαια, υποδιαιρούμενα σε μέρη και κανονισμούς.

ΚΕΦΑΛΑΙΟ I	ΓΕΝΙΚΑΙ ΔΙΑΤΑΞΕΙΣ
ΚΕΦΑΛΑΙΟ II-1	ΚΑΤΑΣΚΕΥΗ - ΔΟΜΗ, ΥΠΟΔΙΑΙΡΕΣΗ ΚΑΙ ΕΥΣΤΑΘΕΙΑ, ΜΗΧΑΝΟΛΟΓΙΚΕΣ ΚΑΙ ΗΛΕΚΤΡΟΛΟΓΙΚΕΣ ΕΓΚΑΤΑΣΤΑΣΕΙΣ
ΚΕΦΑΛΑΙΟ II-2	ΚΑΤΑΣΚΕΥΗ - ΠΥΡΟΠΡΟΣΤΑΣΙΑ, ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΚΑΤΑΣΒΕΣΗ ΠΥΡΚΑΪΑΣ
ΚΕΦΑΛΑΙΟ III	ΣΩΣΤΙΚΑ ΜΕΣΑ. Κ.Λ.Π.
ΚΕΦΑΛΑΙΟ IV	ΡΑΔΙΟΕΠΙΚΟΙΝΩΝΙΕΣ
ΚΕΦΑΛΑΙΟ V	ΑΣΦΑΛΕΙΑ ΝΑΥΣΙΠΛΟΙΑΣ

ΚΕΦΑΛΑΙΟ VI	ΜΕΤΑΦΟΡΑ ΦΟΡΤΙΩΝ ΚΑΙ ΚΑΥΣΙΜΩΝ ΠΕΤΡΕΛΑΙΟΥ
ΚΕΦΑΛΑΙΟ VII	ΜΕΤΑΦΟΡΑ ΕΠΙΚΙΝΔΥΝΩΝ ΦΟΡΤΙΩΝ
ΚΕΦΑΛΑΙΟ VIII	ΠΥΡΗΝΟΚΙΝΗΤΑ ΠΛΟΙΑ
ΚΕΦΑΛΑΙΟ IX	ΔΙΑΧΕΙΡΙΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΠΛΟΙΩΝ
ΚΕΦΑΛΑΙΟ X	ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΤΑΧΥΠΛΟΩΝ ΣΚΑΦΩΝ
ΚΕΦΑΛΑΙΟ XI-1	ΕΙΔΙΚΑ ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΑΥΞΗΣΗ ΤΗΣ ΝΑΥΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
ΚΕΦΑΛΑΙΟ XI-2	ΕΙΔΙΚΑ ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΑΥΞΗΣΗ ΤΗΣ ΝΑΥΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
ΚΕΦΑΛΑΙΟ XII	ΠΡΟΣΘΕΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΑ ΦΟΡΤΗΓΑ ΜΕΤΑΦΟΡΑΣ ΧΥΜΑ ΦΟΡΤΙΩΝ
ΚΕΦΑΛΑΙΟ XIII	ΕΠΑΛΗΘΕΥΣΗ ΣΥΜΜΟΡΦΩΣΗΣ

1.4: Σύνοψη

Στο κεφάλαιο αυτό αναφερθήκαμε στον τομέα της ναυτιλίας και στο πώς γίνεται ο διαχωρισμός των πλοίων. Ορίζουμε το τι είναι η πληροφορία και συγκεκριμένα θέτουμε το τι είναι στον τομέα της τεχνολογίας. Αναφερόμαστε στην ασφάλεια πληροφοριών και γνωστοποιούμε τις συνιστώσες της. Κλείνοντας το κεφάλαιο, αναφερόμαστε στα πρότυπα και τους φορείς που διέπουν τον τομέα της ναυτιλίας .

1.5: Βιβλιογραφία

e-nautilia. (2020, Νοέμβριος 06). *Κατηγορίες φορτηγών πλοίων ανάλογα με το μέγεθος τους.* Ανάκτηση από e-nautilia: https://e-nautilia.gr/katigories-fortigwn-ploiwn-analoga-me-to-megethos-tous/

e-nautilia. (2021, Οκτώβριος 29). *Κατηγορίες και είδη πλοίων.* Ανάκτηση από e-nautilia: https://e-nautilia.gr/katigories-kai-eidi-ploiwn/

International Maritime Organization. (2020). *SOLAS, Consolidated Edition, 2020 Edition.* International Maritime Organization.

Loshin, P. (2021, Οκτώβριο). ISO (International Organization for Standardization) . *TechTarget*.

www.e-nomothesia.gr. (2018, Ιανουάριος 30). Ανάκτηση από Η Διεθνής Συνθήκη για την Ασφάλεια της Ζωής στη Θάλασσα (ΠΑΑΖΕΘ -SOLAS 74) Κωδικοποιημένη: https://www.e-nomothesia.gr/law-news/diethnes-suntheke-gia-ten-asphaleia-tis-zois-sti-thalassa-solas-74.html

Ελληνική Δημοκρατία Υπουρείο Εξωτερικών. (2020). Διεθνής Ναυτιλιακός Οργανισμός (IMO).

Νότης Ηλιόπουλος. (2008, Ιούλιος 1). Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα. *IT Security Pro*.

2 Γενική αναφορά στον γενικό κανονισμό για την προστασία των δεδομένων

Σύμφωνα με το (europa.eu, 2022) και την (Intersoft Consulting), ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ), (General Data Protection Regulation, GDPR) καθορίζει λεπτομερώς τις απαιτήσεις για τη συλλογή, την αποθήκευση και τη διαχείριση προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς. Θεσπίστηκε στις 24 Μάιου του 2016 και τέθηκε σε εφαρμογή το στις 25 Μάιου του 2018. Οι απαιτήσεις ισχύουν για ευρωπαϊκούς οργανισμούς που επεξεργάζονται προσωπικά δεδομένα ατόμων στην Ευρωπαϊκή Ένωση (ΕΕ) , αλλά και για οργανισμούς εκτός της ΕΕ οι οποίοι στοχεύουν άτομα που ζουν στην ΕΕ.

Εφαρμόζεται:

- Σε επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα και εδρεύουν στην ΕΕ, ανεξάρτητα από το πού γίνεται η πραγματική επεξεργασία των δεδομένων.
- Σε επιχειρήσεις που εδρεύουν εκτός της ΕΕ αλλά επεξεργάζονται προσωπικά δεδομένα τα οποία αφορούν την παροχή προϊόντων ή υπηρεσιών σε άτομα εντός της ΕΕ, ή παρακολουθούν τη συμπεριφορά ατόμων εντός της ΕΕ.
- Επίσης, Επιχειρήσεις που δεν εδρεύουν στην ΕΕ αλλά επεξεργάζονται δεδομένα πολιτών της ΕΕ οφείλουν να διορίζουν εκπρόσωπο στην ΕΕ.
- Δεν εφαρμόζεται σε περίπτωση που:
- το υποκείμενο των δεδομένων είναι νεκρό.
- το υποκείμενο των δεδομένων είναι νομικό πρόσωπο.
- η επεξεργασία γίνεται από πρόσωπο που ενεργεί για σκοπούς εκτός του εμπορικού, επιχειρηματικού ή επαγγελματικού του πεδίου.

Ως προσωπικά δεδομένα ορίζονται, όλες οι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο, το οποίο καλείται υποκείμενο των δεδομένων. Τα προσωπικά δεδομένα περιέχουν πληροφορίες όπως:

- Όνομα
- Διεύθυνση
- Αριθμό δελτίου ταυτότητας
- Αριθμό διαβατηρίου
- Εισόδημα
- Πολιτισμικό προφίλ
- Κωδικό πρωτοκόλλου διαδικτύου
- Δεδομένα που διατηρούν νοσοκομεία ή γιατροί.

Ειδικές κατηγορίες δεδομένων είναι τα ακόλουθα χαρακτηριστικά ενός προσώπου, στα οποία δεν επιτρέπεται η επεξεργασία:

- φυλετική ή εθνοτική καταγωγή.
- σεξουαλικός προσανατολισμός.
- πολιτικά φρονήματα.
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις.
- συμμετοχή σε συνδικαλιστικές οργανώσεις.
- γενετικά ή βιομετρικά δεδομένα και δεδομένα υγείας, εξαιρουμένων ειδικών περιπτώσεων.
- προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα, εκτός αν αυτό επιτρέπεται από τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία.

Κατά την επεξεργασία τους, τα προσωπικά δεδομένα μπορεί να περάσουν από διάφορες επιχειρήσεις ή οργανισμούς. Μέσα σε αυτόν τον κύκλο, υπάρχουν δύο βασικά προφίλ που ασχολούνται με την επεξεργασία των προσωπικών δεδομένων:

- ο υπεύθυνος επεξεργασίας, οποίος αποφασίζει τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων
- ο εκτελών την επεξεργασία, ο οποίος φυλάσσει και επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

Ο τρόπος επεξεργασίας των προσωπικών δεδομένων παρακολουθείτε μέσα στην επιχείρηση από τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) που μπορεί να έχει οριστεί από την επιχείρηση, είναι αρμόδιος να παρακολουθεί την επεξεργασία των προσωπικών δεδομένων, καθώς και να ενημερώνει και να συμβουλεύει τους υπαλλήλους επεξεργασίας των προσωπικών δεδομένων σχετικά με τις υποχρεώσεις τους. Ο ΥΠΔ συνεργάζεται επίσης με την Αρχή Προστασίας Δεδομένων (ΑΠΔ), λειτουργώντας ως σημείο επαφής μεταξύ της ΑΠΔ και μεμονωμένων ατόμων.

ΥΠΔ ορίζεται σε περιπτώσεις όπου η επιχείρηση:

- παρακολουθεί άτομα, σε τακτική ή συστηματική βάση, ή επεξεργάζεται ειδικές κατηγορίες δεδομένων.
- έχει ως μία από τις κύριες επιχειρηματικές της δραστηριότητες την επεξεργασία δεδομένων.
- επεξεργάζεται δεδομένα σε ευρεία κλίμακα.

Ο ΥΠΔ μπορεί να προέρχεται από το προσωπικό του οργανισμού ή να είναι εξωτερικός συνεργάτης βάσει σύμβασης παροχής υπηρεσιών. Ο ΥΠΔ μπορεί να είναι μεμονωμένο άτομο ή μέρος οργανισμού. Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να αναθέσει την επεξεργασία δεδομένων μόνο σε άτομο που παρέχει επαρκείς εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνονται σε γραπτή σύμβαση μεταξύ των ενδιαφερόμενων μερών. Η σύμβαση αυτή πρέπει επίσης να περιέχει ορισμένες υποχρεωτικές ρήτρες. Όταν προσωπικά δεδομένα μεταφέρονται εκτός της ΕΕ, η προστασία που παρέχει ο ΓΚΠΔ εξακολουθεί να ισχύει για τα εν λόγω δεδομένα. Αυτό σημαίνει ότι αν εξάγετε δεδομένα στο εξωτερικό, η επιχείρησή σας πρέπει να διασφαλίζει ότι τηρείται ένα από τα παρακάτω μέτρα:

- η χώρα εκτός της ΕΕ εφαρμόζει κανόνες που κρίνονται επαρκείς από την ΕΕ
- η επιχείρησή λαμβάνει τα αναγκαία μέτρα για να παράσχει τις κατάλληλες διασφαλίσεις, όπως να περιλάβει συγκεκριμένες ρήτρες στη συμφωνηθείσα σύμβαση με τον εκτός της ΕΕ εισαγωγέα προσωπικών δεδομένων
- η επιχείρησή βασίζεται σε συγκεκριμένα επιχειρήματα για την μεταφορά, όπως η συγκατάθεση του υποκειμένου των δεδομένων.

Σύμφωνα με τους κανόνες της ΕΕ για την προστασία δεδομένων, η επεξεργασία πρέπει να γίνεται με θεμιτό και σύννομο τρόπο, για έναν συγκεκριμένο και νόμιμο σκοπό και να καλύπτει μόνο τα δεδομένα που είναι αναγκαία για την επίτευξη αυτού του σκοπού. Για την επεξεργασία προσωπικών δεδομένων πρέπει να διασφαλιστεί ότι ικανοποιούν έναν από τους παρακάτω όρους :

- Συγκατάθεση του συγκεκριμένου υποκειμένου των δεδομένων
- τα προσωπικά δεδομένα για την τήρηση συμβατικής υποχρέωσης έναντι του υποκειμένου των δεδομένων.
- τα προσωπικά δεδομένα για την εκπλήρωση νομικής υποχρέωσης.
- τα προσωπικά δεδομένα για την προστασία ζωτικών συμφερόντων του υποκειμένου των δεδομένων.
- επεξεργάζεστε προσωπικών δεδομένων για την διεκπεραίωση αποστολής δημοσίου συμφέροντος.
- ενεργείτε προς όφελος των νομίμων συμφερόντων της επιχείρησής, εφόσον δεν θίγονται σοβαρά τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που δέχονται επεξεργασία. Σε περίπτωση που τα δικαιώματα του υποκειμένου υπερισχύουν των συμφερόντων της επιχείρησής, δεν επιτρέπεται η επεξεργασία των προσωπικών του δεδομένων.

Ο ΓΚΠΔ ορίζει αυστηρούς κανόνες για την επεξεργασία δεδομένων βάσει συγκατάθεσης. Σκοπός των κανόνων αυτών είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έχει δώσει τη συγκατάθεσή του. Αυτό σημαίνει ότι η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα. Η συγκατάθεση πρέπει να δίνεται με καταφατική πράξη.

Όταν έχει δοθεί συγκατάθεση για την επεξεργασία προσωπικών δεδομένων, επιτρέπεται η επεξεργασία των δεδομένων μόνο για τους σκοπούς για τους οποίους δόθηκε η συγκατάθεση. Πρέπει επίσης να δίνετε στο υποκείμενο των δεδομένων τη δυνατότητα να αποσύρει τη συγκατάθεσή του. Πρέπει να παρέχετε στα υποκείμενα των δεδομένων σαφείς πληροφορίες σχετικά με το ποιος επεξεργάζεται τα προσωπικά τους δεδομένα και γιατί. Οφείλετε να παρέχετε τουλάχιστον τις παρακάτω πληροφορίες:

- ποιος είστε.
- γιατί δέχονται επεξεργασία τα προσωπικά δεδομένα.
- ποια είναι η νομική βάση.
- ποιος θα λάβει τα δεδομένα, εφόσον υπάρχει.

Σε ορισμένες περιπτώσεις, πρέπει επίσης να δίνονται οι παρακάτω πληροφορίες:

- ποια είναι τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, εφόσον υπάρχει.
- ποιο νόμιμο συμφέρον επιδιώκει η επιχείρηση, όταν για την επεξεργασία βασίζεστε σε αυτό το νομικό επιχείρημα.
- ποια μέτρα ισχύουν για τη μεταφορά δεδομένων σε μια χώρα εκτός της ΕΕ.
- για πόσο διάστημα αποθηκεύονται τα δεδομένα.
- ποια είναι τα δικαιώματα του υποκειμένου των δεδομένων σχετικά με την προστασία των δεδομένων του.
- πώς μπορεί να αποσυρθεί η συγκατάθεση.
- αν υπάρχει καταστατική ή συμβατική υποχρέωση για την παροχή των δεδομένων.
- ποιο είναι το σκεπτικό, η σημασία και οι επιπτώσεις της απόφασης, στην περίπτωση αυτοματοποιημένης λήψης απόφασης.

2.1: Ιδιωτικότητα στην ναυτιλία

Με τον όρο ιδιωτικότητα στην ναυτιλία, αναφερόμαστε στα προσωπικά δεδομένα του κάθε μέλους του πληρώματος και στην προστασία αυτών. Σύμφωνα με (Seacrew Management, 2018), τα προσωπικά δεδομένα τα οποία συλλέγονται από τις εταιρίες ναυτιλιακής απασχόλησης είναι:

- Προσωπικά στοιχεία
- Στοιχεία ταυτότητας
- Στοιχεία επικοινωνίας
- Φωτογραφία Διαβατηρίου
- Πλησιέστερος Συγγενής
- Ιατρικές πληροφορίες
- Πιστοποιητικά ικανότητας
- Έγγραφα του κράτους σημαίας
- Visas
- Πιστοποιητικά εκπαίδευσης
- Τραπεζικά στοιχεία
- Στοιχεία σύμβασης με άλλες εταιρείες
- Εκθέσεις αξιολόγησης
- Στοιχεία μισθών και μισθοδοσίας
- Αναφορές τραυματισμών και ασθενειών
- Στοιχεία σύμβασης με την εταιρεία

Περιστασιακά, η ναυτιλιακή εταιρία χρειάζεται να συλλέξει κάποια επιπρόσθετα προσωπικά δεδομένα του πληρώματος. Σε κάθε περίπτωση οφείλει να παρέχει τους λόγους για τους οποίους απαιτούνται αυτά τα επιπρόσθετα προσωπικά δεδομένα και τον τρόπο επεξεργασία αυτών. Η συλλογή, αποθήκευση, ενημέρωση, μεταφορά και επεξεργασία προσωπικών δεδομένων από την εταιρία γίνεται στον βαθμό που απαιτείται για:

- εξασφάλιση απασχόλησης γι' αυτούς στα πλοία που διαχειρίζεται η εταιρεία.
- σκοπούς που σχετίζονται με την απασχόλησή τους στα πλοία που διαχειρίζεται η εταιρεία.
- σκοπούς που σχετίζονται με την παροχή των υπηρεσιών διαχείρισης του πληρώματος.

Η επεξεργασία των δεδομένων από την εταιρία γίνεται σε περίπτωση που ισχύει ένα ή περισσότερα από τα ακόλουθα:

- οι ναυτικοί έχουν δώσει τη συγκατάθεσή τους για την επεξεργασία των προσωπικών τους δεδομένων.
- η επεξεργασία είναι απαραίτητη για τη σύναψη ή την εκτέλεση των συμβάσεων εργασίας των ναυτικών.
- η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με τους ισχύοντες νόμους και κανονισμούς στους οποίους η Εταιρεία, οι πλοιοκτήτες ή οι διαχειριστές πλοίων υπόκεινται.
- η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων των ναυτικών ή άλλου φυσικού προσώπου.
- η επεξεργασία είναι απαραίτητη για σκοπούς έννομων συμφερόντων που επιδιώκει η εταιρεία ή τρίτο συμβαλλόμενο μέρος, εκτός εάν αυτά τα συμφέροντα υπερισχύουν των συμφερόντων ή των δικαιωμάτων και ελευθεριών των ναυτικών.

Η ναυτιλιακή εταιρεία μεταφέρει τα προσωπικά δεδομένα των ναυτικών σε τρίτους, εντός της Ευρωπαϊκής Ένωσης και σε χώρες εκτός Ευρωπαϊκής Ένωσης, ως μέρος των λειτουργιών και της παροχής υπηρεσιών της και για την απόδοση των συμβάσεων εργασίας των ναυτικών. Οι κατηγορίες τέτοιων τρίτων μπορεί να είναι:

- ταξιδιωτικοί πράκτορες για κρατήσεις πτήσεων και τακτοποίηση βίζας.
- ξενοδοχεία για κράτηση καταλύματος.
- εταιρείες τρένων, λεωφορείων και ταξί για κρατήσεις χερσαίων μεταφορών.
- λιμενικοί πράκτορες για τη φροντίδα των διατυπώσεων μετανάστευσης και τη διευθέτηση της μεταφοράς ναυτικών από και προς το αεροδρόμιο.
- πλοιοκτήτες και διαχειριστές πλοίων για να αποφασίσουν εάν οι ναυτικοί είναι κατάλληλοι για απασχόληση στο πλοίο τους και για λόγους συμμόρφωσης με τις κανονιστικές απαιτήσεις.
- αρχές του κράτους σημαίας για την έκδοση εγγράφων του κράτους σημαίας.
- κυβερνητικές υπηρεσίες ή αρχές για σκοπούς συμμόρφωσης με κανονιστικές υποχρεώσεις.
- τράπεζες για την πληρωμή των μισθών των ναυτικών.
- ασφαλιστικές εταιρείες για την ασφάλιση ναυτικών και την καταβολή αποζημιώσεων σε αυτούς ή στους δικαιούχους τους.
- εκπαιδευτικά κέντρα για την παροχή μαθημάτων.

Η Εταιρεία θα διαβιβάσει τα προσωπικά δεδομένα των ναυτικών σε τρίτα μέρη σε χώρες εκτός Ευρωπαϊκής Ένωση μόνο εάν ισχύει ένα ή περισσότερα από τα ακόλουθα:

- οι ναυτικοί έχουν δώσει ρητά τη συγκατάθεσή τους για τη διαβίβαση των προσωπικών τους δεδομένων.
- η μετάθεση είναι απαραίτητη για την εκτέλεση των συμβάσεων εργασίας των ναυτικών.
- η μεταβίβαση είναι απαραίτητη για τη σύναψη ή εκτέλεση σύμβασης που έχει συναφθεί προς το συμφέρον του ναυτικού μεταξύ της εταιρείας και άλλου φυσικού ή νομικού προσώπου.

2.2: Δικαιώματα του πληρώματος

Σύμφωνα με το (International Labour Conference, 2006), τα δικαιώματα του πληρώματος έρχονται σε συμφωνία με τον πλοιοκτήτη και την εταιρία για την οποία εργάζεται το πλοίο. Ο λόγος για τον οποίο υπογράφεται η συμφωνία είναι η διασφάλιση της δίκαιης εργασιακής συμφωνίας.

1. Οι όροι και οι προϋποθέσεις για την απασχόληση του ναυτικού καθορίζονται ή εκ νέου αναφέρονται σε μια σαφή γραπτή νομικά εκτελεστέα συμφωνία και θα είναι συνεπής με τα πρότυπα που ορίζονται στον Κώδικα της Σύμβασης Ναυτικής Εργασίας.
2. Οι συμφωνίες απασχόλησης των ναυτικών θα επικυρώνονται από τον ναυτικό σύμφωνα με συνθήκες που διασφαλίζουν ότι ο ναυτικός έχει την ευκαιρία να επανεξετάσει και να ζητήσει συμβουλές σχετικά με τους όρους και τις προϋποθέσεις της συμφωνίας και τους αποδέχεται ελεύθερα πριν από την υπογραφή.
3. Στο βαθμό που είναι συμβατές με την εθνική νομοθεσία και πρακτική του μέλους, οι συμβάσεις εργασίας των ναυτικών θα πρέπει να νοείται ότι ενσωματώνουν τυχόν ισχύουσες συλλογικές συμβάσεις εργασίας.

1) Κάθε χώρα επιπλέων θεσπίζει νόμους ή κανονισμούς συμμόρφωσης των ναυτιλιακών εταιριών που φέρουν την δική τους σημαία. Τέτοιοι κανονισμοί είναι:
   a) οι ναυτικοί που εργάζονται σε πλοία που φέρουν τη σημαία της έχουν συμφωνία ναυτικής απασχόλησης που υπογράφεται τόσο από τον ναυτικό όσο και από τον πλοιοκτήτη ή εκπρόσωπο του πλοιοκτήτη παρέχοντάς τους αξιοπρεπείς συνθήκες εργασίας και διαβίωσης επί του πλοίου όπως απαιτείται από την παρούσα Σύμβαση.
   b) οι ναυτικοί που υπογράφουν την σύμβαση θα έχουν την ευκαιρία να εξετάσουν και να ζητήσουν συμβουλές σχετικά με τη συμφωνία πριν από την υπογραφή, για να διασφαλιστεί ότι έχουν εισέλθει ελεύθερα σε συμφωνία με επαρκή κατανόηση των δικαιωμάτων και των υποχρεώσεών τους.
   c) ο ενδιαφερόμενος πλοιοκτήτης και ναυτικός πρέπει να έχουν ο καθένας υπογεγραμμένο πρωτότυπο της σύμβασης ναυτικής απασχόλησης.
   d) λαμβάνονται μέτρα για την διασφάλιση σαφών πληροφορίων σχετικά με τις συνθήκες της απασχόλησης τους οπού μπορούν εύκολα να επιτευχθούν επί του πλοίου από ναυτικούς, συμπεριλαμβανομένου του πλοίαρχου και ότι αυτές οι πληροφορίες, συμπεριλαμβανομένου ενός αντιγράφου της ναυτικής σύμβασης, είναι επίσης προσβάσιμη για έλεγχο από στελέχη αρμόδιας αρχής, όπως επίσης των λιμένων που πρέπει να επισκεφθούν.
   e) στους ναυτικούς χορηγείται έγγραφο που περιέχει το αρχείο απασχόλησής κατά την εργασίας τους στο πλοίο.
2) Όταν μια συλλογική σύμβαση εργασίας αποτελεί το σύνολο ή μέρος της ναυτικής εργασίας-συμφωνία απασχόλησης, αντίγραφο αυτής της συμφωνίας θα είναι διαθέσιμο στο πλοίο. Όπου η γλώσσα της σύμβασης εργασίας των ναυτικών και κάθε ισχύουσας συλλογικής σύμβασης δεν θα είναι στα αγγλικά, τα ακόλουθα θα είναι διαθέσιμα στα αγγλικά(εκτός από πλοία που εκτελούν μόνο ταξίδια εσωτερικού):
   a) Αντίγραφο της συμφωνίας και
   b) τα τμήματα της συλλογικής σύμβασης εργασίας που υπόκεινται σε λιμένα Κρατική επιθεώρηση βάσει του κανονισμού 5.2.
3) Το έγγραφο που αναφέρεται στην παράγραφο 1(e) του παρόντος Προτύπου δεν πρέπει να περιέχει οποιαδήποτε δήλωση σχετικά με την ποιότητα της εργασίας των ναυτικών ή ως προς τον μισθό τους. Η μορφή του εγγράφου, τα στοιχεία που πρέπει να καταγράφονται και ο τρόπος με τον οποίο τα στοιχεία αυτά πρέπει να εισαχθούν, καθορίζονται από το εθνικό δίκαιο.
4) Κάθε Μέλος θεσπίζει νόμους και κανονισμούς που προσδιορίζουν τα θέματα που πρέπει να περιλαμβάνονται σε όλες τις συμβάσεις εργασίας ναυτικών που διέπονται από την οικεία νομοθεσία του. Οι συμβάσεις εργασίας ναυτικών πρέπει σε κάθε περίπτωση να περιέχουν τα ακόλουθα στοιχεία:
   a) το πλήρες όνομα του ναυτικού, η ημερομηνία γέννησης ή η ηλικία και ο τόπος γέννησης.

b) το όνομα και τη διεύθυνση του πλοιοκτήτη.
c) τον τόπο και την ημερομηνία σύναψης της σύμβασης εργασίας των ναυτικών.
d) την ιδιότητα με την οποία πρόκειται να απασχοληθεί ο ναυτικός.
e) το ποσό του μισθού του ναυτικού ή, κατά περίπτωση, τον τύπο που χρησιμοποιείται για υπολογισμό του.
f) το ποσό της ετήσιας άδειας μετ' αποδοχών ή, κατά περίπτωση, τον τύπο που χρησιμοποιήθηκε για τον υπολογισμό του.
g) τη λύση της συμφωνίας και τους όρους αυτής, συμπεριλαμβανομένων:
   i) εάν η συμφωνία έχει συναφθεί για αόριστο χρονικό διάστημα, οι όροι που δίνουν το δικαίωμα σε κάθε μέρος να τη λύσει, καθώς και την απαιτούμενη περίοδο ειδοποίησης, η οποία δεν πρέπει να είναι μικρότερη για τον πλοιοκτήτη από ό,τι για τον ναυτικό.
   ii) εάν η συμφωνία έχει συναφθεί για ορισμένο χρονικό διάστημα, η ημερομηνία που έχει καθοριστεί για αυτήν λήξη.
   iii) εάν η συμφωνία έχει συναφθεί για ταξίδι, ο λιμένας προορισμού και ο χρόνος που πρέπει να λήξει μετά την άφιξη πριν απολυθεί ο ναυτικός.
h) τις παροχές υγείας και κοινωνικής ασφάλισης που παρέχονται στον ναυτικό από τον πλοιοκτήτη.
i) το δικαίωμα του ναυτικού στον επαναπατρισμό.
j) αναφορά στη συλλογική σύμβαση εργασίας, εάν ισχύει.
k) κάθε άλλο στοιχείο που μπορεί να απαιτεί το εθνικό δίκαιο.

5) Κάθε Μέλος θεσπίζει νόμους ή κανονισμούς που θεσπίζουν την προθεσμία ελάχιστης προειδοποίησης που πρέπει να δίνουν οι ναυτικοί και οι πλοιοκτήτες για την πρόωρη λύση της σύμβασης εργασίας ναυτικών. Η διάρκεια αυτών των ελάχιστων περιόδων καθορίζεται μετά από διαβούλευση με τις ενδιαφερόμενες οργανώσεις πλοιοκτητών και ναυτικών, αλλά δεν θα είναι μικρότερη από επτά ημέρες.
6) Μπορεί να δοθεί περίοδος ειδοποίησης μικρότερη από την ελάχιστη, υπό περιστάσεις οι οποίες αναγνωρίζονται βάσει της εθνικής νομοθεσίας ή κανονισμών ή των ισχυουσών συλλογικών συμβάσεων εργασίας ότι δικαιολογούν τη λήξη της σύμβασης εργασίας σε συντομότερη ειδοποίηση ή χωρίς προειδοποίηση. Κατά τον καθορισμό αυτών των περιστάσεων, κάθε μέλος διασφαλίζει ότι η ανάγκη του ναυτικού να καταγγείλει, χωρίς κυρώσεις, τη σύμβαση εργασίας με συντομότερη προειδοποίηση ή χωρίς προειδοποίηση για συμπονετικούς ή άλλους επείγοντες λόγους.

2.3: Σύνοψη

Στο κεφάλαιο αυτό αναφερθήκαμε στο γενικό κανονισμό για την προστασία των δεδομένων και το πως σχετίζεται με το κομμάτι της ναυτιλίας. Στην συνέχεια αναφέρουμε τα προσωπικά δεδομένα του πληρώματος ενός πλοίου και το πως αυτά χρησιμεύουν στην εταιρία έτσι ώστε το μέλος του πληρώματος να μπορεί να παραβρεθεί στον εργασιακό του χώρο. Εν κατακλείδι αναφερόμαστε στα δικαιώματα των μελών του πληρώματος και το πως αυτά έρχονται σε συμφωνία για να μπορέσει το μέλος του πληρώματος να εργαστεί και να διασφαλίσει μια δίκαιη εργασιακή συμφωνία.

2.4: Βιβλιογραφία

europa.eu. (2022). *Προστασία δεδομένων στο πλαίσιο του ΓΚΠΔ*. Ανάκτηση από europa.eu: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm

International Labour Conference. (2006). *Maritime Labour Convention.* International Labour Conference.

Intersoft Consulting. *General Data Protection Regulation*. Ανάκτηση από gdpr-info: https://gdpr-info.eu/

Seacrew Management. (2018, Μάιος 1). *Privacy Notice for Seafarers.* Ανάκτηση από https://seacrew.co/wp-content/uploads/2018/06/Privacy-Notice-for-Seafarers.pdf.

3 ΝΑΥΤΙΛΙΑΚΑ ΠΡΟΤΥΠΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Σε αυτό το κεφάλαιο, αναφέρεται το συγκεκριμένο κανονιστικό πλαίσιο που διέπει την κυβερνοασφάλεια και έχει άμεση ή έμμεση εφαρμογή στις ναυτιλιακές δραστηριότητες. Η βασική ομάδα κανονισμών σε αυτόν τον τομέα είναι ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων και το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο το οποίο καθορίζει το πλαίσιο για την ασφάλεια πληροφορίων στην ναυτιλία. Ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων αποτελεί τη βάση για ένα ολοκληρωμένο υποχρεωτικό καθεστώς ασφαλείας για τη διεθνή ναυτιλία ενώ το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο διασφαλίζει και προσθέτει αξία στις επιχειρήσεις των μελών της με απώτερο σκοπό να είναι ο εκλεκτός συνεργάτης για την ηγεσία την παγκόσμιας ναυτιλιακής βιομηχανίας.

3.1: Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων

Σύμφωνα με (International Maritime Organization, 2021) και (The Editorial Team, 2019), ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (International Ship and Port Facility Security Code, ISPS) είναι ένα σύνολο μέτρων ασφαλείας του IMO, που εφαρμόζεται σε απάντηση στις επιθέσεις της 11ης Σεπτεμβρίου, στο πλαίσιο της Σύμβασης για την Ασφάλεια της Ζωής στη Θάλασσα. Έχοντας τεθεί σε ισχύ σύμφωνα με το κεφάλαιο XI-2 της SOLAS, την πρώτη Ιουλίου 2004, ο Διεθνής Κώδικας για την Ασφάλεια των Πλοίων και Λιμενικών Εγκαταστάσεων αποτελεί τη βάση για ένα ολοκληρωμένο υποχρεωτικό καθεστώς ασφαλείας για τη διεθνή ναυτιλία. Χωρίζεται σε δύο ενότητες, το μέρος Α και το μέρος Β.

Το μέρος Α περιγράφει λεπτομερείς απαιτήσεις σχετικά με την ασφάλεια στην θάλασσα και τους λιμένες, τις οποίες πρέπει να τηρούν οι συμβαλλόμενες κυβερνήσεις, οι λιμενικές αρχές και οι ναυτιλιακές εταιρείες της SOLAS, προκειμένου να συμμορφώνονται με τον Κώδικα. Το μέρος Β του Κώδικα παρέχει μια σειρά προτεινόμενων κατευθυντήριων γραμμών σχετικά με τον τρόπο εκπλήρωσης των απαιτήσεων και των υποχρεώσεων που ορίζονται στις διατάξεις του μέρους Α. Οι κύριοι στόχοι του κώδικα ISPS είναι:

- Η θέσπιση ενός διεθνούς πλαισίου που προάγει τη συνεργασία μεταξύ των συμβαλλομένων κυβερνήσεων, των κυβερνητικών υπηρεσιών, των τοπικών διοικήσεων και των ναυτιλιακών και λιμενικών βιομηχανιών, για την αξιολόγηση και τον εντοπισμό πιθανών απειλών για την ασφάλεια σε πλοία ή λιμενικές εγκαταστάσεις που χρησιμοποιούνται για το διεθνές εμπόριο, προκειμένου να εφαρμοστούν προληπτικά μέτρα ασφαλείας κατά των απειλών.
- Καθορισμός των αντίστοιχων ρόλων και αρμοδιοτήτων όλων των ενδιαφερομένων μερών για τη διασφάλιση της ασφάλειας στη θάλασσα σε λιμένες και επί των πλοίων, σε εθνικό, περιφερειακό και διεθνές επίπεδο.
- Η διασφάλιση έγκαιρης και αποτελεσματικής συνεργασίας και ανταλλαγής πληροφοριών σχετικά με την ασφάλεια στη θάλασσα, σε εθνικό, περιφερειακό και διεθνές επίπεδο.
- Η παροχή μιας μεθοδολογίας για αξιολογήσεις ασφάλειας πλοίων και λιμένων, η οποία διευκολύνει την ανάπτυξη σχεδίων και διαδικασιών ασφάλειας πλοίων, εταιριών και λιμενικών εγκαταστάσεων, η οποία πρέπει να χρησιμοποιηθεί για την ανταπόκριση στα διαφορετικά επίπεδα ασφαλείας πλοίων ή λιμένων. Και
- Να διασφαλιστεί ότι εφαρμόζονται επαρκή και αναλογικά μέτρα ασφαλείας στη θάλασσα στα πλοία και στους λιμένες.

Προκειμένου να επιτευχθούν οι παραπάνω στόχοι, οι αναθέτουσες κυβερνήσεις της SOLAS, οι λιμενικές αρχές και οι ναυτιλιακές εταιρείες υποχρεούνται, βάσει του κώδικα ISPS, να ορίσουν κατάλληλους αξιωματικούς ασφαλείας και προσωπικό, σε κάθε πλοίο, λιμενική εγκατάσταση και ναυτιλιακή εταιρεία. Αυτοί οι αξιωματικοί ασφαλείας, που ορίζονται αξιωματικοί ασφαλείας λιμενικής διευκόλυνσης, αξιωματικοί ασφαλείας πλοίων και αξιωματικοί ασφαλείας εταιρείας, επιφορτίζονται με τα καθήκοντα αξιολόγησης, καθώς και προετοιμασίας και εφαρμογής αποτελεσματικών σχεδίων ασφαλείας που είναι σε θέση να διαχειριστούν οποιαδήποτε πιθανή απειλή για την ασφάλεια.

3.2: Το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο

Σύμφωνα με τις (BIMCO, International Chamber of Shipping, Witherby Publishing Group, 2022) και τον (Munoz, 2016), το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο (Baltic and International Maritime Organization Council, BIMCO) είναι μια ένωση της οποίας τα μέλη είναι οι σημαντικότερες και οι περισσότερες ναυτιλιακές εταιρίες του κόσμου. Η αποστολή της BIMCO είναι να βρίσκεται στην πρώτη γραμμή των παγκόσμιων εξελίξεων στη ναυτιλία, παρέχοντας εξειδικευμένες γνώσεις και πρακτικές συμβουλές για τη διαφύλαξη και την προσθήκη αξίας στις επιχειρήσεις των μελών της και το όραμά της είναι να είναι ο εκλεκτός συνεργάτης που θα εμπιστεύονται για την ηγεσία της παγκόσμιας ναυτιλιακής βιομηχανίας. Η BIMCO έχει καθεστώς μη κυβερνητικής οργάνωσης με γραφεία στην Κοπεγχάγη, τη Σιγκαπούρη, τη Σαγκάη, την Αθήνα και το Λονδίνο και τα μέλη της κυμαίνονται από τους μεγαλύτερους εφοπλιστές στον κόσμο έως μικρούς τοπικούς λιμενικούς πράκτορες και δικηγορικά γραφεία.

Τα συμβόλαια της BIMCO είναι τα πιο ευρέως χρησιμοποιούμενα στη ναυτιλία και σχεδιάζει να διευρύνει συνεχώς το χαρτοφυλάκιό της με περισσότερες από 350 συμβάσεις και ρήτρες. Το κανονιστικό έργο της BIMCO υποστηρίζει τους στόχους της παρέχοντας τη βάση για διαφανή και αμερόληπτα πρότυπα για τη ναυτιλιακή βιομηχανία (ίσοι όροι ανταγωνισμού). Η μείωση των εκπομπών αερίων θερμοκηπίου από τη ναυτιλία, μαζί με τους Στόχους Βιώσιμης Ανάπτυξης των Ηνωμένων Εθνών, θέτουν τη στρατηγική ατζέντα του IMO και θα παρέχει συμβουλές από ειδικούς για την επίτευξη εφικτών και πρακτικών λύσεων. Η φυσική και ψηφιακή ασφάλεια είναι επίσης ψηλά στην ατζέντα της καθώς οδηγούνται στην ανάπτυξη κατευθυντήριων γραμμών και προτύπων που βελτιώνουν την φυσική ασφάλεια, την ψηφιακή ασφάλεια και την αποτελεσματικότητα της ναυτιλίας. Τα μέλη μπορούν να έχουν πρόσβαση σε ολοκληρωμένες πληροφορίες σχετικά με τεχνικά ζητήματα, προειδοποιήσεις ασφαλείας, πληροφορίες πάγου, πληροφορίες λιμένων, βάσεις δεδομένων φορτίου και την πλατφόρμα BIMCO Shipping KPI(Key Performance Indicator).

3.3: Σύνοψη

Στο κεφάλαιο αυτό, κάνουμε αναφορά πάνω στα ναυτιλιακά πρότυπα κυβερνοασφάλειας με βασική ομάδα κανονισμών πάνω σε αυτά τον Διεθνή Κώδικα Ασφάλεια Πλοίων και Λιμενικών Εγκαταστάσεων του διεθνή ναυτιλιακού οργανισμού και του Βαλτικού και Διεθνές Ναυτιλιακού Συμβούλιου οι οποίες καθορίζουν εξίσου το πλαίσιο για την ασφάλεια πληροφορίων στην ναυτιλία.

3.4: Βιβλιογραφία

BIMCO; International Chamber of Shipping; Witherby Publishing Group. (2022). *Cyber Security Workbook for On Board Ship Use.* BIMCO International Chamber of Shipping & Witherby Publishing Group.

International Maritime Organization. (2021). *Guide to Maritime Security and the ISPS CODE.* International Maritime Organization.

Munoz, T. (2016, Δεκεμβρίου 2). BIMCO. *The Maritime Executive*. Ανάκτηση από Baltic and International Maritime Council.

The Editorial Team. (2019, Ιούνιος 18). *Security Measures: A brief review of ISPS Code implementation*. Ανάκτηση από Safety4Sea: https://safety4sea.com/cm-security-measures-a-brief-review-of-isps-code-implementation/

4 ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΗ ΝΑΥΤΙΛΙΑ

Στο κεφάλαιο αυτό θα παρουσιάσουμε το τμήμα της πληροφορικής και της ασφάλειας στην ναυτιλία, η ψηφιοποίηση και η αυτοματοποίηση των διαδικασιών αντιμετωπίζουν πολλές προκλήσεις, διότι οι απειλές στον κυβερνοχώρο φαίνεται να αυξάνονται. Ο κλάδος των θαλάσσιων μεταφορών χρησιμοποιεί διάφορες λειτουργικές τεχνολογίες όπως τα: Global Positioning System, Automatic identification system, Electronic Chart Display and Information System και τεχνολογίες πληροφοριών. Ζημιά σε αυτά τα συστήματα μπορεί να οδηγήσει σε φυσική βλάβη στο πλοίο καθώς και διαρροή δεδομένων, θέτοντας σε κίνδυνο όλη τη ζωή στο σκάφος. Οι εσωτερικές απειλές, είτε εκ προθέσεως είτε όχι, θεωρούνται μία από τις μεγαλύτερες απειλές στον κυβερνοχώρο για τις επιχειρήσεις. Επίσης, κάνουμε αναφορά στα πρότυπα και τις καλές πρακτικές στον τομέα της ναυτιλίας.

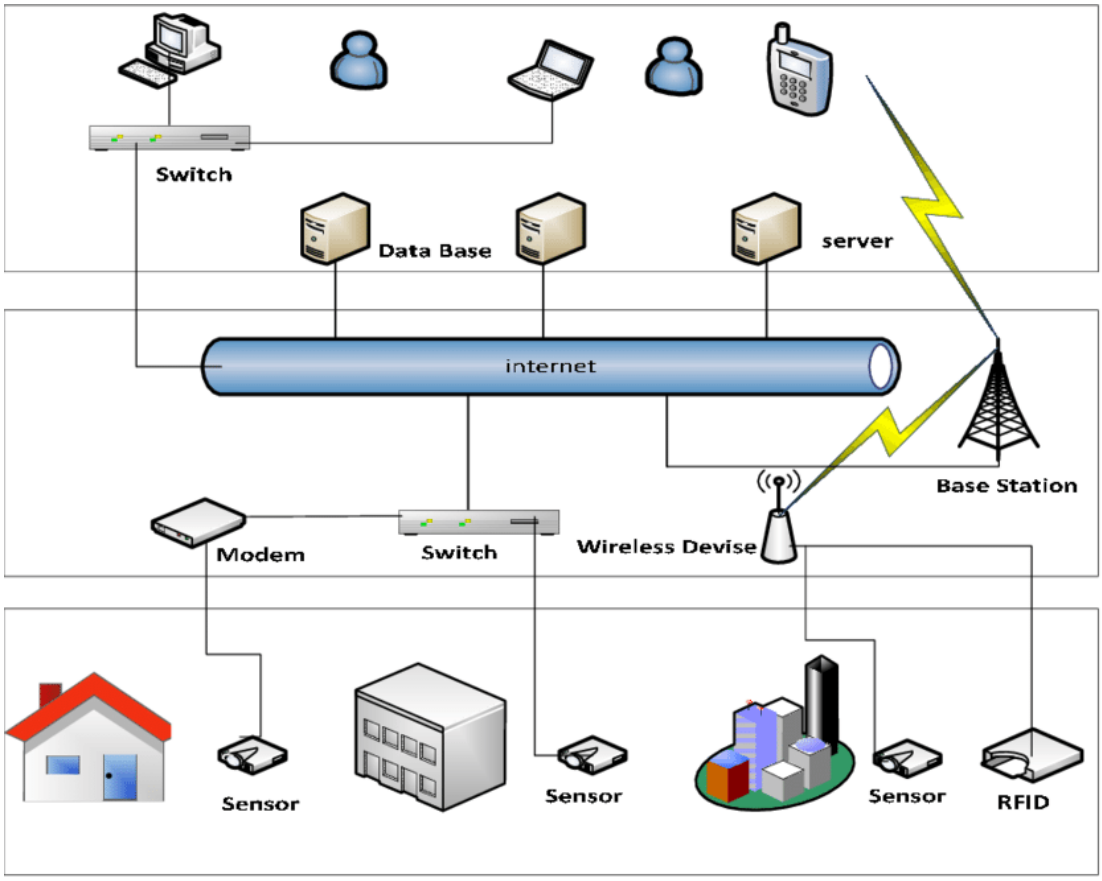
4.1: Τεχνολογία Πληροφοριών

Οι ναυτιλιακές εταιρίες ανεξάρτητα από την συγκεκριμένη επιχειρησιακή δραστηριότητα που ασκούν, διαθέτουν προσωπικό οργανωμένο σε τμήματα, δεδομένα που πρέπει να αποθηκευτούν, εταιρικές επικοινωνίες και εφαρμογές γραφείου ή ειδικότερες. Έτσι κατά ένα μέρος η πληροφορική μιας ναυτιλιακής εταιρίας μοιάζει με την πληροφορική οποιασδήποτε άλλης μεγάλης εταιρίας. Το κομμάτι αυτό της τεχνολογίας είναι η παραδοσιακή τεχνολογία πληροφοριών (Information Technology, IT).

Σύμφωνα με (Indeed Editorial Team, 2020), το περιβάλλον πληροφορικής μιας επιχείρησης αποτελείται από:

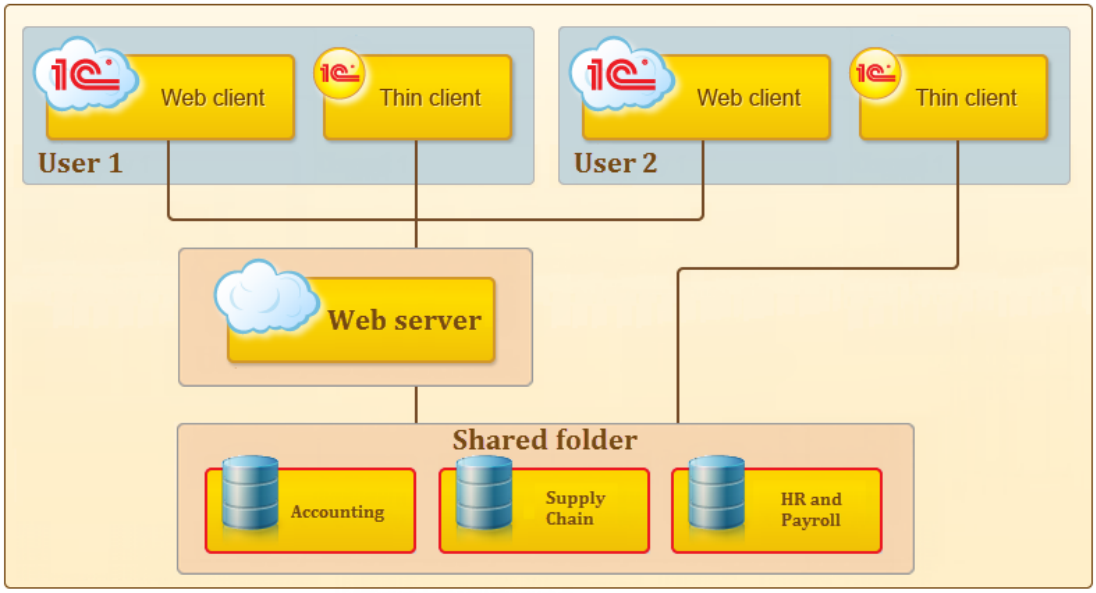
- Υποδομές
- Επικοινωνίες
- Προγραμματισμός-Ανάπτυξη εφαρμογών
- Ιστοσελίδα της Εταιρίας
- Τεχνική Υποστήριξη

Οι υποδομές είναι τα κεντρικά συστήματα hardware και storage στα οποία βασίζονται οι εφαρμογές και η αποθήκευση των δεδομένων. Οι επικοινωνίες είναι τα συστήματα διαχείρισης της ηλεκτρονικής αλληλογραφίας, της πρόσβασης στο διαδίκτυο και της τηλεφωνίας. Ο προγραμματισμός- ανάπτυξη εφαρμογών είναι η υλοποίηση νέων εφαρμογών και η ενημέρωση παλαιών προγραμμάτων για την ομαλή και ασφαλή λειτουργία της εταιρίας. Η Ιστοσελίδα της Εταιρίας και άλλες ενδοεταιρικές σελίδες είναι και αυτές μέρος των συστημάτων πληροφορικής που θα πρέπει να συντηρεί οποιαδήποτε εταιρία. Η τεχνική υποστήριξη είναι μέρος των διαδικασιών πληροφορικής και περιλαμβάνει την υποστήριξη είτε των κεντρικών συστημάτων είτε των συστημάτων γραφείου. Στις επόμενες εικόνες φαίνεται ένα τυπικό IT εταιρικό δίκτυο καθώς και αντιπροσωπευτικές εφαρμογές που περιλαμβάνει και υποστηρίζει.



Εικόνα 4.1: Τυπικό εταιρικό δίκτυο

Στην εικόνα 4.1 παρατηρούμε ένα διάγραμμα διευρυμένης αρχιτεκτονικής στο οποίο απεικονίζεται η συνύπαρξη του παραδοσιακού εταιρικού δικτύου με δίκτυο συλλογής δεδομένων από απομακρυσμένους αισθητήρες σε οικιακές συσκευές και βιομηχανικούς χώρους. Στο επάνω μέρος της εικόνας φαίνεται το εσωτερικό δίκτυο με τους application και data base servers, οι οποίοι παρέχουν εφαρμογές διαθέσιμες σε ηλεκτρονικούς υπολογιστές και φορητές συσκευές μέσω δικτυακών συσκευών όπως είναι τα switches και τα access points. Στο κάτω μέρος φαίνεται η απομακρυσμένη πρόσβαση μέσω modems και ασύρματων σταθμών βάσης (base station), δικτύου αισθητήρων (π.χ. θερμοκρασίας) σε οικίες και εταιρικά περιβάλλοντα, καθώς και Radio Frequency Identification συσκευών που θα μπορούσαν να βρίσκονται ενδεικτικά σε αποθηκευτικούς χώρους.



Εικόνα 4.2: Τυπική αρχιτεκτονική εφαρμογών

Στην εικόνα 4.2 αναπαριστάτε ένα τυπικό διάγραμμα εταιρικού IT δικτύου, όπου εφαρμογές όπως λογιστηρίου, εφοδιαστικής αλυσίδας και διαχείρισης ανθρώπινων πόρων τίθεται στη διάθεση των εργαζομένων μέσω διακομιστή ιστού ή απ' ευθείας. Μια τυπική εφαρμογή λογιστηρίου (accounting) χρησιμεύει στην τήρηση λογιστικών βιβλίων και έκδοση ισολογισμών. Οι εφαρμογές εφοδιαστικής αλυσίδας (supply chain) χρησιμοποιούνται για τις διαδικασίες αποθήκης και οι εφαρμογές ανθρώπινων πόρων εκδίδουν μισθολογικές καταστάσεις και τηρούν αξιολογήσεις των υπαλλήλων. Οι εφαρμογές αυτές παρέχονται μέσω Web Server (π.χ. Apache) και είναι προσβάσιμες από απλούς φυλλομετρητές (π.χ. google chrome) ή με custom πρόγραμμα πελάτη (Thin Client) πάνω από το εταιρικό δίκτυο.

4.2: Λειτουργική Τεχνολογία

Καθώς το επιχειρησιακό σκέλος των ναυτιλιακών εταιριών είναι πάνω στα πλοία, ο τεχνολογικός εξοπλισμός που αφορά την λειτουργία, την ασφάλεια και τις επικοινωνίες του πλοίου δεν συμπεριλαμβάνεται στην κλασσική-παραδοσιακή πληροφορική, αλλά έχει τις δικές του πλέον ιδιαιτερότητες. Σύμφωνα με (Marine Digital), ο εξοπλισμός αυτός, η λειτουργία του και οι σχετικές αρχιτεκτονικές τοπολογίες συνιστούν την λειτουργική τεχνολογία (Operational Technology, OT) της ναυτιλίας.

- Electronic Chart Display and Information System: Σύμφωνα με (Παλλήκαρη, Κατσούνη, & Δακακλή, 2018), το Electronic Chart Display and Information Systems (ECDIS) είναι ένα σύστημα γεωγραφικών πληροφοριών που χρησιμοποιείται για την πλοήγηση και πρέπει να συμμορφώνεται με τους κανονισμούς του Διεθνούς Ναυτιλιακού Οργανισμού ως εναλλακτική λύση έναντι των ναυτικών χαρτών. Η συνεχιζόμενη ασφαλής και αποτελεσματική χρήση του ECDIS περιλαμβάνει πολλούς ενδιαφερόμενους, συμπεριλαμβανομένων ναυτικών, κατασκευαστών εξοπλισμού, παραγωγών χαρτών, παρόχων συντήρησης υλικού και λογισμικού, πλοιοκτήτες και χειριστές και παρόχους εκπαίδευσης. Είναι σημαντικό όλοι αυτοί οι ενδιαφερόμενοι να έχουν σαφή και κοινή κατανόηση των ρόλων και των ευθυνών τους σε σχέση με το ECDIS.
- Γυροσκοπική Πυξίδα: Η γυροσκοπική Πυξίδα είναι μέσω προσανατολισμού, χρησιμοποιείται για να βρει την σωστή κατεύθυνση. Χρησιμοποιείται για τον προσδιορισμό της σωστής βόρειας θέσης, η οποία είναι και ο άξονας περιστροφής της Γης για να παρέχει μια σταθερή πηγή κατεύθυνσης. Δεν έχει καμία σχέση με το μαγνητικό πεδίο της γης και έτσι η ακρίβεια της ένδειξης της δεν επηρεάζεται από μαγνητικές επιδράσεις. Στην γυροσκοπική πυξίδα

μπορεί επίσης, να συνδεθεί ο αυτόματος πιλότος όπου χάρει σε αυτό μπορεί και διορθώνει την πορεία του πλοίου ενεργοποιώντας το πηδάλιο.

- Ραντάρ: Σύμφωνα με (Λιναρδάτου & Λιναρδάτου, 2021), το ραντάρ είναι μια περιστρεφόμενη κεραία που ανιχνεύει την γύρω περιοχή του πλοίου. Τα πλοία βασίζονται σε συστήματα ραντάρ S-band και X-band για πλοήγηση, λόγο της ανίχνευσης των στόχων και της εμφάνισης πληροφοριών στην οθόνη για την αποφυγή σύγκρουσής ή βλάβης. Κάποιες από αυτές τις πληροφορίες είναι η απόσταση του πλοίου από το έδαφος, διάφορα πλωτά αντικείμενα και άλλα σκάφη.
- Μαγνητική Πυξίδα: Η Μαγνητική πυξίδα είναι το κύριο μέσο του δείκτη κατεύθυνσης και λειτουργεί σε συνδυασμό με το μαγνητικό πεδίο της γης. Χρησιμοποιείται για την απόκτηση της προγραμματισμένης διαδρομής ταξιδιού. Η πληροφορία που παρέχει η μαγνητική πυξίδα, για να μπορέσει να την αξιοποιήσει το πλοίο, χρειάζεται έναν μαγνητικό αισθητήρα για να μπορέσει να μεταδώσει το ηλεκτρικό σήμα στην μονάδα επεξεργασίας σήματος και το σήμα να μεταδοθεί σε ψηφιακό.
- Αυτόματος Πιλότος: Η γέφυρα είναι γεμάτη με εξοπλισμό και όργανα που χρησιμοποιούνται για την πλοήγηση του πλοίου. Ο αυτόματος πιλότος θεωρείται ένα από τα πιο αποτελεσματικά βοηθήματα πλοήγησης γέφυρας καθώς βοηθά τον χειριστή να κατευθύνει το σκάφος κρατώντας το τιμόνι σε λειτουργία αυτόματου πιλότου, επιτρέποντάς του να επικεντρωθεί στις ευρείες πτυχές της λειτουργίας. Ο αυτόματος πιλότος για την ορθή λειτουργία του παίρνει πληροφορίες και από άλλα ΟΤ συστήματα και σε συνδυασμό με τις πληροφορίες αυτών μπορεί και διατηρεί την πορεία του πλοίου ορθή και ασφαλή.
- Automatic Radar Plotting Aid: (Σύμφωνα με (Λιουλή, 2013), το Automatic Radar Plotting Aid (APRA) εμφανίζει τη θέση του πλοίου και άλλων κοντινών σκαφών. Το ραντάρ εμφανίζει την θέση των κοντινών πλοίων και επιλέγει μια πορεία για την αποφυγή κάθε είδους σύγκρουσης. Παρουσιάζει επίσης ως διανύσματα στην οθόνη, πλοία, σκάφη, ακίνητα ή πλωτά αντικείμενα και άλλα εμπόδια, και ενημερώνει συνεχώς τις παραμέτρους με κάθε περιστροφή της κεραίας, υπολογίζοντας τα πλησιέστερα σημεία προσέγγισής τους στο δικό τους πλοίο, καθώς και το χρόνο πριν συμβεί αυτό.
- Voyage Data Recorder: Το Voyage Data Recorder (VDR) φέρει τον ρόλο της συνεχής καταγραφής σημαντικών πληροφοριών που σχετίζονται με την λειτουργία του πλοίου. Το σύστημα εγγραφής φωνής του καταγράφει τουλάχιστον τις τελευταίες 12 ώρες και έχει παρόμοια σημασία με το μαύρο κουτί στα αεροπλάνα. Σε περίπτωση ατυχήματος το VDR είναι το πρώτο αντικείμενο το οποίο χρησιμοποιείται για την αναγνώριση του σφάλματος ή του ατυχήματος καθώς μέσω αυτού μπορούν και βρίσκουν το τι οδήγησε σε αυτό.
- Global Positioning System Receiver: Το Global Positioning System (GPS) receiver είναι ένα σύστημα απεικόνισης που χρησιμοποιείται για την εμφάνιση της θέσης ενός πλοίου χρησιμοποιώντας έναν παγκόσμιο δορυφόρο εντοπισμού θέσης. Με την καταγραφή της θέσης του πλοίου μπορείτε να υπολογίσετε την ταχύτητα, την πορεία και τον χρόνο που χρειάζεται για να καλύψει την απόσταση μεταξύ 2 επισημασμένων θέσεων.
- Φώτα Πλοήγησης: Τα φώτα πλοήγησης είναι μια από τις πιο σημαντικές συσκευές πλοήγησης που απαιτούνται για την πλεύση στην ανοιχτή θάλασσα, καθώς επιτρέπουν την καθαρή οπτική επαφή του δικού σας πλοίου από άλλα κοντινά πλοία και παράλληλα να έχετε και εσείς την δυνατότητα να δείτε τα άλλα πλοία τα οποία πλέουν κοντά σας. Είναι ένα από τα βασικότερα ΟΤ συστήματα καθώς χάρη σε αυτά αποφεύγονται τυχών σύγκρουσης μεταξύ πλοίων και υπάρχει αναγνώριση από την στεριά ότι πλέει ένα πλοίο κοντά σε λιμένα είτε γενικότερα κοντά σε στεριά.
- Σχεδιαστής Διαδρομής: Ο θαλάσσιος σχεδιαστής διαδρομής, καθορίζει την βέλτιστη διαδρομή κατά μήκος και παράλληλα χρησιμοποιεί δεδομένα διαφόρων καιρικών συνθηκών για να μπορέσει να υπολογίσει την ασφαλέστερη και πιο οικονομική διαδρομή για το πλοίο στο λιμάνι προορισμού. Στοχεύει στην επιλογή της σειράς των λιμένων που πρέπει να παραβρεθεί για να μπορέσει να σχηματίσει ένα ταξίδι μετ' επιστροφής κλειστού βρόχου.
- Σημαία του Πλοίου: Διάφοροι τύποι σημαιών με διαφορετικά χρώματα και σημάδια χρησιμοποιούνται για να υποδείξουν τη θέση ενός πλοίου πλοήγησης. Σημαίες σήμανσης - είναι ευρέως γνωστές, έχουν χρησιμοποιηθεί από την αρχαιότητα και εξακολουθούν να χρησιμοποιούνται σε όλα τα πλοία σήμερα. Σημαία του πλοίου θεωρείτε επίσης και η σημαία της χώρα από την οποία το πλοίο προέρχεται καθώς αναγράφει την εθνικότητα του πλοίου, σύμφωνα με τους νόμους του οποίου το πλοίο ταξιδεύει στα διεθνή ύδατα.

4.3 : Πρότυπα – Καλές πρακτικές

Σε αυτό το κεφάλαιο, κάνουμε στο κομμάτι των προτύπων και των καλών πρακτικών στο κομμάτι της ναυτιλίας. Τα κύρια αυτά πρότυπα δημοσιεύτηκαν από τον ISO και έχουν ως στόχο την ομαλή και ασφαλή λειτουργία ενός οργανισμού. Το κομμάτι των καλών πρακτικών αφορά το πλαίσιο COBIT της ISACA και την βιβλιοθήκη ITIL οι οποίες ομοίως έχουν ως σκοπό την ομαλή αλλά και την ασφαλή λειτουργία ενός οργανισμού.

4.3.1: ISO 27001

Το ISO 27001 (International Organization for Standardization/International Electrotechnical Commission, 2013) δημοσιεύεται από τον ISO και την International Electrotechnical Commission (IEC). Καθορίζει τις απαιτήσεις για τη δημιουργία, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών στο πλαίσιο του οργανισμού. Επίσης περιλαμβάνει τις απαιτήσεις για την εκτίμηση και την αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών με βάση τις ανάγκες του οργανισμού. Οι απαιτήσεις που καθορίζει το ISO/IEC 27001:2013 είναι γενικές και αφορούν όλους τους οργανισμούς, ανεξαρτήτως τύπου, μεγέθους ή φύσης.

4.3.2: ISO 22301

Το ISO 22301:2019 (International Organization for Standardization, 2019) πρόκειται για ένα διεθνές πρότυπο που δημοσιεύεται από τον ISO και καθορίζει τη δομή και τις απαιτήσεις για την εφαρμογή και τη διατήρηση ενός συστήματος διαχείρισης της επιχειρηματικής συνέχειας (Business Continuity Management System, BCMS). Τα αποτελέσματα της διατήρησης ενός BCMS διαμορφώνονται από τις νομικές, κανονιστικές, οργανωτικές και βιομηχανικές απαιτήσεις του οργανισμού, τα προϊόντα και τις υπηρεσίες που παρέχονται, τις διαδικασίες που χρησιμοποιούνται, το μέγεθος και τη δομή του οργανισμού και τις απαιτήσεις των ενδιαφερομένων μερών του.

Το BCMS δίνει έμφαση στα εξής:

- Κατανόηση των αναγκών του οργανισμού.
- Λειτουργία και διατήρηση διαδικασιών, δυνατοτήτων και δομών ανταπόκρισης.
- Παρακολούθηση και επανεξέταση της απόδοσης και της αποτελεσματικότητας του BCMS.
- Συνεχής βελτίωση βάσει ποιοτικών και ποσοτικών μέτρων.

Ένα σύστημα BCMS περιλαμβάνει τα ακόλουθα :

1) Μια πολιτική
2) Αρμόδια άτομα με καθορισμένες αρμοδιότητες
3) Διαδικασίες διαχείρισης που σχετίζονται με :
    a. Πολιτική
    b. Προγραμματισμός
    c. Εφαρμογή και λειτουργία
    d. Αξιολόγηση Επιδόσεων
    e. Ανασκόπηση της διοίκησης
    f. Συνεχής βελτίωση
4) Τεκμηριωμένες πληροφορίες που υποστηρίζουν τον επιχειρησιακό έλεγχο και επιτρέπουν την αξιολόγηση των επιδόσεων.

4.3.3: Control Objectives for Information and Related Technology

Σύμφωνα με (Brook, 2020), (Harisaiprasad, και συν., 2020), το Control Objectives for Information and Related Technology (COBIT) δημιουργήθηκε από την Information Systems Audit and Control Association (ISACA) για να γεφυρώσει το κρίσιμο χάσμα μεταξύ τεχνικών θεμάτων, επιχειρηματικών κινδύνων και απαιτήσεων ελέγχου. Το πλαίσιο COBIT δημιουργήθηκε για τη διαχείριση και τη διακυβέρνηση των πληροφοριακών συστημάτων μιας επιχείρησης.

Το πλαίσιο COBIT αποτελείται από:

- Το κύριο πλαίσιο. Καθορίζει κατευθυντήριες γραμμές, στόχους και καλές πρακτικές. Αυτά στην συνέχεια συνδέονται με τις ανάγκες και τις απαιτήσεις της επιχείρησης.
- Την περιγραφή των διαδικασιών. Βοηθά τον οργανισμό να έχει ένα μοντέλο διαδικασίας αναφοράς και αντίστροφα μια κοινή γλώσσα που θα χρησιμοποιηθεί από όλους στον οργανισμό.
- Τον έλεγχο στόχων. Κατάλογος απαιτήσεων που η διοίκηση είχε επισημάνει νωρίτερα ως απαραίτητες για τον αποτελεσματικό έλεγχο των διαδικασιών IT.
- Τις Οδηγίες διαχείρισης. Αναφέρουν λεπτομερώς ποιος θα είναι υπεύθυνος για ποια καθήκοντα, καθώς και πως θα μετρηθεί η απόδοση της εταιρείας στην εφαρμογή του COBIT.
- Τα Μοντέλα ωριμότητας. Αξιολόγηση ωριμότητας του οργανισμού και τον τρόπο με τον οποία κάθε μια από τις διαδικασίες IT θα είναι σε θέση αντιμετωπίσει οποιαδήποτε ανάπτυξη.

Το COBIT 2019 βασίζεται σε 6 αρχές :

1. Παροχή αξίας στα ενδιαφερόμενα μέρη
2. Ολιστική Προσέγγιση
3. Σύστημα δυναμικής διακυβέρνησης
4. Διακυβέρνηση διακριτή από τη Διοίκηση
5. Προσαρμοσμένο στις ανάγκες της επιχείρησης
6. Σύστημα διακυβέρνησης από άκρο σε άκρο(end-to-end)

4.3.4: Information Technology Infrastructure Library

Σύμφωνα με (AXELOS Limited, 2020) και (White & Greiner, 2022), το Information Technology Infrastructure Library (ITIL) υποστηρίζει οργανισμούς και άτομα να αποκτήσουν βέλτιστη αξία από τις υπηρεσίες πληροφορικής και ψηφιακών υπηρεσιών. Βοηθά στον καθορισμό της κατεύθυνσης του παρόχου υπηρεσιών με ένα σαφές μοντέλο δυνατοτήτων και τους ευθυγραμμίζει με την επιχειρηματική στρατηγική και τις ανάγκες των πελατών. Το ITIL, ένα επαγγελματικά αναγνωρισμένο σύστημα πιστοποίησης, παρέχει ολοκληρωμένες, πρακτικές και αποδεδειγμένες οδηγίες για τη δημιουργία ενός συστήματος διαχείρισης υπηρεσιών, παρέχοντας ένα κοινό γλωσσάριο όρων για τις επιχειρήσεις που χρησιμοποιούν υπηρεσίες με δυνατότητα πληροφορικής.

4.4: Σύνοψη

Στο κεφάλαιο αυτό αναφερθήκαμε στις τεχνολογίες IT και OT που διατηρούν την ομαλή και ασφαλή πλεύση του πλοίου. Στην συνέχεια αναφέρουμε πρότυπα και πρακτικές που βοηθάνε όχι μόνο την ίδια την επιχείρηση αλλά και τον δέκτη. Αναγνωρίζουμε ότι οι τεχνολογίες αυτές μόνες τους όμως, χωρίς την βοήθεια προτύπων και διαφόρων πρακτικών, μπορούν να θέσουν σε κίνδυνο όχι μόνο το πλήρωμα αλλά και την επιχείρηση εκτός των μελών του πλοίου.

4.5: Βιβλιογραφία

AXELOS Limited. (2020). *ITIL Foundation ITIL 4 Edition.* The Stationery Office.

Brook, C. (2020, Σεπτέμβριος 29). *What is COBIT?* Ανάκτηση από Digital Guardian: https://digitalguardian.com/blog/what-cobit

Harisaiprasad, K., CISA, APP, LI, I. 2., LA, I. 2., LA, I. 9., & Belt, S. S. (2020, Απρίλιος 27). COBIT 2019 and COBIT 5 Comparison. *ISACA*.

Indeed Editorial Team. (2020, Φεβρουάριος 25). *What Does the IT Department Do To Help a Business?* Ανάκτηση από www.indeed.com: https://www.indeed.com/career-advice/career-development/it-department

Marine Digital. *Marine Digital*. Ανάκτηση από 21 Types of Navigation Equipment onboard Ships in Maritime: https://marine-digital.com/article_21types_of_navigation_equipment

White, S. K., & Greiner, L. (2022, Μάιος 16). What is ITIL? Your guide to the IT Infrastructure Library. *CIO*.

Βασιλειάδου, Μ., Υάκινθος, Χ., & Μπαρμουνάκη, Σ. (2020). *Πληροφορική Ηλεκτρονικοί Υπολογιστές*. Ίδρυμα Ευγενίδου.

Λιναρδάτου, Γ. Σ., & Λιναρδάτου, Δ. Σ. (2021). *PANTAP.* Ίδρυμα Ευγενίδου.

Λιουλή, Ι. Σ. (2013). *Διεθνείς κανονισμοί συγκρούσεων στη θάλασσα τήρηση φυλακής/APRA*. Ίδρυμα Ευγενίδου.

Παλλήκαρη, Α. Η., Κατσούνη, Γ. Θ., & Δακακλή, Δ. Α. (2018). *Ναυτικά ηλεκτρονικά όργανα και συστήματα ηλεκτρονικού χάρτη ECDIS.* Ίδρυμα Ευγενίδου.

5 ΠΕΡΙΣΤΑΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΝΑΥΤΙΛΙΑ

Στο ακόλουθο κεφάλαιο, περιγράφονται κάποιες από τις πιο γνωστές περιπτώσεις παραβίασης της ασφάλειας πληροφοριακών συστημάτων σε ναυτιλιακούς οργανισμούς και η έκταση των συνεπειών τους σε οικονομικό και επιχειρησιακό επίπεδο.

5.1: Περιστατικό MAERSK

Το πιο γνωστό και πρόσφατο περιστατικό κυβερνοασφάλειας αφορά την γνωστή Δανέζικη εταιρία Maersk. Η (MAERSK) ιδρύθηκε τον Απρίλιο του 1904 από τον καπετάνιο Peter Maersk Moller και τον γιο του Arnold Peter Moller. Σήμερα Διευθύνων Σύμβουλο της Maersk είναι ο Soren Skou. Ο Δανέζικος κολοσσός της Maersk είναι γνωστός στον κόσμο για την Αποστολή εμπορευματοκιβωτίων και για τους τερματικούς σταθμούς. Παράλληλα ασχολείται με τον εφοδιασμό και αποστολή εμπορευμάτων, την μεταφορά πορθμείων και δεξαμενόπλοιων, τις ημιβυθιζόμενες εξέδρες γεώτρησης, την πλωτή παραγωγή αποθήκευση και εκφόρτωση, την εξερεύνηση και παραγωγή πετρελαίου και φυσικού αερίου, τα ναυπηγεία και τέλος τα καταστήματα λιανικής.

Ως προς τον τύπο της επίθεσης, σύμφωνα με την ιστοσελίδα (www.trellix.com), ο NotPetya είναι μια παραλλαγή του ιού Petya και ονομάζεται έτσι λόγο κάποιων αλλαγών στην συμπεριφορά του κακόβουλου αυτού λογισμικού. Ο Petya ανακαλύφθηκε τον Μάρτιο του 2016 από ερευνητές ασφαλείας και παρατηρήσαν ότι παρότι δεν είναι τόσο εύκολο να προσβληθούν τα πληροφορικά συστήματα, ο ιός είναι μοναδικός στην λειτουργία του. Στην συνέχεια εμφανίστηκαν και άλλες παραλλαγή του κακόβουλου λογισμικού Petya οπού περιείχε μια πρόσθετη δυνατότητα να χρησιμοποιηθεί ο ιός εάν δεν μπορούσε να αποκτήσει πρόσβαση διαχειριστή σε κάποιο πληροφοριακό σύστημα. Λίγο καιρό μετά βλέπουμε την εξέλιξη του ιού με την ονομασία NotPetya ρίχνοντάς οργανισμούς σε όλον τον κόσμο μέσα σε διάστημα λίγων ωρών.

Σύμφωνα με το περιοδικό (The Editorial Team, 2018), τον Ιούνιο του 2017 η Maersk έπεσε θύμα της μεγαλύτερης έως σήμερα κυβερνοεπίθεσης όπου προέκυψε από το κακόβουλο λογισμικό NotPetya με αποτέλεσμα ο Δανέζικος κολοσσός να δεχτεί πλήγμα τόσο οικονομικό όσο και στην φήμη του. Αυτό συνέβη όταν ένας από τους υπαλλήλους τους στην Ουκρανία απάντησε σε ένα email όπου αποτελούταν από το κακόβουλο λογισμικό NotPetya. Παρότι όμως η επίπτωση ήταν άμεση, οπού μέσα σε εφτά λεπτά το δίκτυο βγήκε εκτός λειτουργίας και μέσα σε μια ώρα είχε γίνει μεγάλη ζημιά, η λύση άργησε να έρθει με αποτέλεσμα να χρειαστούν εννέα μέρες για να ανακατασκευαστεί το υπηρεσίες καταλόγου, καθώς και να δημιουργηθούν 2000 νέοι φορητοί υπολογιστές και να ενεργοποιήσουν τις βασικές επιχειρηματικές διαδικασίες και τα συστήματα. Παρ 'όλα αυτά, πρέπει να αναγνωριστεί ότι ο Διευθύνων Σύμβουλος Soren Skou πήρε μέρος σε όλα τα meetings που έγιναν κατά την διάρκεια της κρίσης, για να ενημερώσει όλους τους εργαζόμενους για την κατάσταση που βρισκόντουσαν και για να παρέχει σαφείς οδηγίες για το πως θα πρέπει να αντιδράσουν για να καταφέρουν να την αντιμετωπίσουν.

Σύμφωνα με τα ειδησεογραφικά άρθρα τα οποία βγήκαν τον Ιούνιο του 2017 η οικονομική ζημιά που προκλήθηκε από τον ιό NotPetya θα είχε ύψος 300 εκατομμύρια δολάρια διαφυγόντα κέρδη. Όμως, παρά την απώλεια εσόδων και το κόστος για να μπορέσει να ανακάμψει από τον ιό NotPetya, η Maersk, διατήρησε τις προσδοκίες της για υποκείμενα κέρδη.

5.2: Περιστατικό China Ocean Shipping Company

Η China Ocean Shipping Company (COSCO) είναι ένας κινέζικος πολυεθνικός όμιλος ετερογενών δραστηριοτήτων με έδρα την Σαγκάη. Ο όμιλος επικεντρώνεται στις υπηρεσίες θαλάσσιων μεταφορών. Τον Απρίλιο του 2016 εξαγόρασε το 51% του λιμανιού του Πειραιά έναντι 312.51 εκατομμυρίων δολαρίων. Σύμφωνα με τον (Naveen Groud), έναν χρόνο μετά την επίθεση στην Maersk, στις 24 Ιουλίου του 2018 , ο οργανισμός COSCO έπεσε και αυτός θύμα ransomware. Συγκεκριμένα, η επίθεση έγινε λίγο καιρό μετά που η COSCO εξαγόρασε έναν από τους κύριους

αντιπάλους της, την Orient Overseas Container Lines. Το κακόβουλο λογισμικό αυτό ονομαζόταν SamSam και δημιούργησε σφάλμα σε όλα τα δίκτυα της COSCO στις ΗΠΑ, στον Καναδά, στον Παναμά, την Αργεντινή, την Βραζιλία, το Περού, την Χιλή και την Ουρουγουάη. Όπως και με τον NotPetya, το κακόβουλο λογισμικό που προκάλεσε το περιστατικό Maersk, μόλις το SamSam αποκτήσει πρόσβαση στο δίκτυο, οι κακόβουλοι χρήστες μπορούν να αποκτήσουν δικαιώματα διαχειριστή, οπού έχει ως αποτέλεσμα την εκτέλεση και την ανάγνωση εκτελέσιμων και μη-αρχείων.

Παρότι τα πλοία της και τα κύρια επιχειρησιακά της συστήματα λειτουργούσαν σταθερά, ο σταθμός της COSCO στο λιμάνι του Long Beach επηρεάστηκε. Ενεργοποιώντας τα προγραμματισμένα σχέδια έκτακτης ανάγκης, η COSCO κατάφερε μέσα σε πέντε μέρες να επανέλθει. Οι οικονομικές και τυχών άλλες συνέπειες δεν έχουν δημοσιευτεί από την εταιρία.

5.3: Περιστατικό AUSTAL

Η Austal είναι μια Αυστραλιανή κατασκευαστική εταιρία πλοίων η οποία κατασκευάζει περιπολικά πλοία και φρεγάτες για το Αυστραλιανό Ναυτικό. Επίσης, προμηθεύει πλοία για διεθνείς αγορές και πολεμικά πλοία για τις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) και το Βασιλικό Ναυτικό του Ομάν. Η εταιρία ιδρύθηκε το 1988 στην δυτική Αυστραλία αρχικά για τα εμπορικά πλοία και στην συνέχεια έγινε η μεγαλύτερη ναυπηγική εταιρία αλουμινίου στον κόσμο.

Σύμφωνα με τον (Brett Worthington, 2018), τον Νοέμβριο του 2018, η Αυστραλιανή κατασκευαστική εταιρία πλοίων έπεσε θύμα παραβίασης ασφάλειας στον κυβερνοχώρο. Συγκεκριμένα, στην ανακοίνωσή της στο χρηματιστήριο η εταιρία δήλωσε μόνο πως ο δράστης ήταν άγνωστος. Η Austal, επιβεβαίωσε πως κατά την εισβολή υπήρξε πρόσβαση μόνο σε ορισμένες διευθύνσεις email του προσωπικού και σε αριθμούς τηλεφώνων. Επίσης επιβεβαίωσε ότι σχέδια πλοίου για πελάτες και υπεργολάβους μπορεί να έχουν κλαπεί, αλλά η εταιρία επιμένει πως δεν παραβιάστηκαν εμπορικά στοιχεία ούτε λεπτομερείς που μπορεί να επηρεάσουν ζητήματα εθνικής ασφάλειας. Επίσης, σε δήλωση της η Austal είπε πως η επιχείρηση της στις ΗΠΑ δεν επηρεάζεται καθώς δεν είναι συνδεδεμένα τα συστήματα υπολογιστών.

5.4: Σύνοψη

Στο κεφάλαιο αυτό αναφερθήκαμε στις πιο γνωστές περίπτωσης κυβερνοεπίθεσης που αφορά ναυτιλιακές εταιρίες και οργανισμούς καθώς και τις επίπτωσής που είχαν, οικονομικές και λειτουργικές. Το πιο γνωστό περιστατικό είναι αυτό της Maersk. Επίσης υπάρχουν και της Cosco και της Austal τα οποία είναι εξίσου σημαντικά. Παρατηρούμε ότι παρά το ότι το περιστατικό της Maersk είχε γνωστοποιηθεί σε όλων τον κόσμο καμία από τις προαναφερόμενες εταιρίες δεν ήταν έτοιμη να αντιμετωπίσει μια παρόμοια κατάσταση.

5.5: Βιβλιογραφία

Brett Worthington. (2018, Νοέμβριος 2). *ABC News*. Ανάκτηση από Explainer: Here's what you need to know about the Austal cyber attack and extortion attempt: https://www.abc.net.au/news/2018-11-02/austal-ship-cyber-attack-and-extortion-attempt-national-security/10458982

MAERSK. *MAERSK*. Ανάκτηση από MAERSK: https://www.maersk.com/about/our-history/explore-our-history

Naveen Groud. *Cybersecurity Insiders*. Ανάκτηση από Cyber Attack on COSCO: https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/

The Editorial Team. (2018, Μάιο 31). *Safety4Sea*. Ανάκτηση από Maersk Line: Surviving from a cyber attack: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

www.trellix.com. Ανάκτηση από What Is Petya and NotPetya Ransomware?: https://www.trellix.com/en-us/security-awareness/ransomware/petya.html

6 ΙΔΙΩΤΙΚΟΤΗΤΑ ΜΕΣΑ ΑΠΟ ΤΟ ΠΡΙΣΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Το δικαίωμα της ιδιωτικότητας κατοχυρώνεται νομικά από σειρά κανονισμών με βασικότερο τον GDPR. Στο κεφάλαιο αυτό, περιγράφεται το πως η τεχνολογία της ασφάλειας πληροφοριών υπερασπίζει το δικαίωμα αυτό και το πως τα δεδομένα αυτά βρίσκονται εκτεθειμένα είτε είναι σε κατάσταση in transit είτε σε κατάσταση at rest. Παράλληλα παρουσιάζονται και τρόποι μέσα από τους οποίους και στις δυο καταστάσεις αυτές μπορούμε να προστατεύσουμε τα δεδομένα μας.

6.1: Απόρρητο των επικοινωνιών

Το απόρρητο των επικοινωνιών διασφαλίζεται από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών). Συγκεκριμένα, υπάρχει πλαίσιο νομοθεσίας, που απαρτίζεται από τα παρακάτω:

- Ν.4727/2020 «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2029/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ)2018/1972) και άλλες διατάξεις» (ΦΕΚ Α' 184/2020)
- Κοινή Υπουργική Απόφαση 5321/3/4-οε/2017 «Ανάθεση καθηκόντων Πολιτικής Άμυνας στις Αστυνομικές Αρχές» ΦΕΚ 4657/Β/ 29-12-2017
- Ν. 4411/2016 «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών» (ΦΕΚ 142/Α/3-8-2016)
- Ν. 4070/2012 "Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις" ΦΕΚ 82/Α/10-4-2012
- Ν.4055/2012 «Δίκαιη δίκη και εύλογη διάρκεια αυτής» (ΦΕΚ 51/Α/12-3-2012)
- Ν. 3917/2011 «Σύσταση, οργάνωση και λειτουργία Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος» (ΦΕΚ 22/Α/21-02-2011)
- Ν.3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ 136/Α/10-07-2008)
- Ν.3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997» (ΦΕΚ 133/Α/28-06-2006)
- Ν.3431/2006 «Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις» (ΦΕΚ 13/Α/3-2-2006)
- Ν. 3472/2006 «Ρύθμιση θεμάτων αρμοδιότητας Υπουργείου Δικαιοσύνης και άλλες διατάξεις» (ΦΕΚ 135/Α/04-07-2006)
- Ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ 47/Α/27-02-2003)
- Ν.2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» (ΦΕΚ 121/20-7-1994)

6.2: Δεδομένα "in transit"

Σύμφωνα με την (Sealpath, 2020) και (Nate Lord, 2019), τα δεδομένα in transit είναι αυτά που μεταφέρονται από μια περιοχή δικτύου σε μια άλλη ή εντός ιδιωτικού δικτύου. Κατά την διάρκεια που τα δεδομένα μας χαρακτηρίζονται in transit είναι λιγότερο ασφαλή καθώς είναι εκτεθειμένα στο διαδίκτυο. Για την ασφαλή μεταφορά των δεδομένων η λύση έρχεται σε βάρος της ταχύτητας μεταφοράς, καθώς απαιτούνται επιπρόσθετα δεδομένα, λόγου χάρη, για την κρυπτογράφησή

τους. Κάποιες τεχνικές θωράκισης των δεδομένων in transit είναι, όπως προαναφέρθηκε, η κρυπτογράφησή, το Data Leak Prevention, το Manage File Transfer και πολλές άλλες. Καθώς όμως οι λύσεις για την ασφάλεια των δεδομένων in transit είναι πολλές, οι προκλήσεις είναι ακόμα περισσότερες. Μερικές από τις προκλήσεις αυτές είναι:

- Ο τεράστιος αριθμός εφαρμογών επικοινωνίας και πρωτοκόλλων.
- Οι αμέτρητες εφαρμογές cloud.
- Η αδυναμία ελέγχου του παραλήπτη.

Επίσης, η αδυναμία αξιολόγησης των αρχείων είναι ένα τεράστιο πρόβλημα καθώς είναι δύσκολο να κριθεί από το ίδιο το σύστημα ποια πληροφορία δεν πρέπει να διαρρεύσει και ποια μπορεί. Έτσι, η παραμετροποίηση αυτών των συστημάτων μπορεί να καταλήξει να είναι είτε πιο αυστηρή από το απαιτούμενο είτε πολύ χαλαρή.

6.3: Δεδομένα “at rest”

Σύμφωνα με (Sealpath, 2020) και (Nate Lord, 2019), τα δεδομένα at rest είναι αυτά τα οποία είναι αποθηκευμένα σε κάποια φυσική θέση και είναι διαθέσιμα για ανάκτηση. Όσο τα δεδομένα μας βρίσκονται στον σκληρό μας δίσκο, στον server μας και δεν κινούνται στο διαδίκτυο θεωρούνται πιο ασφαλή, αλλά και πάλι δεν είναι πλήρη ασφαλισμένα. Τα δεδομένα τα οποία είναι σε at rest κατάσταση θεωρούνται ασφαλισμένα όταν είναι κρυπτογραφημένα, όμως υπάρχουν και άλλοι τρόποι ασφάλισης αυτών των δεδομένων. Μερικοί από αυτούς είναι:

- Η πλήρη κρυπτογράφηση του δίσκου, της συσκευής ή του server.
- Η κρυπτογράφηση συγκεκριμένων δεδομένων για όλες τις καταστάσεις τους.
- Μέσω Cloud Access Security Brokers
- Mobile Device Management

Όπως όμως αναφερθήκαμε και στο προηγούμενο κεφάλαιο υπάρχουν και αρκετές προκλήσεις όσων αφορά τις λύσεις για την ασφάλεια των δεδομένων. Κάποιες από αυτές είναι:

- Ότι τα δεδομένα είναι αποθήκευα σε διάφορα μέσα.
- Δεν υπάρχει πλήρης έλεγχος του cloud.
- Πρέπει να ακολουθείτε συγκεκριμένη νομοθεσία για την ασφάλεια δεδομένων.

Για την αντιμετώπιση των προκλήσεων πρέπει να γίνει ανάλυση των κίνδυνων και να εφαρμοστεί ο ανάλογος τρόπος ασφάλισης των δεδομένων.

6.4: Εργαλεία και τεχνολογία της ιδιωτικότητας

Σύμφωνα με τον (Dan Daniels, 2019), το απόρρητο των επικοινωνιών μπορεί να εξασφαλιστεί σε μεγάλο βαθμό από τεχνολογικά εργαλεία και πολιτικές. Κάποια από τα τεχνολογικά εργαλεία μέσα από τα οποία διασφαλίζεται το απόρρητο των επικοινωνιών είναι:

- Το Access control, ο έλεγχος προσβάσεις χρηστών σε συστήματα.
- Το Anti-malware software, όπου μας παρέχει προστασία από κακόβουλα λογισμικά και ιούς.
- Anomaly Detection, κατανόηση του πως πρέπει να λειτουργεί κανονικά το δίκτυο έτσι ώστε όταν υπάρξει κάποια ανωμαλία να την εντοπίσουμε.
- Application Security, ασφάλεια σε επίπεδο εφαρμογής.
- Data Loss Prevention, αποτρέπει τους εσωτερικούς χρήστες ενός οργανισμού να διαρρεύσουν προς τα έξω εμπιστευτικές πληροφορίες.
- Email Security, αποτρέπει την κακόβουλη εισερχόμενη αλληλογραφία.

- Endpoint Security, είναι εφαρμογή που εγκαθιστάτε στους υπολογιστές των τελικών χρηστών ενός οργανισμού και επικοινωνεί με τον server.
- Firewall, επιτρέπει την εισερχομένη και εξερχομένη εξουσιοδοτημένη κίνηση ενώ παράλληλα αποτρέπει τις μη-εξουσιοδοτημένες.
- Intrusion Prevention System, σκανάρει και αναλύει τις κινήσεις του δικτύου με σκοπό την γρήγορη αντιμετώπιση διάφορών επιθέσεων.
- Network Segmentation, περιορισμός κίνησης από ύποπτες πηγές.
- Security Information and Event Management, δίνει στους χρήστες την πληροφορία που χρειάζονται για γρήγορη αντιμετώπιση.
- Το Εικονικό ιδιωτικό δίκτυο, που εξασφαλίζει κρυπτογραφημένη πληροφορία από άκρο σε άκρο.
- Web Security, χρησιμοποιείται για την ασφαλή χρήση του διαδικτύου.
- Wireless security, εξασφάλιση ότι οι μη-εξουσιοδοτημένοι χρήστες δεν έχουν πρόσβαση στο δίκτυο, μέσω ασύρματης σύνδεσης.
- Ο έλεγχος ταυτοποίησης και ο έλεγχος ασφαλείας, που τώρα πια εφαρμόζεται στις περισσότερες εφαρμογές και ιστοσελίδες, για την διασφάλιση των πληροφοριών και του απορρήτου των χρηστών.
- Το Captcha, που είναι διαδικασία αναγνώρισης χρηστών, και χρησιμοποιείτε για τον διαχωρισμό μεταξύ ανθρώπων και bots.

Ως προς το διαδικαστικό κομμάτι, οι μεγάλοι ναυτιλιακοί και μη-οργανισμοί εφαρμόζουν διαδικασίες και πρακτικές όπως είναι οι παρακάτω:

- Αξιολόγηση κινδύνων και προσδιορισμός απαιτήσεων πληροφοριών.
- Διαμόρφωση Εταιρικού πλαισίου Διαχείρισης Ασφάλειας Πληροφοριών.
- Επιβολή της Πολιτικής και των οδηγιών Ασφαλείας, Επιλογή και Υλοποίηση των κατάλληλων Δικλείδων Ασφαλείας.
- Διαρκής Παρακολούθηση και αποτίμηση του επιπέδου ασφάλειας.
- Ενημέρωση και ευαισθητοποίηση του προσωπικού σε θέματα ασφαλείας πληροφοριών.

6.5: Σύνοψη

Στο κεφάλαιο αυτό αναφέραμε ονομαστικά τα Φύλλα Εφημερίδας της Κυβέρνησης τα οποία σχετίζονται με το απόρρητο των επικοινωνιών. Στην συνέχεια ασχοληθήκαμε με τις καταστάσεις που μπορούν τα δεδομένα μας να βρίσκονται και επισημάνουμε ότι και στις δύο καταστάσεις βρίσκονται εκτεθειμένα. Κλείνοντας αναφέραμε τρόπους και εργαλεία μέσα από τα οποία μπορούμε να προστατεύσουμε τα αρχεία μας και τον ίδιο μας τον εαυτό.

6.6: Βιβλιογραφία

Dan Daniels. (2019, Ιούνιος 13). *www.blog.gigamon.com*. Ανάκτηση από 14 Network Security Tools and Techniques to Know: https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/

Nate Lord. (2019, Ιούλιος 15). *www.digitalguardian.com*. Ανάκτηση από Data Protection: Data In transit vs. Data At Rest: https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

Sealpath. (2020, Ιούνιος 23). *ww.sealpath.com*. Ανάκτηση από Protecting the three states of data: https://www.sealpath.com/blog/protecting-the-three-states-of-data/

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. *Νόμοι που αφορούν το απόρρητο των επικοινωνιών*. Ανάκτηση από http://www.adae.gr: http://www.adae.gr/nomothetiko-plaisio/elliniki-nomothesia/nomoi-gia-to-aporrito-epikoinonion/

7 ΣΥΓΧΡΟΝΕΣ ΕΡΕΥΝΗΤΙΚΕΣ ΤΑΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΝΑΥΤΙΛΙΑΣ

Στο ακόλουθο κεφάλαιο αναφέρονται περιληπτικά παλαιότερες ερευνητικές εργασίες μέσα από τις οποίες επηρέασαν γνωστικά την παρούσα εργασία και βοήθησαν περεταίρω στην κατανόηση και την αναγνώριση ορισμών και θεμάτων της ασφάλειας και ιδιωτικότητας στην ναυτιλία. Στην πρώτη εργασία αναφέρουμε ένα μοντέλο Υβριδικής Επίγνωσης Καταστάσεων το οποίο έχει ως στόχο την ανίχνευση και την αντιμετώπιση εξεζητημένων κυβερνοεπιθέσεων. Στην δεύτερη εργασία γίνεται σύγκριση διαφόρων μεθοδολογιών αξιολόγησης για την φυσική και ψηφιακή ασφάλεια ενός λιμένα και παρατηρούμε ότι πρέπει να βρεθεί μια νέα μεθοδολογία η οποία θα πρέπει να έχει ως στόχο την αύξηση της συνεργατικότητας μεταξύ όλων των συμμετεχόντων. Στην τρίτη εργασία περιγράφονται προκλήσεις και κίνδυνοι σχετικά με την ασφάλεια στον κυβερνοχώρο σε περιβάλλον αλυσίδας εφοδιασμού και εστιάζει στην μεθοδολογία της εκτίμησης κινδύνου εφοδιαστικής αλυσίδας MITIGATE.

7.1: Μοντέλο hybrid situational awareness

Στο (Stefan Schauer, 2019) περιγράφεται μια μέθοδος ανίχνευσης και αντιμετώπισης εξεζητημένων κυβερνοεπιθέσεων με την εφαρμογή ενός μοντέλου Hybrid Situational Awareness (HSA). Αυτό το μοντέλο επιτρέπει τη δημιουργία μιας ολιστικής εικόνας της κατάστασης της ασφάλειας εντός των Ναυτιλιακών Υποδομών ζωτικής σημασίας λαμβάνοντας υπόψη τα πιθανά κλιμακωτά αποτελέσματα τέτοιων συνδυασμένων κυβερνοφυσικών επιθέσεων. Στην συνέχεια, η εργασία παρουσιάζει ορισμένα ενδεικτικά παραδείγματα, τα οποία δείχνουν πώς το Hybrid Situational μοντέλο ευαισθητοποίησης μπορεί να ενσωματωθεί σε θαλάσσιο περιβάλλοντα για τον εντοπισμό πιθανών μελλοντικών συντονισμένων επιθέσεων και πώς μπορεί να διευκολύνει την επικοινωνία με τους πρώτους ανταποκριτές και με τις οργανώσεις έκτακτης ανάγκης μιας πόλης σε περίπτωση κρίσης.

Οι λιμενικές υποδομές χρησιμοποιούν δύο συστήματα για την επισκόπηση της τρέχουσας κατάστασης των παγίων. Το Physical Situational Awareness (PSA) του οποίου στόχο είναι η παροχή συνεπούς επισκόπησης όλων των φυσικών παγίων που βρίσκονται εντός των λιμενικών εγκαταστάσεων για εντοπισμό και την πρόληψη κάθε είδους φυσικής επίθεσης σε πραγματικό χρόνο. Το Cyber Situational Awareness (CSA) έχει σαν στόχο την παροχή συνεπούς επισκόπησης όλων των παγίων κυβερνοχώρου που διαχειρίζεται το λιμάνι για τον εντοπισμό και την πρόληψη κάθε είδους κυβερνοεπίθεσης. Βλέποντας και τα δυο συστήματα κατανοούμε ότι, υπάρχουν εξεζητημένες απειλές οπού δεν μπορούν να ανιχνευθούν από κανένα από τα δυο συστήματα, για αυτόν τον λόγο αναπτύχθηκε ένα τρίτο σύστημα, το HSA. Το HSA λειτουργεί σαν σύνδεσμος μεταξύ του PSA και του CSA ενσωματώνοντας πληροφορίες που έρχονται και από τα δύο συστήματα και παρέχει μια πιο ολιστική οπτική για τις υποδομές του λιμανιού. Χρησιμοποιεί δύο κύρια τμήματα, το Event Correlation Engine (ECE) και το Threat Protagonist Engine (TPE). Το ECE καθιερώνει συσχετίσεις μεταξύ των γεγονότων που συμβαίνουν στο φυσικό τομέα και στον τομέα του κυβερνοχώρου για τον εντοπισμό ανωμαλιών. Το TPE υπολογίζει τις πιθανές συνακόλουθες επιπτώσεις που μπορεί να φέρει ένα περιστατικό σε ολόκληρη την υποδομή, δηλαδή τόσο στον φυσικό τομέα όσο και στον τομέα του κυβερνοχώρου.

Παράλληλα το HSA συνδυάζεται με το Emergency Population Alert System (EPAS), όπου δίνει την δυνατότητα στον χειριστή του λιμανιού να έρθει σε απευθείας επικοινωνία με τις πλατφόρμες της έξυπνης πόλης και να ενημερώσει το ευρύ κοινό σε κατάσταση έκτακτης ανάγκης, καθώς και να μπορέσει να αλληλοεπιδράσει με του πρώτους ανταποκριτές και να συντονίσει τις ενέργειές τους. Με την απεικόνιση ενδεικτικών σεναρίων επίθεσης σε δύο κρίσιμες για την αποστολή λιμενικές υπηρεσίες, Κυβερνοφυσική επίθεση στο λιμάνι στην Υπηρεσία Πλεύσης (Cruise Service) και Πολύπλοκη επίθεση στο λιμάνι στην υπηρεσία φορτίου (Container Service), βλέπουμε ότι το προτεινόμενο μοντέλο HSA μπορεί να ενσωματωθεί σε θαλάσσιο περιβάλλοντα, είτε από την αρχή είτε σε συνεργασία με τα υπάρχοντα συστήματα επίγνωσης κατάστασης.

7.2: Φυσική και ψηφιακή ασφάλεια – Κριτική αξιολόγηση

Ο (Georgios Makrodimitris, 2014) παρουσιάζει ήδη υπάρχουσες μεθοδολογίες αξιολόγησης για την φυσική και ψηφιακή ασφάλεια ενός λιμένα. Παρατηρούμε ότι πάρα το μεγάλο εύρος των ήδη υπαρχουσών μεθοδολογιών, οι τρέχουσες διαδικασίες αξιολόγησης φαίνεται να βασίζονται στους πόρους των κινδύνων (χρόνος, κόστος, ανθρώπινο δυναμικό), κάτι το οποίο αναλώνει περισσότερο χρόνο και πόρους και επιπρόσθετα τα αποτελέσματα των αναλύσεων εξαρτώνται όχι μόνο από τα χαρακτηρίστηκα των κινδύνων που αναλύονται αλλά επίσης και από την ποιοτική και ποσοτική προσέγγιση της ίδιας της εκάστοτε μεθοδολογίας, μόνο μια ασχολείται μερικώς και με τις δυο προσεγγίσεις ασφάλειας αλλά καμία δεν ικανοποιεί πλήρως τις ανάγκες των σημερινών απαιτητικών συστημάτων Information and Communication Technology (ICT). Για αυτόν τον λόγο, προτείνεται η ανάπτυξη μιας νέας προσέγγισης λιγότερο περίπλοκης η οποία θα καλύψει επαρκώς τις αναγνωρισμένες αδυναμίες και θα είναι συμβατή με τα πρότυπα του ISO με την ασφάλεια καθώς επίσης θα είναι ανεξάρτητη με το περιβάλλον στο οποίο θα εφαρμοστεί.

Υπάρχουν περισσότερες από 200 μεθοδολογίες αξιολόγησης κίνδυνου και οι πιο γνωστές είναι αυτές που παρουσιάζονται στον επόμενο πίνακα. Ένα κοινό χαρακτηριστικό αυτών των μεθοδολογιών, είναι ότι ασχολούνται μόνο με την ψηφιακή ασφάλεια και όχι την φυσική. Ο παρακάτω πίνακας παρουσιάζει τα χαρακτηριστικά των μεθοδολογιών αυτών:

		Characteristics			
		Evaluation scale	**Impact evaluation**	**Collaboration capabilities**	**Required skills**
Methods	**OCTAVE**	Qualitative	Based on critical assets	Medium	Standard
	CRAMM	Qualitative	Based on open damage scenarios	Low	ICT Experts
	Ebios	Qualitative	Based on security needs	Medium	Standard
	MAGERIT	Quantitative / Qualitative	Based on open damage scenarios	Low	ICT Experts
	MEHARI	Qualitative	Based on fixed damage scenarios	Low	ICT Experts
	STORM	Qualitative	Based on open damage scenarios	High	Low
	IT-Grundschutz	Qualitative	Based on open damage scenarios	Low	Standard
	ISAMM	Qualitative	Based on monetary loss	Low	Standard

Εικόνα 7.1: Μεθοδολογίες αξιολόγησης - φυσική και ψηφιακή ασφάλεια ενός λιμένα

Στην εικόνα 7.2 παρατηρούμε έναν πίνακα που παρουσιάζει τα βασικά χαρακτηριστικά κάθε μεθοδολογίας και παράλληλα δείχνει και μερικά από τα μοναδικά τους χαρακτηρίστηκα. Το OCTAVE σύμφωνα με τον (ENISA) είναι μια σουίτα εργαλείων, τεχνικών και μεθόδων για πληροφορίες που βασίζονται στον κίνδυνο στρατηγικής αξιολόγησης και σχεδιασμού ασφάλειας, βλέπουμε ότι υλοποιείται σε έναν οργανισμό από συγκεκριμένη ομάδα, απαιτείται οι δεξιότητες των συμμετεχόντων να είναι πολύ υψηλές και η συνεργατικότητα της μεθοδολογίας είναι χαμηλή. Έχοντας ως βάση τον (ENISA), το Central Communication and Telecommunication Agency Risk Analysis and Management Method (CRAMM) μπορεί να χρησιμοποιηθεί για την ανάλυση κινδύνου συστημάτων και δικτύων πληροφοριών, για τον εντοπισμό απαιτήσεων ασφαλείας και πιθανές λύσεις και για τον εντοπισμό. Παρατηρούμε στην μεθοδολογία CRAMM πως οι απαιτούμενες δεξιότητες των συμμετεχόντων είναι πολύ υψηλές και η συνεργατικότητα αυτής της μεθοδολογίας είναι επίσης χαμηλή. Λαμβάνοντας υπόψη τον (ENISA) παρατηρούμε πως , η Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) είναι μια μεθοδολογία αξιολόγησης και αντιμετώπισης κινδύνων στον τομέα της πληροφόρησης ασφάλεια συστημάτων

που μπορεί να εφαρμοστεί σε διάφορους οργανισμούς και επιχειρήσεις. Αν και η μεθοδολογία EBIOS είναι συνεργατική και δεν υπάρχει προηγμένη υπολογιστικό σχήμα για τη συσχέτιση και τον προσδιορισμό των αποτελεσμάτων. Αυτό το χαρακτηριστικό αποτελεί σημαντικό μειονέκτημα της μεθοδολογίας. Σύμφωνα με τον (ENISA) η MAGERIT είναι μια μεθοδολογία για τον εντοπισμό και τον μετριασμό των κινδύνων ασφαλείας σε έναν οργανισμό . Μπορεί να χρησιμοποιηθεί και να συντηρηθεί μόνο από ειδικούς χρήστες πληροφορικής. Επομένως, οι απαιτούμενες δεξιότητες των συμμετεχόντων είναι πολύ υψηλή και η συνεργατικότητα της μεθοδολογίας είναι χαμηλή, παρόλο που υπάρχουν αλληλεπιδράσεις μεταξύ των ειδικών και ορισμένων από το προσωπικό του οργανισμού. Στην μεθοδολογία MEthod for Harmonized Analysis of RIsk (MEHARI) λαμβάνοντας υπόψη και τον (ENISA), τα χαρακτηριστικά της μεθοδολογίας MEHARI είναι το μοντέλο κινδύνου, τη συνεκτίμηση της αποτελεσματικότητας των μέτρων ασφαλείας που εφαρμόζονται ή τον σχεδιασμό και την ικανότητα αξιολόγησης και προσομοίωσης του υπολειπόμενου επιπέδου κινδύνου που προκύπτει από πρόσθετα μέτρα, υπάρχει σημαντική συμμετοχή ορισμένων χρηστών σε συγκεκριμένες φάσεις που προκύπτουν σε χαμηλή συνεργατικότητα. Επιπλέον, οι συμμετέχοντες πρέπει να γνωρίζουν ότι έχουν μια διεξοδική κατανόηση του εύρους και του βάθους του οργανισμού, επομένως οι απαιτούμενες δεξιότητές τους είναι πολύ ψηλά. Με βάση την εικόνα 7.2 και την (STORM Guidance) φαίνεται ότι η Strategic, Tactical & Operational Risk Management (STORM) είναι η κατάλληλη μεθοδολογία για να χρησιμοποιηθεί σε κάποιον λιμένα. Το πρόβλημα στη χρήση του STORM όμως είναι το υπολογιστικό σχήμα του συνολικού κινδύνου. Για τον υπολογισμό του κινδύνου, λαμβάνει υπόψη τη μέγιστη τιμή κάθε απάντησης. Αυτό σημαίνει ότι εάν οι χρήστες δίνουν ακραίες τιμές στις απαντήσεις τους, το αποτέλεσμα δεν θα αντιστοιχεί στον αναμενόμενο κίνδυνο του οργανισμού και στην επιλογή του τα αντίμετρα θα είναι λανθασμένα και μη αποτελεσματικά. Το IT-Grundschutz σύμφωνα και με τον (ENISA) μπορεί να εφαρμοστεί από χρήστες που γνωρίζουν πολύ καλά τα πρότυπα πληροφορικής και αναλαμβάνει την ευθύνη υλοποίησης της όλης διαδικασίας. Οι συνεργατικές ικανότητες του IT-Grundschutz μπορεί να θεωρηθούν χαμηλές, επειδή οι χρήστες συμμετέχουν μόνο σε ορισμένα συγκεκριμένα βήματα της αξιολόγησης κινδύνου. Έχοντας ως βάση τον (ENISA) η μεθοδολογία Information Security Assessment & Monitoring Method (ISAMM), αποτελείται από τρία μέρη, το πεδίο εφαρμογής, το πεδίο αξιολόγηση και την ανάλυση της συμμόρφωσης και των απειλών, και έχει ως αποτέλεσμα τους απαραίτητους υπολογισμούς και την υποβολή εκθέσεων. Διαφοροποιείται από τις άλλες διότι οι κίνδυνοι εκφράζονται σε νομισματικές μονάδες.

Οι μεθοδολογίες αυτές δεν αποτυπώνουν την πολυπλοκότητα διασύνδεσης, τις διατομεακές, τις εξαρτήσεις από άλλα συστήματα ή υποδομές και τις κλιμακωτές επιδράσεις σε έναν τομέα ή σε όλους τους τομείς. Θεωρούν το ρίσκο ως συνδυασμό πιθανής απειλής και των επιπτώσεων της, καθώς και του βαθμού ευπάθειας. Επιπρόσθετα, μόνο η μεθοδολογία STORM επιτυγχάνει μεγάλο βαθμό συνεργατικότητας μεταξύ φυσικής και ψηφιακής ασφάλειας. Σε ό,τι αφορά τα πρότυπα φυσικής ασφάλειας, αυτά καλύπτουν τις προδιάγραφες της τρέχουσας ναυτιλιακής νομοθεσίας και προτυποποίησης αλλά όχι την ασφάλεια πληροφοριών των λιμανιών. Δεν αντιμετωπίζουν τις λιμενικές εγκαταστάσεις ως ανεξάρτητες κρίσιμες υποδομές, οι οποίες επίσης διαθέτουν συστήματα πληροφορικής. Έτσι, επιβεβαιώνεται η ανάγκη για μια προσέγγιση που θα φέρει στο προσκήνιο την ασφάλεια πληροφοριών σε αυτό το περιβάλλον.

Η προτεινόμενη νέα μεθοδολογία θα πρέπει να έχει ως στόχο την αύξηση της συνεργατικότητας μεταξύ όλων των συμμετεχόντων προκειμένου να ενισχυθεί η φυσική ασφάλεια και η ασφάλεια πληροφοριών κρίσιμων υποδομών, βασισμένη σε πρότυπα, νομοθεσίες, καλές πρακτικές και οδηγίες. Με βάση τον στόχο της νέας αυτής μεθοδολογίας θα πρέπει να αναπτυχθεί και ένα νέο σύστημα το οποίο θα αναλύσει και θα διαχειριστεί όλα τα είδη απειλών και χρησιμοποιώντας σενάρια κρίσης, θα πρέπει να είναι σε θέση να δημιουργήσει και να ενημερώσει έγγραφα ασφαλείας. Επίσης, πρέπει να χρησιμοποιηθεί η γνώση ενός μεγάλου αριθμού χρηστών για την εκτίμηση και τις αποφάσεις που θα πρέπει να παρθούν με απώτερο σκοπό το να εξαχθούν αποτελέσματα που θα οδηγήσουν σε ενισχυμένη φυσική και ψηφιακή ασφάλεια στις λιμενικές εγκαταστάσεις. Τα κύρια χαρακτηριστικά που διαφοροποιούν τη μεθοδολογία αυτή είναι η συνεργατικότητα και τα υπολογιστικά σχήματα των επιπέδων απειλής και κινδύνου. Παράλληλα είναι μια πολυκριτιριακή τεχνική απόφασης όπου οι χρήστες είναι καταλυτικός παράγοντας στην εκτίμηση του κινδύνου και των επιπτώσεων.

7.3: Ασφάλεια πληροφοριών στην Αλυσίδα Εφοδιασμού

Ο (Spyridon Papastergiou, 2020) περιγράφει προκλήσεις και κίνδυνους σχετικά με την ασφάλεια στον κυβερνοχώρο σε περιβάλλον αλυσίδας εφοδιασμού. Συγκεκριμένα, εστιάζει στην μεθοδολογία της εκτίμησης κινδύνου εφοδιαστικής αλυσίδας Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs (MITIGATE). Παρουσιάζεται μια σειρά από βέλτιστες πρακτικές με μορφή κατευθυντήριων γραμμών για την επιτυχή εφαρμογή του MITIGATE της (CORDIS, 2015) σε περιβάλλον αλυσίδας εφοδιασμού. Επίσης, παρέχονται περιπτώσεις χρήσης οι οποίες είναι βασισμένες σε πραγματικά ναυτιλιακά σενάρια και συλλογή δεδομένων του πραγματικού κόσμου.

Παρουσιάζονται κάποιες από τις βέλτιστες πρακτικές που μπορούν να εφαρμοστούν με επιτυχία στο σύστημα MITIGATE και να χρησιμοποιηθούν από εφοδιαστική αλυσίδα για την κατασκευή ενσωματωμένων μοντέλων διαχείρισης κινδύνου. Αυτές οι βέλτιστες πρακτικές μπορούν να χρησιμοποιηθούν με τα εργαλεία και τις τεχνολογίες που τους είναι απαραίτητες για να εντοπίσουν αποτελεσματικά, να αξιολογήσουν και να αντιμετωπίσουν τα προβλήματα και τα θέματα ασφαλείας τους.

Στην συνέχεια ακολουθεί χαρτογράφηση των βασικών προκλήσεων ασφαλείας της αλυσίδας εφοδιασμού και των βέλτιστων πρακτικών MITIGATE. Βάση αυτού αποδεικνύεται ότι οι λειτουργίες του συστήματος είναι ικανές να αντιμετωπίσουν τις προκλήσεις και τα ζητήματα ασφαλείας στον κυβερνοχώρο. Επιπλέον, δημιουργεί ένα πλαίσιο ασφαλείας στον κυβερνοχώρο. Λαμβάνει υπόψη τις προτεραιότητες της επιτροπής για την κάλυψη των απαιτήσεων ασφαλείας του τρέχοντος και του εξελισσόμενου τοπίου απειλών.

Οι εφοδιαστικές αλυσίδες περιβάλλοντος ναυτιλίας και μεταφορών έχουν κοινά χαρακτηριστικά και αντιμετωπίζουν παρόμοιες προκλήσεις όσων αφορά την ασφάλεια στον κυβερνοχώρο. Λόγω αυτού, το MITIGATE ταιριάζει στις ανάγκες και τις ιδιαιτερότητες τους. Παρατηρούμε επίσης ότι το MITIGATE μπορεί να χρησιμοποιηθεί από διάφορες υποδομές μεταφορών, είτε αερολιμένες είτε σιδηροδρομικές υποδομές, και από διάφορες λιμενικές εγκαταστάσεις, ανεξαρτήτως του μεγέθους και της δραστηριότητάς τους.

7.4: Σύνοψη

Στο κεφάλαιο αυτό παρουσιάστηκαν τρεις ερευνητικές εργασίες. Στην πρώτη περιγράφεται μια μέθοδος ανίχνευσης και αντιμετώπισης εξεζητημένων κυβερνοεπιθέσεων με την εφαρμογή ενός μοντέλου HSA. Στην δεύτερη παρουσιάζονται ήδη υπάρχουσες μεθοδολογίες αξιολόγησης για την φυσική και ψηφιακή ασφάλεια ενός λιμένα και προτείνεται νέα μεθοδολογία η οποία θα πρέπει να έχει ως στόχο την αύξηση της συνεργατικότητας μεταξύ όλων των συμμετεχόντων προκειμένου να ενισχυθεί η φυσική ασφάλεια και η ασφάλεια πληροφοριών κρίσιμων υποδομών. Στην τρίτη περιγράφονται προκλήσεις και κίνδυνοι σχετικά με την ασφάλεια στον κυβερνοχώρο σε περιβάλλον αλυσίδας εφοδιασμού και εστιάζει στην μεθοδολογία της εκτίμησης κινδύνου εφοδιαστικής αλυσίδας MITIGATE.

7.5 Βιβλιογραφία

CORDIS. (2015, Σεπτέμβριος 1). *www.cordis.europa.eu*. Ανάκτηση από Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs: https://cordis.europa.eu/project/id/653212

ENISA. *Cramm*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

ENISA. *Ebios*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

ENISA. *ISAMM*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html

ENISA. *IT-Grundschutz*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html

ENISA. *MAGERIT*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

ENISA. *MEHARI*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

ENISA. *OCTAVE*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

Georgios Makrodimitris, N. P. (2014). *Security Risk Assessment Challenges in Port Information Technology Systems.*

Spyridon Papastergiou, E.-M. K. (2020). *Challenges and Issues in Risk Assessment in Modern Maritime Systems.*

Stefan Schauer, E. -M. (2019). Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness. International Conference on Information and Communication Technologies for Disaster Management (ICT-DM).

STORM Guidance. *www.stormguidance.com*. Ανάκτηση από About us: https://www.stormguidance.com/about-us

8 Συμπεράσματα

Στην διατριβή αυτή έγινε περιγραφή των βασικών εννοιών και των κυριότερων κανονισμών που διέπουν τη ναυτιλία γενικότερα. Αναλύθηκαν από νομικής άποψης τα δικαιώματα του πληρώματος, η σχετική νομοθεσία και παρουσιάστηκε το General Data Protection Regulation. Αναφερθήκαμε στα τρέχοντα ναυτιλιακά πρότυπα για την ασφάλεια της πληροφορίας αναφέροντας και τον ISPS και την BIMCO. Παρουσιάσαμε τα συστήματα Information Technology των Ναυτιλιακών εταιρειών και τα κυριότερα συστήματα Operational Technology των πλοίων. Αναφερθήκαμε στα περιστατικά διαρροών δεδομένων της MAERSK, της COSCO και της AUSTAL και αναλύσαμε τις οικονομικές επιπτώσεις που προκλήθηκαν. Παρουσιάστηκαν τα χαρακτηριστικά της ασφάλειας πληροφορίας που αφορούν τη ναυτιλία και αναφέρθηκαν τεχνικοί τρόποι προστασίας της ιδιωτικότητας. Αναφέραμε περιληπτικά παλαιότερες ερευνητικές εργασίες μέσα από τις οποίες κατανόησα και αναγνώρισα ορισμούς και θέματα της ασφάλειας και της ιδιωτικότητας στην ναυτιλία.