

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
University of the Peloponnese

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία

Πληροφοριακά συστήματα για ασφάλεια στη ναυσιπλοΐα με διατήρηση ενεργειακής αποδοτικότητας σε συνθήκες κυβερνοεπίθεσης

(Maritime security information systems with energy efficiency maintenance under cyberattack conditions)

ΑΛΕΞΑΝΔΡΟΣ ΠΛΑΓΙΑΝΝΑΚΟΣ

Α.Μ.: 2022202002029

Επιβλέπων: Κώστας Βασιλάκης

Τρίπολη, Νοέμβριος 2026

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ....3

Ευρετήριο Εικόνων....7

Ευρετήριο Πινάκων....8

Περίληψη....9

Abstract....10

1 Εισαγωγή....11

2 Πληροφοριακά Συστήματα....12

2.1 Ορισμός Πληροφοριακού Συστήματος....12

2.2 Δομή ενός Πληροφοριακού Συστήματος....12

2.3 Κατηγοριοποιήσεις Πληροφοριακών Συστημάτων....15

2.4 Πλεονεκτήματα και Ζητήματα των Πληροφοριακών Συστημάτων....17

3 Πληροφοριακά Συστήματα στη Ναυτιλία....19

3.1 Κυριότερα Πληροφοριακά Συστήματα....19

3.1.1 Γεωγραφικά Συστήματα Πληροφοριών....19

3.1.2 Πληροφοριακά Συστήματα Διαχείρισης Κυκλοφορίας Σκαφών....21

3.1.3 Ηλεκτρονικά Συστήματα Απεικόνισης Χαρτών και Πληροφοριών....22

3.1.4 Σύστημα Αυτόματης Αναγνώρισης....24

3.1.5 Παγκόσμιο Ναυτιλιακό Σύστημα Κινδύνου και Ασφάλειας....25

4 Ασφάλεια Πληροφοριακών Συστημάτων στη Ναυτιλία....28

4.1 Τα στάδια της Ασφάλειας....28

4.2 Βασικοί Ορισμοί Ασφάλειας....31

4.3 Ζητήματα Ασφάλειας στο Διαδίκτυο....34

4.4 Μεθοδολογία Υλοποίησης Πολιτικών Ασφάλειας....37

4.4.1 Φάση 1: «Καταγραφή υφιστάμενης κατάστασης»....37

4.4.2 Φάση 2: «Ανάλυση επικινδυνότητας» 38

4.5 Φάση 3: «Πολιτική ασφαλείας» 40

4.5.1 Φάση 4: «Καθορισμός Μέτρων Ασφαλείας» 41

4.5.2 Φάση 5: «Σχέδιο έκτακτης ανάγκης» 43

5 Απειλές-Τρωτότητες συστημάτων του πλοίου και διαδικασία ζημιογόνων γεγονότων 45

5.1 Απειλές και κίνδυνοι πληροφοριακών συστημάτων και ανάλυση ζημιογόνων γεγονότων. 45

5.2 Τύποι επιθέσεων 45

5.2.1 Δυσαρεστημένοι Εργαζόμενοι 46

5.2.2 Κακόβουλοι Χάκερς 46

5.2.3 Βιομηχανική Κατασκοπεία 47

5.2.4 Εξωτερική Κυβερνητική Κατασκοπεία 47

5.2.5 Σφάλματα και Παραλείψεις 48

5.2.6 Κακόβουλο λογισμικό 48

5.2.7 Ηλεκτρονικό ψάρεμα 49

5.2.8 Watering Hole Attack 50

5.2.9 Φυσικές υποδομές 50

5.2.10 Προστασία Προσωπικών Δεδομένων 51

5.3 Ευπάθειες (Vulnerabilities) και Ευάλωτα Συστήματα Πλοίου 51

5.4 Ανάλυση Επικινδυνότητας 53

5.4.1 Μέθοδοι ανάλυσης επικινδυνότητας 55

5.5 Ανάλυση επικινδυνότητας 56

5.6 Θεραπεία κινδύνου 58

6 Πολιτικές Ασφαλείας και μέτρα προστασίας 61

6.1 Πολιτικές Ασφαλείας και Διαδικασίες 61

6.2 Μέτρα για την ενίσχυση της επί του πλοίου ασφάλειας στον Κυβερνοχώρο 62

6.3 Εμπλεκόμενοι στην Ανάπτυξη Πολιτικών Ασφάλειας 62

6.4 Βέλτιστη πρόταση μέτρων ασφάλειας 63

6.5 Υλοποίηση Μέτρων Ασφαλείας στην Πράξη 63

6.6 «Άμυνα σε βάθος» (“defense in depth”) 64

6.7 «Άμυνα σε πλάτος» (“ defense in breadth”) 65

6.8 Προστασία και Αποτροπή Επιθέσεων 65

6.9 Τεχνικά Μέτρα Προστασίας 66

6.10 Διαδικαστικά Μέτρα Προστασίας 68

7 Ενεργειακή Αποδοτικότητα κατά τη διάρκεια Κυβερνοεπιθέσεων 71

7.1 Επιπτώσεις κυβερνοεπιθέσεων στην ενεργειακή κατανάλωση των πλοίων 71

7.1.1 Κυβερνοεπιθέσεις και αποσταθεροποίηση των συστημάτων ελέγχου ενέργειας 71

7.1.2 Διακοπές λειτουργίας και αύξηση ενεργειακού κόστους 72

7.1.3 Επιπτώσεις στις λειτουργίες των μηχανών και της πρόωσης 73

7.1.4 Η ενεργειακή αποδοτικότητα υπό καθεστώς απώλειας επικοινωνιών 74

7.1.5 Παράδειγμα ενεργειακής αναποτελεσματικότητας λόγω κυβερνοεπίθεσης 75

7.2 Στρατηγικές εξοικονόμησης ενέργειας σε περίπτωση επίθεσης 76

7.2.1 Άμεσες παρεμβάσεις για αποκατάσταση ενεργειακής ισορροπίας 76

7.2.2 Ρόλος των εφεδρικών συστημάτων στη διαχείριση ενέργειας 77

7.2.3 Οικονομικές στρατηγικές για μείωση του κόστους ενέργειας κατά την επίθεση 78

7.2.4 Ενεργειακά αποδοτικές επιλογές διαδρομής σε συνθήκες έκτακτης ανάγκης 79

7.2.5 Συνεργασία με παρόχους τεχνολογίας για άμεσες λύσεις εξοικονόμησης 80

7.3 Αναδυόμενες τεχνολογίες για την ενεργειακή αποδοτικότητα υπό συνθήκες έκτακτης ανάγκης 80

7.3.1 Τεχνητή νοημοσύνη για ανάλυση ενεργειακής κατανάλωσης σε πραγματικό χρόνο 81

7.3.2 Αυτοματοποίηση συστημάτων πρόωσης για βέλτιστη ενεργειακή διαχείριση 82

7.3.3 Έξυπνα συστήματα παρακολούθησης καυσίμου σε περιπτώσεις κυβερνοεπίθεσης 83

7.3.4 Δικτυακά ενεργειακά συστήματα για τη μείωση των απωλειών 84

7.3.5 Blockchain για ασφαλή διαχείριση δεδομένων ενέργειας 84

7.4 Παραδείγματα εφαρμογής συστημάτων εξοικονόμησης ενέργειας σε πραγματικές συνθήκες κυβερνοεπίθεσης 85

7.4.1 Μελέτη περίπτωσης: Εφαρμογή αυτόματου ελέγχου ενέργειας σε πλοία 85

7.4.2 Υποβάθμιση ενεργειακής απόδοσης κατά την κυβερνοεπίθεση σε δεξαμενόπλοιο 86

7.4.3 Σενάρια ανασυγκρότησης ενεργειακών συστημάτων μετά από κυβερνοεπίθεση 87

7.4.4 Συνδυασμός φυσικής και κυβερνοασφάλειας για ενίσχυση ενεργειακής απόδοσης 88

7.4.5 Βέλτιστες πρακτικές για ολοκληρωμένα συστήματα ενεργειακής διαχείρισης και ασφάλειας 89

7.5 Οικονομική αποτίμηση της ενεργειακής αποδοτικότητας κατά τη διάρκεια κυβερνοεπιθέσεων 90

7.5.1 Κόστος και οφέλη της άμεσης ενεργειακής απόκρισης σε κυβερνοεπιθέσεις 90
7.5.2 Μακροπρόθεσμες οικονομικές επιπτώσεις των ενεργειακών απωλειών λόγω κυβερνοεπιθέσεων 91
7.5.3 Επιπτώσεις της απώλειας ενεργειακής αποδοτικότητας στη ναυτιλιακή αγορά 92

7.6 Κυβερνοασφάλεια και ενεργειακή αποδοτικότητα: Μια ολοκληρωμένη προσέγγιση 93

7.6.1 Συνεργασία κυβερνοασφάλειας και ενεργειακής διαχείρισης 93
7.6.2 Προσαρμογή πολιτικών ασφάλειας για αύξηση της ενεργειακής αποδοτικότητας 94
7.6.3 Ενεργειακά αποδοτική άμυνα έναντι κυβερνοεπιθέσεων: Σύγχρονες τάσεις 95

8 Συμπεράσματα 96

Πηγές – Βιβλιογραφία 97

Ευρετήριο Εικόνων

Εικόνα 1 - Δομή ενός Πληροφοριακού Συστήματος 13

Εικόνα 2 Υποσύστημα VTMIS (Raptis, 2018) 22

Εικόνα 3. Ηλεκτρονικά Συστήματα Απεικόνισης Χαρτών και Πληροφοριών – ECDIS (Tokyo Keiki, 2017) 24

Εικόνα 4 Σύστημα Αυτόματης Αναγνώρισης – AIS (Season Ship Management & Maritime Services, n.d.).....25

Εικόνα 5. Τα στάδια της ασφάλειας (Li et al., 2019).....28

Εικόνα 6. Συσχέτιση Βασικών Εννοιών (Μπεσαράτ, 2022) 33

Εικόνα 7. Συχνότητα Τύπων απειλών – επιθέσεων κατά των Πληροφοριακών Συστημάτων (Identity Finder, 2009) 51

Εικόνα 8. Ανάλυση Επικινδυνότητας (με πληροφορίες από Pfleeger, Pfleeger & Coles-Kemp, 2023).....54

Εικόνα 9. Ανάλυση Επικινδυνότητας Επιπτώσεις και Αντίμετρα (Σαλτσίδης, 2018). 55

Εικόνα 10. Θεραπεία κινδύνου (Καρατζάς, 2013) 59

Ευρετήριο Πινάκων

Πίνακας 1. Ενέργειες για την επαύξηση της ασφάλειας του χώρου μιας εταιρείας 29

Πίνακας 2. Επιπτώσεις των κυβερνοεπιθέσεων στις λειτουργίες των μηχανών και της πρόωσης 74

Περίληψη

Η ανάπτυξη των υπολογιστικών συστημάτων και η επέκταση του διαδικτύου έχει καθιερώσει τη χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) τόσο στην καθημερινότητα του ανθρώπου όσο και στη λειτουργία των επιχειρήσεων. Πρόσωπα και οργανισμοί αλληλοεπιδρούν μεταξύ τους, αναζητούν πληροφορίες και επιδιώκουν την διαχείρισή τους. Ο τομέας της ναυτιλίας αποτελεί έναν από τους όπου αξιοποιούνται οι ΤΠΕ.

Η ναυτιλία, είτε αφορά την διακίνηση αγαθών είτε την μεταφορά προσώπων, αποτελεί το μεγαλύτερο κεφάλαιο στην παγκόσμια οικονομία. Η τεχνολογία των πλοίων εξελίσσεται συνεχώς, οδηγώντας σε ψηφιοποιημένες διαδικασίες, αυτόματους μηχανισμούς και ενοποίηση συστημάτων. Τα Πληροφοριακά Συστήματα αναλαμβάνουν να φέρουν σε πέρας αυτές τις λειτουργίες, ενώ πρόσθετοι τομείς λειτουργικότητας αναπτύσσονται διαρκώς. Καθώς όμως, τα Πληροφοριακά Συστήματα, δικτυώνονται μεταξύ τους και αποκτούν διασύνδεση με το Διαδίκτυο, αυξάνεται και ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης ή επίθεσης μέσω κακόβουλων λογισμικών.

Η παρούσα εργασία εστιάζει στα προβλήματα ασφαλείας που μπορεί να προκύψουν στο περιβάλλον ενός πλοίου και αφορούν τα Πληροφοριακά Συστήματα που λειτουργούν σε αυτό. Προσομοιώνεται επίσης μέσω μοντέλου η κίνηση του σκάφους προκειμένου για την εύρεσης βέλτιστης διαδρομής συνυπολογίζοντας τις επικρατούσες καιρικές συνθήκες. Επιπλέον εξετάζονται ζητήματα κυβερνοεπιθέσεων στο πλοίο και αντίστοιχων αντίμετρων.

Keywords—Ναυτιλία, ασφάλεια, Πληροφοριακά Συστήματα, Πολιτικές Ασφαλείας, Ανάλυση Επικινδυνότητας, Κυβερνοεπιθέσεις, Ενεργειακή αποδοτικήτητα

Abstract

The development of computer systems and the proliferation of the internet have established the use of Information and Communication Technologies (ICT) both in the daily life of people and in the modus operandi of businesses. Individuals and organizations interact with each other, search for information and aspire to manage it. The shipping sector is one of the business areas where ICT is extensively used.

Shipping, whether concerning the transport of goods or the transportation of people, is the biggest asset in the world economy. Vessel technology is constantly evolving, leading to digitized processes, automated mechanisms and systems integration. Information Systems undertakes the task of carrying out these functionalities, while new areas of functionality are constantly added. However, as Information Systems network with each other and also gain access to the Internet, the risk of unauthorized access or attack malware- based attacks increases.

The present work deals with the security problems that may arise in the environment of a ship and concern the Information Systems that operate on it. A model vessel is used to simulate the movement of the ship, taking into account the weather conditions. Additionally, issues related to the launching of cyber-attacks against the ship, as well as the relevant countermeasures are discussed.

Keywords—Maritime; Security; Information Systems; Security policies; Risk Analysis; Cyber-Attacks; Energy efficiency

1 Εισαγωγή

Η ναυτιλία, αφορά τις μεθόδους, τις διαδικασίες και τις ενέργειες , που εφαρμόζονται προκειμένου ένα πλοίο να πραγματοποιήσει τη διαδρομή από ένα σημείο σε ένα άλλο, το ταχύτερο δυνατόν αλλά πρωτίστως με ασφάλεια. Ταυτόχρονα, αποτελεί την επιστήμη και την τέχνη της διακυβέρνησης, της πρόωσης και της φόρτωσης ενός πλοίου. Από την άλλη πλευρά, με τον όρο εμπορική ναυτιλία νοείται ο κλάδος εκείνος των μεταφορών, που πραγματεύεται την παροχή υπηρεσιών για την διακίνηση προϊόντων, αγαθών και προσώπων μέσω θαλάσσιων διαδρομών.

Η ναυτιλία ήταν για χιλιάδες χρόνια και παραμένει ως και σήμερα η ραχοκοκαλιά του παγκόσμιου εμπορίου. Η ναυτιλιακή βιομηχανία επωμίζεται τη διά θαλάσσης μεταφορά του 90% των εμπορευμάτων που διακινούνται παγκοσμίως (Afenyo, M. & Caesar, L., 2023). Για το έτος 2017, η αύξηση του όγκου των μεταφερόμενων αγαθών, ήταν της τάξης του 4%, με εκτιμώμενο όγκο που άγγιξε τους 10.7 δις τόνους (Safety for Sea, 2018).

Οι συνεχώς αυξανόμενες ανάγκες στην μεταφορά προϊόντων και αγαθών παγκοσμίως, σε συνδυασμό με το μερίδιο της ναυτιλίας στην ικανοποίηση αυτών των αναγκών, υποδεικνύουν τον κρίσιμο ρόλο της ναυτιλίας και σημαντική εξάρτησή της οικονομίας και συνακόλουθα της κοινωνίας από τη ναυτιλία.

Η ναυτιλία αξιοποιεί τις τεχνολογίες της πληροφορικής και των τηλεπικοινωνιών (ΤΠΕ/ICT) και βασίζεται σε αυτές, όπως άλλωστε συμβαίνει και με άλλα πεδία της ανθρώπινης δραστηριότητας. Η αξιοποίηση των ΤΠΕ είναι σημαντικός παράγοντας για την απλοποίηση της διαχείρισης των πόρων και των διαδικασιών, στην περιστολή του κόστους, καθώς και την αύξηση του παραγόμενου έργου αλλά και της ποιότητάς του.

Στην ναυτιλία οι τεχνολογίες ΤΠΕ βρίσκουν εφαρμογή σε λειτουργίες όπως είναι η πλοήγηση, η πρόωση, η διαχείριση φόρτου, οι επικοινωνίες ελέγχου κυκλοφορίας κ.ά.

2 Πληροφοριακά Συστήματα

Τα πληροφοριακά συστήματα κατατάσσονται σε δύο μεγάλες κατηγορίες: σε αυτά που στηρίζουν την λειτουργία τους στον ηλεκτρονικό υπολογιστή και τα χειρογραφικά. Τα περισσότερα πληροφοριακά συστήματα σήμερα, ακόμα και το μικρότερο, είναι πλέον μηχανογραφημένα, καθώς, έτσι η εταιρεία ή ο οργανισμός αποκτούν το πλεονέκτημα της αποτελεσματικής διαχείρισης.

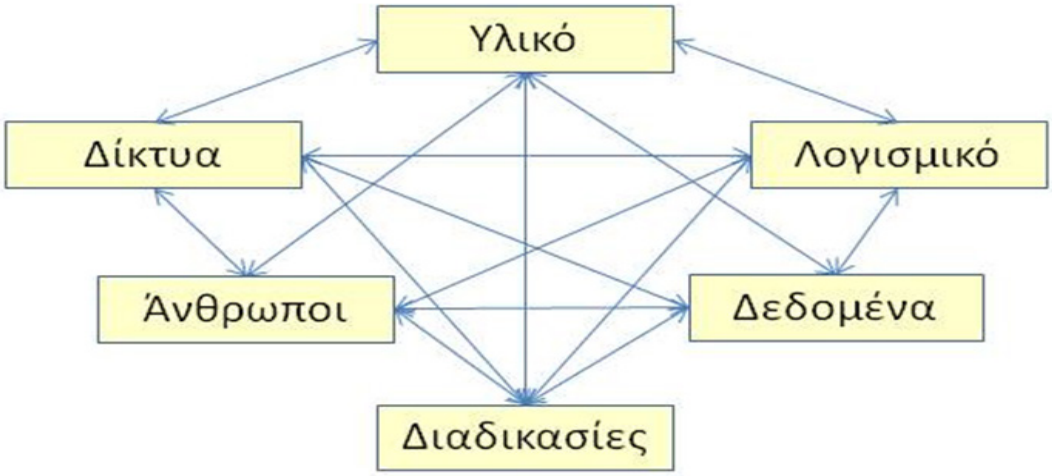
2.1 Ορισμός Πληροφοριακού Συστήματος

Ένα πληροφοριακό σύστημα είναι ένα οργανωμένο σύνολο αλληλοσχετιζόμενων τμημάτων που συναπαρτίζεται από υλικό, λογισμικό, ανθρώπους, δεδομένα και διαδικασίες. Οι παράγοντες αυτοί συνεργάζονται προκειμένου να επιτευχθεί η συλλογή, καταγραφή, αναζήτηση/ανάκτηση, επεξεργασία, τροποποίηση, αποθήκευση, ανάλυση και μετάδοση/λήψη πληροφοριών (Bidgoli, 2006). Τυπικά, τα πληροφοριακά συστήματα περιλαμβάνουν και τα δίκτυα.

Τα πληροφοριακά συστήματα μπορεί να είναι ανοιχτά ή κλειστά ανάλογα με το αν αλληλοεπιδρούν με το εξωτερικό περιβάλλον ή όχι αντίστοιχα. Στην πλειοψηφία τους είναι ανοιχτά, αφού σε αντίθετη περίπτωση και με τις ανταγωνιστικές συνθήκες που επικρατούν στην αγορά, καμιά επιχείρηση δεν θα εξασφάλιζε την μακροβιότητα της.

2.2 Δομή ενός Πληροφοριακού Συστήματος

Τα πληροφοριακά συστήματα δομούνται από διαφορετικά τμήματα τα οποία αλληλεπιδρούν μεταξύ τους ώστε να παρέχουν αξία σε μία εταιρεία ή έναν οργανισμό. Τα στοιχεία αυτά είναι έξι, (εκ των οποίων, τα τέσσερα πρώτα ανήκουν στην τεχνολογία της πληροφορικής (Information Technology)): το υλικό, το λογισμικό, το δίκτυο, τα δεδομένα, οι άνθρωποι κα οι διαδικασίες. Η δομή ενός πληροφοριακού συστήματος παρουσιάζεται στην Εικόνα 1 (Δουφεξής, 2018).



Εικόνα 1 - Δομή ενός Πληροφοριακού Συστήματος

Τα τμήματα του Πληροφοριακού συστήματος έχουν ως ακολούθως:

- Υλικό: αποτελεί βασικό συστατικό ενός πληροφοριακού συστήματος, καθώς οι δυνατότητες του καθορίζουν και τις δυνατότητες των πληροφοριακών συστημάτων. Ο όρος υλικό περιλαμβάνει τις συσκευές αλλά και τα επιμέρους τμήματα συσκευών, που διαθέτουν απτή φυσική υπόσταση. Τέτοιες συσκευές είναι:
  - Επιτραπέζιοι Ηλεκτρονικοί Υπολογιστές
  - Φορητοί Ηλεκτρονικοί Υπολογιστές
  - Κινητά Τηλέφωνα
  - Ηλεκτρονικές Ταμπλέτες
  - Συσκευές Αποθήκευσης
  - Συσκευές Εισόδου, όπως πληκτρολόγια, ποντίκια, σαρωτές
  - Συσκευές Εξόδου, όπως εκτυπωτές και ηχεία. (Bourgeois, 2014).
- Λογισμικό: είναι το σύνολο των εντολών που ελέγχουν το υλικό και τα περιφερειακά, ώστε να εκτελούν διάφορες εργασίες. Δημιουργείται μέσω της διαδικασίας του προγραμματισμού και καθιστά το υλικό λειτουργικό.

  Διακρίνεται σε δύο μεγάλες κατηγορίες:

  - Τα Λειτουργικά Συστήματα (Operating Systems) που ελέγχουν το υλικό και αποτελούν την διεπαφή μεταξύ του χρήστη και του υλικού.

- Τις Εφαρμογές (Application Software) που εξυπηρετούν τις ανάγκες του χρήστη.

- Δίκτυο: ως δίκτυο νοείται μια ομάδα διασυνδεδεμένων υπολογιστών, οι οποίοι ανταλλάσσουν μεταξύ τους πληροφορίες και πόρους. Επιπλέον, σε ένα δίκτυο υπολογιστών, υπάρχει η δυνατότητα διασύνδεσης και άλλου τύπου συσκευών εκτός από ηλεκτρονικούς υπολογιστές όπως είναι οι εκτυπωτές, οι σαρωτές κ.ά., αλλά και πλέον συσκευές του διαδικτύου των πραγμάτων. Ταξινομούνται ανάλογα με το φυσικό μέσο διασύνδεσής τους, τον τρόπο πρόσβασης σε αυτά και την γεωγραφική κάλυψη του δικτύου.
- Δεδομένα: είναι μια αναπαράσταση γεγονότων, εννοιών ή οδηγιών με έναν τρόπο κατάλληλο για επικοινωνία, ερμηνεία ή επεξεργασία από ανθρώπους ή με αυτόματα μέσα. Τα δεδομένα μπορούν να είναι ποσοτικά ή ποιοτικά. Τα ποσοτικά δεδομένα είναι αριθμητικά, όπως το αποτέλεσμα μιας μέτρησης ή μιας μαθηματικής πράξης. Τα ποιοτικά δεδομένα είναι περιγραφικού τύπου. Τα δεδομένα χρησιμοποιούνται από τα προγράμματα για τη δημιουργία, την επεξεργασία και την παρουσίαση της πληροφορίας.
- Άνθρωποι: περιλαμβάνει τους ανθρώπους που εμπλέκονται άμεσα με ένα πληροφοριακό σύστημα. Σε αυτούς ανήκουν οι άνθρωποι που οραματίστηκαν το πληροφοριακό σύστημα, το σχεδίασαν, το ανέπτυξαν, το υποστηρίζουν και αυτοί που το χρησιμοποιούν καθημερινά. Ο ανθρώπινος παράγοντας είναι κρίσιμος, καθώς αποτελεί τη βασική κινητήριο δύναμη αλλά και την κύρια αιτία εμφάνισης αποτυχιών για ένα πληροφοριακό σύστημα μπορεί. Αυτό μπορεί να οφείλεται είτε στην απουσία ικανοτήτων είτε στην αρνητική διάθεση έναντι ενός συστήματος. Από την άλλη πλευρά, σημαντικό ρόλο στην επιτυχία ενός πληροφοριακού συστήματος παίζει η εκπαίδευση του προσωπικού και ο χρόνος ώστε να εξοικειωθούν με αυτό μέσω της χρήσης του.
- Διαδικασίες: είναι μια σειρά από ανατιθέμενες εργασίες, οι οποίες συνδέονται μεταξύ τους με συγκεκριμένους κανόνες, οι οποίες αφού ολοκληρωθούν οδηγούν στην επίτευξη ενός επιχειρησιακού στόχου. Οι διαδικασίες, είναι ένα σημαντικό συστατικό για τα πληροφοριακά συστήματα, αλλά και για την εταιρική πρακτική και λειτουργία, αφού δύναται να οδηγήσουν σε επιχειρησιακό πλεονέκτημα έναντι των ανταγωνιστών. (Bourgeois, 2014).

2.3 Κατηγοριοποιήσεις Πληροφοριακών Συστημάτων

Τα πρώτα χρόνια της Πληροφορικής, όποτε υπήρχε απαίτηση για την δημιουργία ενός πληροφοριακού συστήματος για την κάλυψη ενός προβλήματος, αυτό γινόταν εντελώς εξατομικευμένα και μόνο για το συγκεκριμένο πρόβλημα. Με τον καιρό, κατέστη προφανές ότι πολλές από τις ανάγκες για συστήματα πληροφορικής παρουσίαζαν κοινά στοιχεία. Ως εκ τούτου, ξεκίνησε προσπάθεια υλοποίησης ενός ενιαίου πλαισίου που θα παρείχε απαντήσεις σ' ένα σύνολο όμοιων θεμάτων. Προς αυτή την κατεύθυνση, απαιτήθηκε πρώτα να γίνει καθορισμός των απαιτήσεων των πληροφοριακών συστημάτων, με πρώτο βήμα την προσπάθεια κατηγοριοποίησης των πληροφοριακών συστημάτων η οποία ανέδειξε τις ακόλουθες κατηγορίες:.

- Ανάλογα με το επίπεδο λειτουργίας τους:
  - Συστήματα Λειτουργικού Επιπέδου (Operational Level Systems): Υποστηρίζουν τη διεκπεραίωση των καθημερινών συναλλαγών του φορέα. Σκοπός των συστημάτων που τοποθετούνται στο λειτουργικό επίπεδο είναι η απάντηση σε τρέχοντα ερωτήματα που ακολουθούν προκαθορισμένους κανόνες κατά την λήψη αποφάσεων.
  - Συστήματα Επιπέδου Γνώσης (Knowledge Level Systems): Μερικές εταιρείες είναι πιο ανταγωνιστικές καθώς επιτυγχάνουν καλύτερα αποτελέσματα στην δημιουργία, την παραγωγή, τη διανομή και την υποστήριξη από κάποιες άλλες, αφού διαθέτουν μεγαλύτερη γνώση. Η επιχειρηματική γνώση δεν μπορεί να αντιγραφεί και αποφέρει αποτέλεσμα συνήθως σε μακροχρόνια στρατηγική.
  - Συστήματα Διοικητικού Επιπέδου (Management Level Systems): Συγκεντρώνουν και επεξεργάζονται πληροφορίες από διάφορες πηγές εντός της επιχείρησης.
  - Συστήματα Στρατηγικού Επιπέδου (Strategic Level Systems): Εφαρμόζουν την τεχνολογία της πληροφορικής σε προϊόντα και σε υπηρεσίες ή ακόμα και επιχειρηματικές δράσεις με σκοπό να αποκτήσει ο οργανισμός στρατηγικό πλεονέκτημα έναντι του ανταγωνισμού.
- Ανάλογα με τη λειτουργικότητα που προσφέρουν:
  - Συστήματα Επεξεργασίας Συναλλαγών (Transaction Processing Systems): Υποστηρίζουν καθημερινές λειτουργικές αναγκαιότητες μιας επιχείρησης και λειτουργούν με σταθερούς και προκαθορισμένους κανόνες. Συγκεντρώνουν και παρακολουθούν όλα τα δεδομένα που προκύπτουν από τις στοιχειώδεις λειτουργίες

ενός οργανισμού όπως είναι οι πωλήσεις, οι αγορές, οι καταθέσεις, οι διαχείριση των αποθηκών κ.ά. Αποτελούν το σημείο επαφής της επιχείρησης με το περιβάλλον τους.

- Πληροφοριακά Συστήματα Διοίκησης (Management Information Systems): Ασχολούνται με τη συλλογή, την επεξεργασία, την αποθήκευση και την μετάδοση πληροφοριών για χρήση από το θεσμικό όργανο λήψης αποφάσεων στο Διοικητικό Επίπεδο (Management Level) (Heidarkhani, Khomami, Jahanbazi, & Alipoor, 2013). Παρέχουν στους χρήστες δεδομένα που προέρχονται από Συστήματα Επεξεργασίας Συναλλαγών σε συγκεντρωτικές καταστάσεις με τη μορφή αναφορών, γραφικών παραστάσεων, κ.ά.
- Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems): Αποτελούν εξειδικευμένες εφαρμογές, οι οποίες χρησιμοποιώντας μεθόδους στατιστικής και πρότυπα που έχουν προκύψει μέσα από επιχειρησιακή έρευνα, αναλύουν δεδομένα, προκειμένου να υποβοηθήσουν τις διαδικασίες λήψης αποφάσεων. (Δουφεξής, 2018).
- Έμπειρα Συστήματα (Expert Systems): Αποτελούνται από υλικό και λογισμικό για την αποθήκευση γνώσης. Σκοπός είναι η διάγνωση περιπτώσεων επιχειρησιακών προβλημάτων και η εξαγωγή συμπερασμάτων, προσομοιώνοντας την ανθρώπινη εμπειρία [12]. Η συλλογή ανθρώπινης εμπειρίας και η δημιουργία μιας βάσης δεδομένων γνώσεων, προσφέρει σημαντικά πλεονεκτήματα σε μια επιχείρηση.
- Συστήματα Πληροφόρησης Ανώτατων Στελεχών (Executive Support Systems): Αποτελούν εξειδικευμένο Σύστημα Υποστήριξης Αποφάσεων τα οποία περιλαμβάνουν όλο το υλικό, το λογισμικό, τα δεδομένα, διαδικασίες και τους ανθρώπους. Παρέχουν στα υψηλόβαθμα στελέχη επιχειρήσεων και οργανισμών ειδική και συγκεκριμένη πληροφόρηση αλλά και την δυνατότητα να δημιουργούν τα ίδια πληροφορίες και να τις διανέμουν στους κατάλληλους παραλήπτες [14] (Hicks, 1993; Checkland and Holwell, 1998 in Boland. 1985).
- Συστήματα Αυτοματισμών Γραφείου (Office Automation Systems): είναι από τα πιο διαδεδομένα πληροφοριακά συστήματα. Βασίζονται σε δίκτυα Η/Υ και παρέχουν υποστήριξη στους διαχειριστές ώστε να μπορούν να διατηρούν τον έλεγχο της ροής της πληροφορίας. Το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων, η

τηλεδιάσκεψη, τα πολυμέσα, τα συστήματα ροής εργασιών κ.ά. εντάσσονται σε αυτή την κατηγορία.

2.4 Πλεονεκτήματα και Ζητήματα των Πληροφοριακών Συστημάτων

Η υιοθέτηση πληροφοριακών συστημάτων από τις επιχειρήσεις για την εύρυθμη λειτουργία παρέχει σημαντικά πλεονεκτήματα, συμπεριλαμβάνοντας τα ακόλουθα:

- Απλοποιούν καθημερινές διαδικασίες, ακόμα και τις πιο σύνθετες, οδηγώντας σε αύξηση του κύκλου εργασιών με ταυτόχρονη βελτίωση των προσφερόμενων προϊόντων ή υπηρεσιών.
- Αυξάνεται η ταχύτητα και ακρίβεια στην επεξεργασία των δεδομένων, με επακόλουθο τη μείωση του συνολικού κόστους, ενώ μειώνεται και η πιθανότητα σφάλματος καθώς υπάρχουν ενδελεχείς έλεγχοι στην εξαγόμενη πληροφορία από το ίδιο το σύστημα.
- Η επεξεργασία των δεδομένων πραγματοποιείται σε πραγματικό χρόνο. Όλα τα πληροφοριακά συστήματα που είναι συνδεδεμένα μεταξύ τους, συγχρονίζονται με τις αλλαγές την ίδια στιγμή με αποτέλεσμα την έγκαιρη πληροφόρηση των εμπλεκόμενων μερών.
- Διασφαλίζεται η ακεραιότητα και η εχεμύθεια των δεδομένων, καθώς μπορούν να εφαρμοστούν κανόνες πρόσβασης και διαδικασίες τροποποίησης της πληροφορίας.
- Επιτρέπουν την συλλογή μεγάλου όγκου δεδομένων. Το μέγεθος των αποθηκευμένων δεδομένων μπορεί να θεωρηθεί απεριόριστο αφού εξαρτάται αποκλειστικά από το φυσικό μέσο, το οποίο μπορεί εύκολα να επεκταθεί.
- Καταργούν τους χωρικούς και χρονικούς περιορισμούς στην πρόσβαση στις πληροφορίες και τη λειτουργικότητα. Αυτό ισχύει ιδιαίτερα όταν, το πληροφοριακό σύστημα συνδέεται στο διαδίκτυο.

Η υιοθέτηση πληροφοριακών συστημάτων πέρα από τα πολλά πλεονεκτήματα, έχει ως επακόλουθο και κάποια ζητήματα που χρήζουν προσοχής:

- Οι αποφάσεις που παίρνονται μέσω ενός πληροφοριακού συστήματος, λαμβάνουν υπόψη κριτήρια τα οποία στηρίζονται σε αυστηρούς κανόνες, οικονομικούς και επιχειρηματικούς

κατά κύριο λόγο. Αυτό έχει ως αποτέλεσμα την έλλειψη δημιουργικότητας στη λήψη αποφάσεων αλλά και τον αποκλεισμό άλλων παραγόντων όπως η διαίσθηση, η ενσυναίσθηση κ.λπ.

- Η εισαγωγή πληροφοριακών συστημάτων στις επιχειρήσεις και αυτοματοποίηση των διαδικασιών επέφερε μείωση των θέσεων εργασίας, χωρίς πάντοτε να υπάρχει μέριμνα για το προσωπικό που κατέστη πλεονάζον (επανεκπαίδευση, στήριξη κ.λπ.).
- Η χρήση των πληροφορικών συστημάτων απαιτεί συνεχή εκπαίδευση του προσωπικού, ιδιαίτερα για νέους χρήστες. Αυτό δημιουργεί αύξηση στις απαιτούμενες εργατοώρες με αντίκτυπο στον οικονομικό τομέα.
- Για να μπορούν να λειτουργούν αποτελεσματικά και να συμβαδίζουν με τις εξελίξεις, τα πληροφοριακά συστήματα απαιτούν συντήρηση και αναβάθμιση ανά τακτά χρονικά διαστήματα.
- Έχει δημιουργηθεί μεγάλος εξάρτησης των επιχειρήσεων από τα πληροφοριακά συστήματα. Μια διακοπή στη λειτουργία των πληροφοριακών συστημάτων θα οδηγήσει σε σημαντική υποβάθμιση ή παύση των δραστηριοτήτων της εταιρείας. Τα μεγέθη των φορέων που στηρίζουν την λειτουργία τους στα πληροφοριακά συστήματα είναι τέτοια που και μια μικρή δυσλειτουργία έχει σημαντικό κόστος και πιθανώς ορατές επιπτώσεις στο επίπεδο της κοινωνίας.

3 Πληροφοριακά Συστήματα στη Ναυτιλία

Καθώς οι ναυτιλιακές εταιρείες διαδραματίζουν σπουδαίο ρόλο στην παγκόσμια οικονομία, αναπτύσσονται μεταξύ τους σχέσεις ανταγωνισμού, ενώ παράλληλα οι συμφωνίες μεταφοράς εμπορευμάτων εμπεριέχουν ρήτρες. Κατά συνέπεια οποιαδήποτε καθυστέρηση στο πλοίο ή στο φορτίο λόγω καιρού, μηχανικής βλάβης ή ακόμα και κακού προγραμματισμού του δρομολογίου μπορεί να αποβεί αρκετά δαπανηρή για την εταιρεία.

Επιπλέον, η φύση της δομής μιας ναυτιλιακής εταιρείας, δηλαδή η ύπαρξη γραφείων ανά τον κόσμο και η ιδιαιτερότητα της παροχής υπηρεσιών σε πελάτες που βρίσκονται σε διάφορες χώρες, αυξάνουν περαιτέρω την πολυπλοκότητα των διαδικασιών. Απαιτείται συνακόλουθα η ταχεία, έγκαιρη και έγκυρη μεταφορά πληροφορίας καθώς και η διασφάλιση της συνεχούς επικοινωνίας μεταξύ των συμβαλλόμενων μελών της συμφωνίας μεταφοράς.

Για τους προαναφερθέντες λόγους, τα πληροφοριακά συστήματα είναι αναγκαία πλέον στον τομέα της Ναυτιλίας και διαμορφώνουν σε μεγάλο βαθμό τις δυνατότητες και την ανταγωνιστικότητα των οργανισμών/εταιρειών.

3.1 Κυριότερα Πληροφοριακά Συστήματα

3.1.1 Γεωγραφικά Συστήματα Πληροφοριών

Με τον όρο Γεωγραφικά Συστήματα Πληροφοριών (ΓΣΠ/GIS - Geographic Information Systems) αναφερόμαστε σε ολοκληρωμένα συστήματα τα οποία παρέχουν υπηρεσίες συλλογής, αποθήκευσης, διαχείρισης, ανάλυσης, επεξεργασίας καθώς και απεικόνισης πληροφοριών σχετικών με ζητήματα γεωγραφικής φύσης. Χρησιμοποιούνται προκειμένου να δημιουργηθούν πειραματικά μοντέλα μέσω των οποίων θα μελετηθούν διαδικασίες που αφορούν το περιβάλλον, θα αναλυθούν τάσεις, θα εκτιμηθούν και θα εξετασθούν πιθανές συνέπειες και επιπτώσεις ενός σχεδιασμού κ.ά. (Ευελπίδου & Αντωνίου, 2015)

Τα πλεονεκτήματα των ΓΣΠ, συνοψίζονται ως ακολούθως (Νικολακόπουλος, 2015; Ευελπίδου & Αντωνίου, 2015):

- Παρέχονται υπηρεσίες απεικόνισης των αποτελεσμάτων μέσω διαγραμμάτων, χαρτών κ.λπ.
- Παρέχουν εμπλουτισμένες δυνατότητες επεξεργασίας καθώς και ποιοτικής και ποσοτικής ανάλυσης δεδομένων.
- Επιτρέπουν τον ταχύ έλεγχο εναλλακτικών λύσεων.
- Υποστηρίζουν τη δημιουργία κοινού πλαισίου δραστηριοτήτων και επικοινωνίας μεταξύ χρηστών και επιστημόνων που χρησιμοποιούν τα ΓΣΠ.
- Διευκολύνουν την ενημέρωση του αποθετηρίου των δεδομένων, αλλά και την άμεση και αποτελεσματική ενσωμάτωση καινοτόμων αλγορίθμων και μεθοδολογιών ανάλυσης και επεξεργασίας.
- Επιτυγχάνουν την παροχή προηγμένων και σύνθετων μεθόδων ανάλυσης με μειωμένο κόστος.
- Παρέχουν αντικειμενικό και κοινό τρόπο ανάλυσης και παρουσίασης των αποτελεσμάτων.

Από την άλλη πλευρά, ορισμένα ζητήματα που ανακύπτουν από τη χρήση ΓΣΠ μπορούν να συνοψισθούν στα ακόλουθα (Νικολακόπουλος, 2015; Ευελπίδου & Αντωνίου, 2015):

- Υπολογίσιμο αρχικό κόστος κτήσης, συμπεριλαμβάνοντας το σύστημα καθ' εαυτό, τον εξοπλισμό, αλλά και τη δαπάνη για την τεχνική υποστήριξη και συντήρηση.
- Απαιτεί πολύ καλή εκπαίδευση των χρηστών.
- Δυσχέρειες στην ψηφιοποίηση, δηλ. στη μετατροπή των υφιστάμενων στοιχείων σε ψηφιακή αναπαράσταση.

Τα ΓΣΠ σε συνδυασμό με το Παγκόσμιο Σύστημα Στιγματοθέτησης (Global Positioning System – GPS) έδωσαν στις ναυτιλιακές εταιρείες την δυνατότητα εντοπισμού του στίγματος του πλοίου σε πραγματικό χρόνο και την παρουσίασή του τους, είτε σε δισδιάστατη απεικόνιση ή ακόμα και τρισδιάστατα (3D).

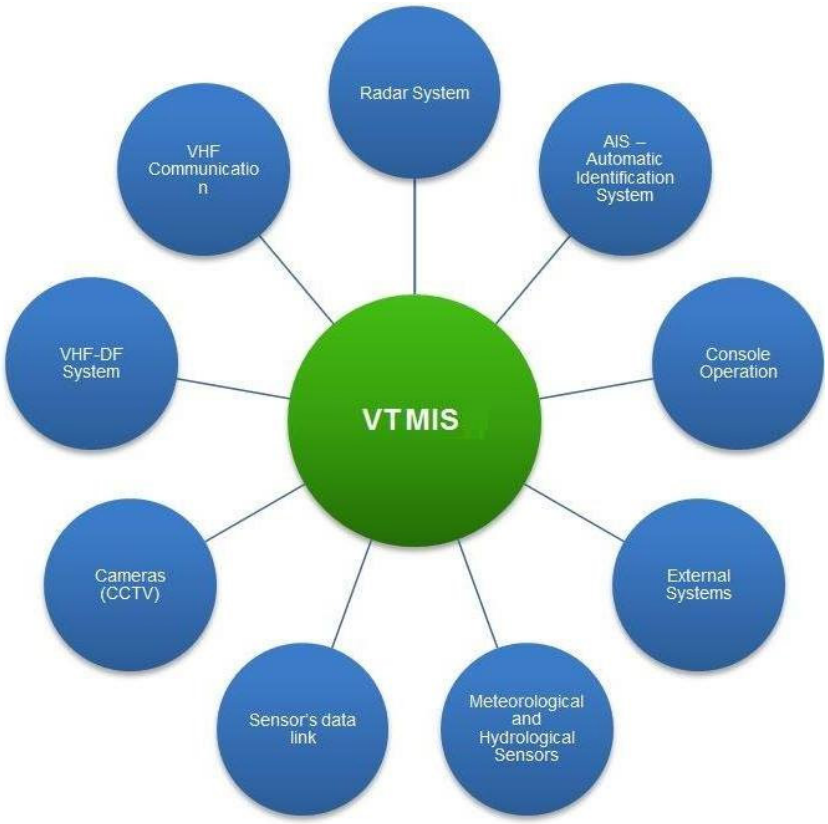
Χρησιμοποιώντας τις παραπάνω δυνατότητες σε συνδυασμό με τη διασύνδεση του ΓΣΠ με τα λοιπά πληροφοριακά συστήματα της επιχείρησης (π.χ. μετεωρολογία, αποθήκες, λογιστήριο) παρέχονται πληροφορίες στον χρήστη που θα βοηθήσουν στη λήψη κρίσιμων αποφάσεων.

3.1.2 Πληροφοριακά Συστήματα Διαχείρισης Κυκλοφορίας Σκαφών

Τα Πληροφοριακά Συστήματα Διαχείρισης Κυκλοφορίας Σκαφών (ΠΣΔΚΣ/ VTMIS - Vessel Traffic Management Information System): Τα ΠΣΔΚΣ αποτελούν επέκταση της Υπηρεσίας Κυκλοφορίας Σκαφών (Vessel Traffic Service – VTS) με τη μορφή ολοκληρωμένης θαλάσσιας επιτήρησης. Η Υπηρεσία Κυκλοφορίας Σκαφών (ΥΚΣ) έχει την δυνατότητα άμεσης επικοινωνίας με τα πλοία και αλληλεπιδρά σε περιπτώσεις θεμάτων ασφαλείας που δημιουργούνται εντός του τομέα ευθύνης τους. Η ΥΚΣ τίθεται σε λειτουργία σε επιλεγμένες περιοχές με στόχο:

- Την αναβάθμιση της ασφάλεια της ναυσιπλοΐας,
- Να προστατευθεί το θαλάσσιο περιβάλλον,
- την αποδοτικότερη κίνηση των σκαφών,
- την υποστήριξη της επιβολής του νόμου,
- την προστασία παρακείμενων υποδομών.

Το VTMIS είναι το Εθνικό Κεντρικό Σύστημα που αντλεί στοιχεία και δεδομένα από τα κατά τόπους κέντρα VTS, και, αφού γίνει η επεξεργασία τους, τα διανέμει στου ενδιαφερόμενους (Raptis, 2018). Τα στοιχεία και τα υποσυστήματα ενός VTMIS φαίνονται στην εικόνα 2.



Εικόνα 2 Υποσύστημα VTMIS (Raptis, 2018)

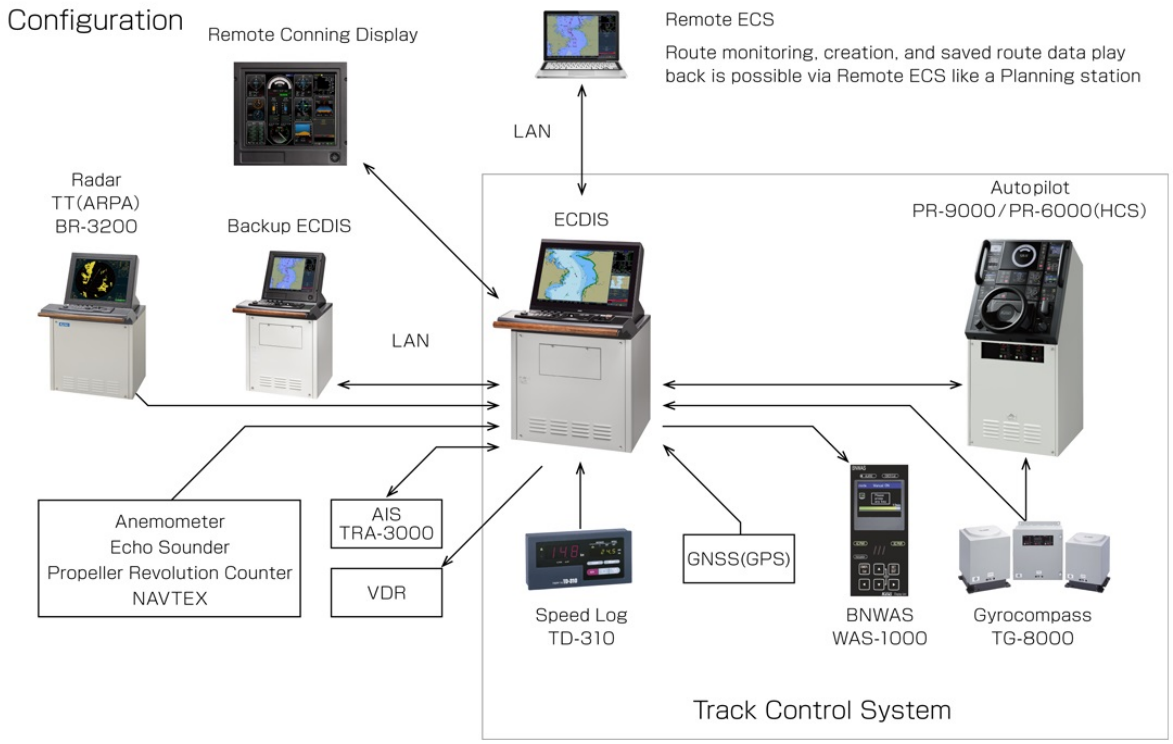
3.1.3 Ηλεκτρονικά Συστήματα Απεικόνισης Χαρτών και Πληροφοριών

Τα Ηλεκτρονικά Συστήματα Απεικόνισης Χαρτών και Πληροφοριών (ΗΣΑΧΠ/ ECDIS - Electronic Chart Display and Information Systems) είναι μηχανογραφημένα συστήματα πλοήγησης τα οποία συμμορφώνονται με το κανονιστικό πλαίσιο του Διεθνούς Οργανισμού Ναυτιλίας. Χρησιμοποιούνται σαν εναλλακτική μέθοδος έναντι της πλοήγησης με φυσικούς χάρτες. Ενσωματώνουν ένα σύνολο από πληροφορίες σε πραγματικό χρόνο και λειτουργούν ως ένα αυτοματοποιημένο βοήθημα λήψης αποφάσεων. Περιλαμβάνουν Ηλεκτρονικά Διαγράμματα Πλοήγησης (Electronic Navigation Charts – ENC) και ενσωματώνουν πληροφορίες της θέσης του πλοίου σε συνδυασμό με το GPS αλλά και με άλλα βοηθήματα πλοήγησης (radar, AIS, βυθόμετρο). Οι κύριες λειτουργίες τους συνοψίζονται στα εξής:

- Πλοήγηση: προσδιορισμός της θέσης και της πορείας του πλοίου, εκτέλεση εναλλακτικής πορείας

- Παρακολούθηση: Συνεχής έλεγχος των πληροφοριών από τις οθόνες των οργάνων και το περιβάλλον προκειμένου να ανιχνευθούν τυχόν ανωμαλίες.
- Σχεδίαση διαδρομής: προκαθορισμός της πορείας και της ταχύτητας σε σχέση με τις επικρατούσες θαλάσσιες συνθήκες και το έργο που πρέπει να εκτελεστεί.
- Παρακολούθηση διαδρομής: συνεχής παρακολούθηση διαδρομής του πλοίου σε σχέση με την προκαθορισμένη διαδρομή και τις επικρατούσες συνθήκες.
- Αποφυγή συγκρούσεων: ανίχνευση και προσδιορισμός της κίνησης σκαφών πέριξ του πλοίου. Εκτέλεση ελιγμών προς αποφυγή επικίνδυνων καταστάσεων.
- Ελιγμοί: χειρισμός του σκάφους για την επίτευξη της επιθυμητής θέσης, κατεύθυνσης και ταχύτητας.
- Ελλιμενισμός: ελιγμοί του σκάφους για την προσέγγιση στη θέση ελλιμενισμού.
- Τεκμηρίωση: καταγραφή δεδομένων και γεγονότων για στατιστικούς, επιχειρησιακούς και νομικούς λόγους.

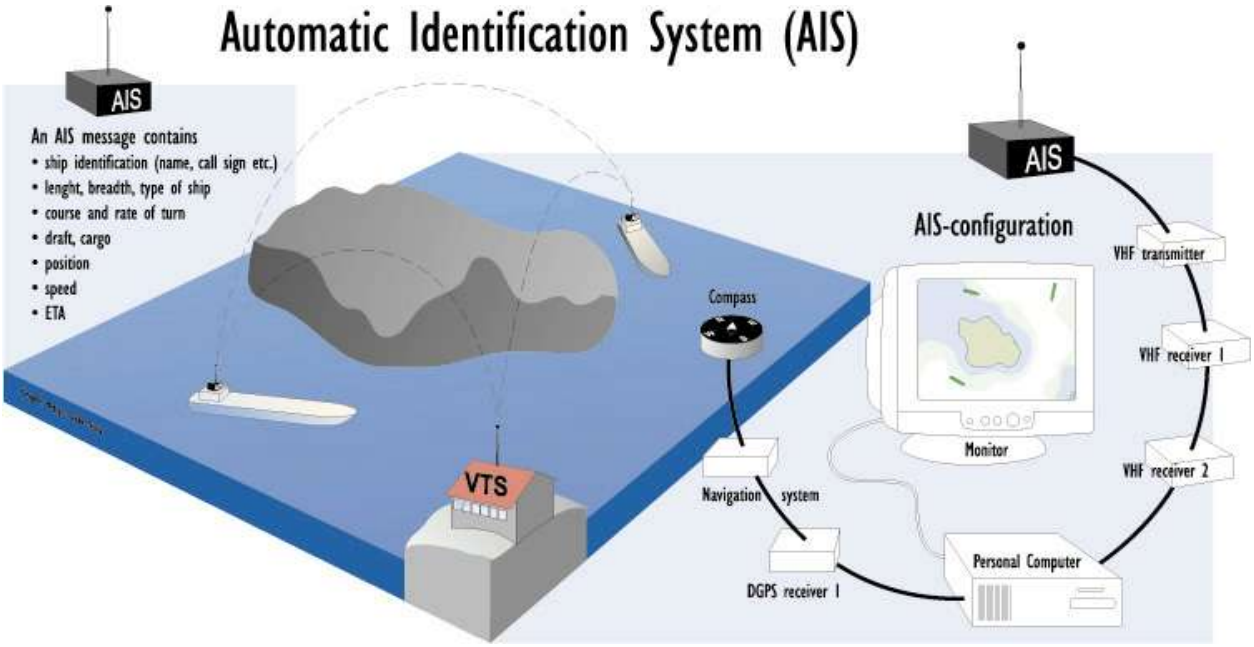
Η δυνατότητα των βοηθημάτων να απεικονίζουν άμεσα στην οθόνη των συστημάτων τις βασικές πληροφορίες πλεύσης (στίγμα, διεύθυνση πορείας, ταχύτητα) συμβάλει στην αύξηση του επιπέδου ασφάλειας της ναυσιπλοΐας, καθώς παρέχει τη δυνατότητα λήψης αποφάσεων ταχέως και με ορθότητα. Ακόμα παρέχει το πλεονέκτημα τις αποφόρτισης της έντασης στη γέφυρα οπότε το πλοίο μπορεί να λειτουργήσει αποτελεσματικά με το ελάχιστο πλήρωμα. Χαρακτηριστικό παράδειγμα αποτελεί το “Triple E Maersk”, το μεγαλύτερο πλοίο μεταφοράς containers. Με ικανότητα μεταφοράς 18000 containers και 400 μέτρα μήκος, μπορεί να λειτουργήσει με μόλις 13 άτομα πλήρωμα.(Ship technology, 2018).



Εικόνα 3. Ηλεκτρονικά Συστήματα Απεικόνισης Χαρτών και Πληροφοριών – ECDIS (Tokyo Keiki, 2017)

3.1.4 Σύστημα Αυτόματης Αναγνώρισης

Το Σύστημα Αυτόματης Αναγνώρισης (ΣΑΑ/ AIS - Automatic Identification System): Το ΣΑΑ σχεδιάστηκε με σκοπό την αποφυγή συγκρούσεων και την υποστήριξη των λιμενικών αρχών στην προσπάθεια για καλύτερο και αποτελεσματικότερο έλεγχο της θαλάσσιας κυκλοφορίας. Η λειτουργία του συστήματος στηρίζεται στους πομπούς AIS που είναι τοποθετημένοι και λειτουργούν στα πλοία. Οι πομποί περιλαμβάνουν δέκτη GPS, με τη βοήθεια του οποίου υπολογίζεται η θέση, η ταχύτητα και η πορεία του πλοίου. Επίσης, συμπεριλαμβάνεται και ένας πομπός VHF, μέσω του οποίου εκπέμπονται περιοδικά τα ανωτέρω στοιχεία. Αυτές λαμβάνονται από άλλα πλοία και παράκτιους σταθμούς βάσης. Στην περίπτωση που βρίσκονται εκτός εμβέλειας των σταθμών βάσης, τη μετάδοση αναλαμβάνουν δορυφόροι με προσαρμοσμένους ειδικούς δέκτες AIS. Οι δέκτες AIS που λαμβάνουν τα δεδομένα, τα αποστέλλουν στη συνέχεια σε μια κεντρική βάση δεδομένων. Μετά από ανάλυση και επεξεργασία των δεδομένων, γίνεται απεικόνιση στις οθόνες του συστήματος (Shine micro, 2021).



Εικόνα 4 Σύστημα Αυτόματης Αναγνώρισης – AIS (Season Ship Management & Maritime Services, n.d.)

3.1.5 Παγκόσμιο Ναυτιλιακό Σύστημα Κινδύνου και Ασφάλειας

Το Παγκόσμιο Ναυτιλιακό Σύστημα Κινδύνου και Ασφάλειας (ΠΝΣΚΑ/ GMDSS - Global Maritime Distress and Safety System) είναι ένα σύστημα παγκόσμιας κλίμακας και κάλυψης με πεδίο εφαρμογής τη ναυτιλία, με στόχο (α) να παρέχει στα πλοία κρίσιμες πληροφορίες για τη ναυτική ασφάλεια, (β) να βελτιώνει τις ραδιοεποικοινωνίες μεταξύ πλοίων αλλά και λοιπών παραγόντων της ναυσιπλοΐας, (γ) να υποστηρίζει τον συντονισμό και (δ) να καθιστά ευχερέστερο και αποτελεσματικότερο τον εντοπισμό των ναυαγών, αλλά και τη διάσωση πλοίων και αεροσκαφών. Στο πλαίσιο αυτό, το ΠΝΣΚΑ περιλαμβάνει:

i) ένα σύστημα αυτοματοποιημένων επικοινωνιών, τόσο επίγειων όσο και δορυφορικών, με χρήση συμφωνημένων πρωτοκόλλων και
ii) ένα καθορισμένο και καθολικά αποδεκτό σύνολο διαδικασιών ασφάλειας.

Πιο αναλυτικά, το ΠΝΣΚΑ συνίσταται στη διασύνδεση συστημάτων με σκοπό:

- Την άμεση ενεργοποίηση των υπηρεσιών έρευνας και διάσωσης, με παράλληλη μετάδοση των ειδοποιήσεων και πληροφοριών προς κάθε δυνητικό αποδέκτη, αξιοποιώντας το σύνολο των επίγειων και δορυφορικών συστημάτων επικοινωνιών.

- Την παροχή αυξημένων δυνατοτήτων επικοινωνιών χωρίς την απαίτηση ύπαρξης πληρώματος επιφυλακής επικοινωνιών.
- Την αυτόματη και άμεση λήψη πληροφοριών ασφαλείας ναυσιπλοΐας.
- Τη δυνατότητα άμεσης και αμφικατευθυνόμενης επικοινωνίας μεταξύ του αφ' ενός του πλοίου και αφ' ετέρου ενός σταθμού ή ενός αεροσκάφους ή ενός ετέρου πλοίου.

Για την καλύτερη διαχείριση και λειτουργία του GMDSS, η υδρόγειος έχει κατατμηθεί σε τέσσερις θαλάσσιες περιοχές, οι οποίες συμβολίζονται με Α1, Α2, Α3 και Α4. Για κάθε ζώνη έχει ορισθεί ένα σύνολο από αποδεκτούς τύπους εξοπλισμού ραδιοεπικοινωνίας, και κάθε πλοίο που ταξιδεύει εντός της περιοχής πρέπει να φέρει τον προβλεπόμενο για τη συγκεκριμένη περιοχή εξοπλισμό.

Συγκεκριμένα, για κάθε περιοχή ισχύουν τα ακόλουθα:

- Θαλάσσια περιοχή Α1 (απόσταση μικρότερη από 20 ναυτικά μίλια από τις ακτές): στις ακτές της περιοχής βρίσκονται τοποθετημένοι παράκτιοι σταθμοί πολύ υψηλής συχνότητας (VHF) οι οποίοι εκτελούν συνεχή ακρόαση Ψηφιακής Επιλογικής Κλήσης (Ψηφιακής Επιλεκτικής Κλήσης - DSC). Το πλοίο πρέπει πάντοτε να βρίσκεται εντός της εμβέλειας και σε επικοινωνία με έναν τουλάχιστον από τους σταθμούς αυτούς. Ο κύριος παράγοντας της εμβέλειας της επικοινωνίας μεταξύ πλοίου και σταθμού ξηράς είναι το ύψος στο οποίο είναι τοποθετημένος ο πομπός στον σταθμό ξηράς.
- Θαλάσσια περιοχή Α2 (απόσταση μεταξύ 20 και 100 ναυτικών μιλίων από τις ακτές): στην περίπτωση αυτή το πλοίο θα πρέπει να βρίσκεται διαρκώς εντός της ραδιοτηλεφωνική εμβέλειας τουλάχιστον ενός παράκτιου σταθμού μεσαίας συχνότητας (MF), ο οποίος τηρεί συνεχή ακρόαση Ψηφιακής Επιλογικής Κλήσης (DSC). Οι κύριοι παράγοντες που καθορίζουν την εμβέλεια της επικοινωνίας μεταξύ πλοίου και σταθμού ξηράς είναι (α) η ισχύς του πομπού και (β) οι επικρατούσες συνθήκες στην περιοχή που επηρεάζουν τη διάδοση του ραδιοτηλεφωνικού σήματος.
- Θαλάσσια περιοχή Α3 (απόσταση άνω των 100 ναυτικών μιλίων από τις ακτές, όταν το πλοίο παράλληλα παραμένει σε γεωγραφικό πλάτος μικρότερο των 70^{o} βόρεια και 70^{o} νότια): η επικοινωνία πραγματοποιείται μέσω των γεωστατικών δορυφόρων του δικτύου INMARSAT.

- Θαλάσσια περιοχή Α4 (περιοχές με γεωγραφικό πλάτος μεγαλύτερο των 70^{o} βόρεια και 70^{o} νότια). Σε αυτή την περιοχή το πλοίο πρέπει να φέρει ραδιοτηλεφωνικό εξοπλισμό HF (υψηλής συχνότητας, high frequency) με Ψηφιακή Επιλογική Κλήση (DSC).

Καθώς τα πλοία πάντοτε προσεγγίζουν τις ακτές, ένα πλοίο που ταξιδεύει σε μία περιοχή θεωρείται αυτονόητο ότι πρέπει να φέρει και τον εξοπλισμό που προβλέπεται και για τις «χαμηλότερες» περιοχές. Π.χ. ένα πλοίο που θα ταξιδέψει σε περιοχή Α3 πρέπει να φέρει και τον εξοπλισμό που είναι απαραίτητος για τις περιοχές Α2 και Α1 (IMSO.org, 2024).

4 Ασφάλεια Πληροφοριακών Συστημάτων στη Ναυτιλία

4.1 Τα στάδια της Ασφάλειας

Η Ασφάλεια Πληροφοριών (Information Security) έχει ως στόχο την προστασία των πόρων (συμπεριλαμβανομένων και των πληροφοριών) ενός πληροφοριακού συστήματος γενικότερα, από τη ζημιές που μπορούν να υποστούν, οι οποίες θα οδηγήσουν σε υποβάθμιση της αξίας τους. Η ασφάλεια μπορεί να μοντελοποιηθεί ως μία διαδικασία που περιλαμβάνει τρία διαδοχικά στάδια, την *πρόληψη*, την *ανίχνευση* και την *αντίδραση*, όπως φαίνεται στην Εικόνα 5.



Εικόνα 5. Τα στάδια της ασφάλειας (Li et al., 2019)

- Ως *πρόληψη* νοείται το στάδιο εκείνο κατά το οποίο σχεδιάζονται και υλοποιούνται μέτρα προστασίας προκειμένου να αποφευχθούν οι συνεπειών από μη επιθυμητές δραστηριότητες ή συμβάντα.
- Ως *ανίχνευση* νοείται το στάδιο εκείνο κατά το οποίο εντοπίζονται ενέργειες που επιχειρούν να προκαλέσουν ή προκάλεσαν ζημίες και αναζητούνται γεγονότα, μηχανήματα και πρόσωπα που σχετίζονται αιτιωδώς τις ενέργειες αυτές, ενώ παράλληλα εντοπίζονται οι όποιες συνέπειες που προέκυψαν ως αποτέλεσμα των ενεργειών αυτών.
- Ως *αντίδραση* νοείται (α) η διαδικασία αποκατάστασης ζημιών που επήλθαν, αποκαθιστώντας την αξία των αγαθών/πόρων που υπέστησαν ζημιά και (β) η εκτέλεση ενεργειών προκειμένου να αντιμετωπισθούν οι επιθέσεις που βρίσκονται σε εξέλιξη ώστε να μην προκληθεί ζημία ή να ελαχιστοποιηθεί η ζημιά που δύναται να προκληθεί.

Τα παραπάνω στάδια είναι όμοια ανεξαρτήτως του πεδίου εφαρμογής. Επί παραδείγματι, προκειμένου για την επαύξηση της ασφάλειας του χώρου μιας εταιρείας, τα ανωτέρω στάδια θα μπορούσαν να απεικονιστούν στις ενέργειες που παρουσιάζονται στον Πίνακα 1:

ΠΡΟΛΗΨΗ	ΑΝΙΧΝΕΥΣΗ	ΑΝΤΙΔΡΑΣΗ
Τοποθέτηση κιγκιδωμάτων στα παράθυρα	Επιθεώρηση/οπτικός έλεγχος για διαπίστωση απουσίας εξοπλισμού (π.χ. λόγω κλοπής)	Κλήση της αστυνομίας
Τοποθέτηση κλειδαριάς ασφαλείας	Τοποθέτηση και λειτουργία συστήματος συναγερμού	Χρήση ασφαλιστικής κάλυψης
Ανέγερση/τοποθέτηση φράκτη	Τοποθέτηση, λειτουργία και επόπτευση κλειστού κυκλώματος τηλεόρασης (CCTV)	Σύναψη σύμβασης με εταιρία φύλαξης

Πίνακας 1. Ενέργειες για την επαύξηση της ασφάλειας του χώρου μιας εταιρείας

Μεταφέροντας τα παραπάνω στο πλαίσιο των πληροφοριακών συστημάτων, μπορούμε να καταγράψουμε ότι οι στόχοι της ασφάλειας στις Τ.Π.Ε. είναι οι ακόλουθοι:

- **Προστασία Υπολογιστικών Συστημάτων (Computer Security)**, η οποία αναφέρεται στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης, αποκάλυψης, διαρροής, φθοράς, αλλοίωσης, διαγραφής ή καταστροφής, τόσο εκούσιας όσο και ακούσιας. Η προστασία καλύπτει τόσο τη φάση της επεξεργασίας, όσο και της αποθήκευσης. Επιπρόσθετα, εξασφαλίζεται και η διαθεσιμότητα των πόρων, ήτοι η δυνατότητα των κατάλληλα εξουσιοδοτημένων χρηστών να προσπελαύνουν, χρησιμοποιούν και να τροποποιούν τους πόρους για τους οποίους τους έχουν παραχωρηθεί σχετικά δικαιώματα, σύμφωνα με την πολιτική ασφάλειας.
- **Προστασία Επικοινωνιών (Communication Security)**, η οποία είναι η είναι η προφύλαξη των τηλεπικοινωνιακών/δικτυακών πόρων, με την παράλληλη διαφύλαξη των δεδομένων από ακούσια ή εκούσια διαρροή, αποκάλυψη, παραφθορά, τροποποίηση, διαγραφή ή καταστροφή κατά τη μετάδοσή τους, μέσω δικτύων υπολογιστών. Επιπρόσθετα, περιφρουρείται και η δυνατότητα των κατάλληλα εξουσιοδοτημένων μερών να κάνουν χρήση της δικτυακής υποδομής προκειμένου για την υλοποίηση της

επικοινωνίας, Η προστασία των επικοινωνιών αφορά όλους τους τύπους δικτύων, π.χ. ενσύρματα και ασύρματα δίκτυα. Παράλληλα διασφαλίζεται και η δυνατότητα των εξουσιοδοτημένων οντοτήτων να χρησιμοποιήσουν τις δικτυακές επικοινωνίες, , σύμφωνα με τα οριζόμενα στην πολιτική ασφάλειας.

Η προστασία και προφύλαξη δεδομένων και πόρων ανάγεται σε τρεις (3) θεμελιώδεις διαστάσεις της Ασφάλειας, οι οποίες έχουν ως εξής:

- **Εμπιστευτικότητα (Confidentiality)**, η οποία αναφέρεται στην προστασία των πόρων (συμπεριλαμβανομένης της πληροφορίας) από τη μη εξουσιοδοτημένη πρόσβαση σε αυτούς, είτε άμεσα είτε έμμεσα (δηλ. μέσω διαρροής).
- **Ακεραιότητα (Integrity)**, η οποία αναφέρεται στην προστασία των πόρων από μη εξουσιοδοτημένη μεταβολή (τροποποίηση ή διαγραφή) τους. Η διατήρηση της ακεραιότητας επιβάλει την τροποποίηση των δεδομένων μόνο από εξουσιοδοτημένες οντότητες και μόνον μέσα από καλά ορισμένες και εγκεκριμένες διαδικασίες.
- **Διαθεσιμότητα (Availability)**, η οποία αναφέρεται στη διασφάλιση της δυνατότητας των εξουσιοδοτημένων χρηστών και εν γένει οντοτήτων να χρησιμοποιήσουν τους πόρους (είτε για ανάγνωση είτε για τροποποίηση) απρόσκοπτα, εντός του πλαισίου που καθορίζεται (Μαυρίδης, 2015) από την πολιτική ασφάλειας.
- **Μη αποποίηση (Non-Repudiation)**, αφορά την παροχή εγγυήσεων για τη σύνδεση υποκειμένων με τις πράξεις τους με ικανό βαθμό βεβαιότητας, υποστηρίζοντας τον καταλογισμό ευθύνης σε συγκεκριμένα πρόσωπα για πράξεις και ενέργειες που πραγματοποιήθηκαν εντός του συστήματος.

Προκειμένου για την επίτευξη των ανωτέρω διαστάσεων, τα συστήματα τεχνολογιών πληροφορικής και τηλεπικοινωνιών πρέπει να ενσωματώνουν το σύνολο των ακόλουθων μηχανισμών:

- **Αναγνώριση (Identification)**, η οποία αναφέρεται στη πλαίσιο αναγνώρισης ενός υποκειμένου από το σύστημα (π.χ. οι χρήστες αναγνωρίζονται μέσω των ονομάτων χρήστη). Το υποκείμενο δύναται να είναι άνθρωπος ή τρίτο σύστημα.
- **Αυθεντικοποίηση (Authentication)**, η οποία αναφέρεται στη πλαίσιο διακρίβωσης από το σύστημα της ταυτότητας του υποκειμένου με το οποίο συνδιαλέγεται. Για παράδειγμα

η διαπίστωση της ταυτότητας ενός χρήστη μπορεί να γίνεται με το όνομα χρήστη και το συνθηματικό.

- **Εξουσιοδότηση (Authorization)** , η οποία αναφέρεται στη πλαίσιο λήψης απόφασης σχετικά με το εάν μία ενέργεια που ζητείται από τον χρήστη θα ικανοποιηθεί ή θα απορριφθεί. Η απόφαση λαμβάνεται εξετάζοντας (α) τα αποτελέσματα της διαδικασίας αυθεντικοποίησης, (β) το αντικείμενο επί του οποίου ζητείται η ενέργεια, (γ) το είδος της ενέργειας και (δ) το σχήμα δικαιωμάτων πρόσβασης στο αντικείμενο.

Η ασφάλεια οφείλει να βρίσκεται στον πυρήνα του σχεδιασμού και της υλοποίησης για κάθε έργο ΤΠΕ. Στη συνέχεια καταγράφονται οι βασικοί ορισμοί ασφάλειας, οι οποίοι είναι απαραίτητοι προκειμένου να υπάρχει κοινό πλαίσιο αναφοράς μεταξύ όλων των εμπλεκομένων (Μαυρίδης, 2015).

4.2 Βασικοί Ορισμοί Ασφάλειας

Στη συνέχεια γίνεται αναφορά σε βασικούς όρους που αφορούν ζητήματα ασφαλείας πληροφοριών και επικοινωνιών:

- **Αγαθό (Asset):** πρόκειται για κάθε πόρο (π.χ. υλικό, λογισμικό ή δεδομένα) που ανήκει σε έναν **ιδιοκτήτη** (Owner) και διαθέτει **αξία** (Value) για αυτόν. Λόγω της ύπαρξης αξίας, το αγαθό θα πρέπει να προστατεύεται προκειμένου να αποφευχθεί απομείωση της αξίας αυτής.
- **Προνόμιο / δικαίωμα (privilege) χρήσης** είναι η τυπική **εκχώρηση** (grant) άδειας, δυνάμει κάποιας επίσημης πολιτικής, σε έναν χρήστη ή σε μία ενεργή οντότητα (υπολογιστή) που δρα για λογαριασμό του χρήστη ώστε να εκτελεί πρόσβαση (access) σε πόρους. Το προνόμιο συνήθως εκχωρείται από τον ιδιοκτήτη του αντικειμένου, ωστόσο σε ορισμένες περιπτώσεις η αρμοδιότητα παραχώρησης ανήκει στον διαχειριστή του συστήματος ή σε ειδικά προς τούτο εξουσιοδοτημένες οντότητες.
- Οι **κίνδυνοι (dangers)** αποτελούν απειλές για τα αγαθά που μπορούν -εάν πραγματοποιηθούν- να οδηγήσουν σε απομείωση της αξίας τους και τη συνακόλουθη πρόκληση **ζημιάς** (harm).
- Ως **απειλή** (threat) νοείται η περίσταση που ενέχει την πιθανότητα να προκληθούν απώλειες ή ζημιές, συμπεριλαμβάνοντας την **υποκλοπή** (interception), την τροποποίηση,

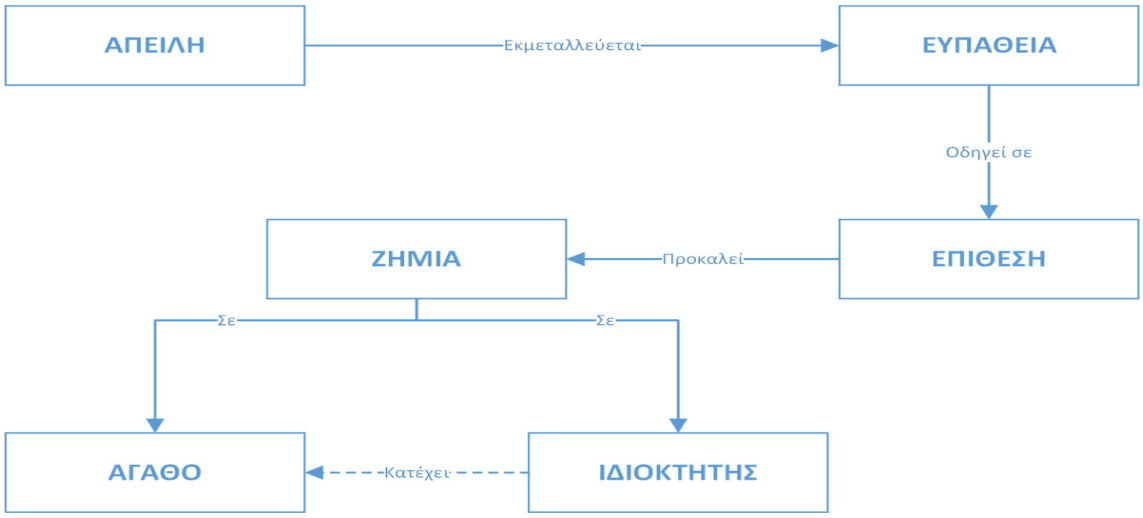
την πλαστογράφηση, ή την παύση της λειτουργίας. Οι απειλές διακρίνονται στις ακόλουθες κατηγορίες:

- Φυσικές απειλές, οι οποίες σχετίζονται με τη φύση των συστημάτων ή με το περιβάλλον εντός του οποίου εγκαθίστανται και τίθενται σε λειτουργία.
- Εκούσιες απειλές, οι οποίες σχετίζονται με κακόβουλες πράξεις που πραγματοποιούνται εκ προθέσεως. Οι πράξεις δύνανται να εκτελούνται είτε από νομότυπους χρήστες του συστήματος, είτε από μη νομότυπους χρήστες (δηλ. χρήστες που στερούνται εξουσιοδότησης).
- Ακούσιες απειλές, οι οποίες σχετίζονται με εσφαλμένες (ακούσιες) πράξεις των χρηστών (Μαυρίδης, 2015).

- Οι **ζημίες** προκύπτουν ως συνέπειες **επιθέσεων** (attacks). Μια επίθεση περιλαμβάνει την αξιοποίηση ευπαθειών (vulnerabilities) του συστήματος. Μία **ευπάθεια** (vulnerability) είναι ένα κενό στην ασφάλεια του συστήματος, το οποίο δύναται να οφείλεται σε κακή ρύθμιση, παρωχημένο/ευάλωτο αλγόριθμο ή μηχανισμό κ.λπ. Οι σημαντικότερες κατηγορίες ευπαθειών είναι οι ακόλουθες:
  - **Ευπάθειες που ανάγονται στον ανθρώπινο παράγοντα (Human):** μπορεί να αφορούν είτε (α) κακόβουλους χρήστες, οι οποίοι εκούσια/εσκεμμένα επιτίθενται στο σύστημα με στόχο να επιφέρουν παραβίαση (και συνακόλουθα ζημιά), είτε (β) χρήστες που θα προξενήσουν παραβίαση/ζημιά χωρίς να έχουν σχετική πρόθεση (ακούσια), συνήθως λόγω άστοχου χειρισμού.
  - **Ευπάθειες που ανάγονται στο υλικό και το Λογισμικό:** οι ευπάθειες αυτές δύνανται να ανάγονται σε ζητήματα πλημμελειών στην κατασκευή ή/και πλημμελειών/σφαλμάτων στη ρύθμιση ή/και εσφαλμένη λειτουργία της μίας συνιστώσας υλικού ή λογισμικού του συστήματος.
  - **Ευπάθειες που ανάγονται στα μέσα (media):** οι ευπάθειες αυτές αφορούν ευαλωτότητες σε μηχανισμούς ή διαδικασίες ασφάλειας, η εκμετάλλευση των οποίων μπορεί να οδηγήσει σε ζημιά στα μέσα (π.χ. τους μαγνητικούς δίσκους), όπως λ.χ. την απόσπασή τους από τα υπολογιστικά συστήματα/τα συστήματα αποθήκευσης ή τη φυσική τους καταστροφή (π.χ. θραύση).

- **Ευπάθειες που ανάγονται στις επικοινωνίες (Communications):** οι ευπάθειες αυτές αφορούν θέματα των καναλιών επικοινωνίας, όπως π.χ. ζητήματα με την κατασκευή τους, ημιβέλιστη/μη ασφαλή ρύθμιση, έκθεση κ.τ.λ.
- **Ευπάθειες που ανάγονται στη φυσική/υλική διάσταση (Physical):** οι ευπάθειες αυτές αφορούν κυρίως τον φυσικό χώρο όπου πραγματοποιείται η εγκατάσταση και η θέση σε λειτουργία των συστημάτων (π.χ. τα υπολογιστικά κέντρα).
- **Ευπάθειες που ανάγονται στη φύση και τα φυσικά φαινόμενα (Natural):** οι ευπάθειες αυτές αφορούν φυσικά φαινόμενα όπως π.χ. πυρκαγιές, τυφώνες, κ.ο.κ.

Οι συνέπειες μιας επιτυχούς επίθεσης εκδηλώνονται κυρίως ως υποβάθμιση της αξίας των περιουσιακών στοιχείων ή/και ως προσωρινή δυσλειτουργία έως και διακοπή της λειτουργίας του συστήματος. Η αντιμετώπιση των σχετικών απειλών επιτυγχάνεται μέσω σχεδιασμού και εφαρμογής μέτρων προστασίας (controls) ή αντίμετρων (countermeasures), τα οποία περιλαμβάνουν ιδίως προληπτικές παρεμβάσεις τεχνικού και οργανωτικού χαρακτήρα, με στόχο τον περιορισμό ή την εξάλειψη της έκθεσης που προκύπτει λόγω γνωστών ευπαθειών του συστήματος (Μαυρίδης, 2015).



Εικόνα 6. Συσχέτιση Βασικών Εννοιών (Μπεσαράτ, 2022)

Καθώς η εφαρμογή μέτρων όλων των κατηγοριών (πρόληψη, ανίχνευση, αντίδραση) ενέχει κόστος, είναι δυνατόν να ορισθεί ότι συνολικότερος στόχος της ασφάλειας είναι η επίτευξη κατάλληλης εξισορρόπησης μεταξύ του κόστους που επέρχεται λόγω της εφαρμογής των μέτρων

και του ενδεχομένου πρόκλησης ζημιάς στα αγαθά λόγω των κινδύνων και των ευπαθειών, που δύνανται εν τέλει να οδηγήσουν σε επιτυχείς επιθέσεις (Μαυρίδης, 2015).

4.3 Ζητήματα Ασφάλειας στο Διαδίκτυο

Ένα δίκτυο απαρτίζεται από (α) διασυνδεδεμένες υπολογιστικές συσκευές, οι οποίες διαθέτουν τη δυνατότητα ανταλλαγής δεδομένων, και (β) και τους διαύλους που υλοποιούν τη διακίνηση των δεδομένων. Τα δίκτυα υλοποιούνται με στόχο να παρέχεται στους χρήστες η δυνατότητα διαμοιρασμού των πόρων και κοινής πρόσβασης σε υπηρεσίες. Πολλαπλά δίκτυα δύνανται να διασυνδέονται, οδηγώντας έτσι σε περιβάλλοντα διαδικτύου (Μαυρίδης, 2015). Ένα περιβάλλον διαδικτύου μπορεί να λειτουργεί ως ένα ενιαίο δίκτυο, ενώ οι επί μέρους δικτυακές συνιστώσες του δύνανται να είναι ανομοιογενείς. Στο διαδίκτυο εμφανίζονται ζητήματα ασφάλειας, μερικά από τα πιο βασικά εξ αυτών σχετίζονται την αντιμετώπιση απειλών, όπως:

- Πλαστοπροσωπία (masquerading): Πρόκειται για την περίπτωση κατά την οποία ένας μη εξουσιοδοτημένος χρήστης επιχειρεί, μέσω αντιποίησης ταυτότητας, να παρακάμψει τους μηχανισμούς ελέγχου πρόσβασης και να αξιοποιήσει πόρους του συστήματος προσποιούμενος έναν νόμιμα εξουσιοδοτημένο χρήστη.
- Παθητική παρακολούθηση (passive tapping): Προκύπτει όταν ο επιτιθέμενος προβαίνει σε καταγραφή των διακινούμενων δεδομένων, απομαστεύοντάς τα από τα κανάλια μετάδοσης, με σκοπό τη μετέπειτα χρήση τους, συμπεριλαμβάνοντας και την ανάλυση.
- Ενεργός παρακολούθηση (active tapping): Προκύπτει όταν ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία και δεν περιορίζεται στην υποκλοπή, αλλά προβαίνει στην τροποποίηση ή παραφθορά των δεδομένων ή την εισαγωγή πλαστογραφημένων δεδομένων.
- Αποποίηση (repudiation): Προκύπτει όταν μία κατάλληλα εξουσιοδοτημένη οντότητα αρνείται ότι έχει συμμετάσχει σε μία πράξη που έλαβε χώρα στο σύστημα (π.χ. δημιουργία ενός εγγράφου), παρ' ότι όντως έχει συμμετάσχει.
- Άρνηση εξυπηρέτησης (denial of service): Προκύπτει όταν η επιτιθέμενη οντότητα δημιουργεί συνθήκες αυξημένης κατανάλωσης πόρων, με στόχο να υποβαθμίσει την ομαλή λειτουργία συστήματος, έως μερικές φορές την πλήρη παύση της λειτουργίας του.

- Επανεκπομπή μηνυμάτων (replay): Συμβαίνει όταν η επιτιθέμενη οντότητα υποκλέπτει και καταγράφει μηνύματα, και σε μεταγενέστερα χρονικά σημεία τα επανεκπέμπει (π.χ. για να πετύχει μη εξουσιοδοτημένη σύνδεση).
- Ανάλυση επικοινωνίας (traffic analysis): Αποτελεί μορφή παθητικής παρακολούθησης, ακόμη και σε περιβάλλοντα με κρυπτογραφημένα δεδομένα, με στόχο τη μελέτη των προτύπων κυκλοφορίας και διακίνησης της πληροφορίας. Μέσω της ανάλυσης αυτών των μοτίβων μπορούν να εξαχθούν έμμεσα συμπεράσματα, τα οποία ενδέχεται να αξιοποιηθούν για την προετοιμασία επόμενης επίθεσης.
- Κακόβουλο λογισμικό (viruses, Trojan horses, worms): Πρόκειται για λογισμικό που ο επιτιθέμενος επιδιώκει να εκτελεστεί από νόμιμα εξουσιοδοτημένους χρήστες ή συστήματα, με στόχο την υποκλοπή δεδομένων, την πρόκληση άρνησης εξυπηρέτησης ή, γενικότερα, την εκτέλεση περαιτέρω επιθέσεων.

Η αποτελεσματική αντιμετώπιση των ανωτέρω θεμάτων αποτελεί βασικό προαπαιτούμενο για την ανάπτυξη των υπηρεσιών του Διαδικτύου και την αποδοχή τους από τους χρήστες. Σε αντίθετη περίπτωση, ενδέχεται να προκύψουν σοβαρές επιπτώσεις, όπως:

- *Αποκάλυψη πληροφοριών:* Οφείλεται σε παραβίαση της εμπιστευτικότητας και οδηγεί στη διαρροή μέρους ή του συνόλου διαβαθμισμένων ή ευαίσθητων δεδομένων που τηρούνται σε ένα πληροφοριακό σύστημα προς μη εξουσιοδοτημένες οντότητες.
- Αλλοίωση πληροφοριών: Προκύπτει από την υποβάθμιση ή/και απώλεια της ακεραιότητας των δεδομένων και οφείλεται σε μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή μέρους ή του συνόλου της πληροφορίας που τηρείται σε ένα πληροφοριακό σύστημα.
- Άρνηση Εξυπηρέτησης: Στις διαδικτυακές υπηρεσίες, η μη εξυπηρέτηση εκδηλώνεται είτε ως συνολική αποτυχία παροχής εξυπηρέτησης, είτε ως υποβάθμιση της ποιότητας υπηρεσίας (π.χ. η υπέρμετρη αύξηση του χρόνου απόκρισης), και καταλήγει στην αδυναμία χρήσης του συστήματος από τους νόμιμα εξουσιοδοτημένους χρήστες. Η απώλεια διαθεσιμότητας συνεπάγεται αύξηση κόστους, είτε με τη μορφή της άμεσης πτώσης κερδών/αδυναμία εκπλήρωσης των στόχων του οργανισμού λόγω της έλλειψης δυνατότητας χρήσης της υπηρεσίας, είτε ως έμμεσα προκύπτουσα απώλεια λόγω διαρροής των χρηστών προς εναλλακτικές υπηρεσίες που προσφέρονται από τον ανταγωνισμό.

- Δυσφήμηση: Το διαδικτυακό περιβάλλον είναι έντονα ανταγωνιστικό, και η φήμη των υπηρεσιών συνιστά ένα πρωτεύον κριτήριο επιλογής. Περιστατικά υποβάθμισης της ασφάλειας διαδίδονται με ταχύτητα και προκαλούν αρνητική φήμη (δυσφήμηση) και απώλεια μελλοντικών ή υφιστάμενων χρηστών.
- Κόστος: Οι συνέπειες των συμβάντων ασφάλειας οδηγούν στην αύξηση του κόστους, είτε λόγω της δυσφήμησης είτε λόγω των απαιτήσεων για ανάταξη των ζημιών και την υλοποίηση αντιμέτρων, είτε λόγω κυρώσεων που δύνανται να καταλογιστούν από τις αρχές που έχουν τη σχετική αρμοδιότητα, π.χ. δικαστικό σύστημα ή εποπτικές αρχές.

Οι συνέπειες που αναφέρονται παραπάνω καθιστούν σαφή την αυξημένη σημασία της ασφάλειας. Προκειμένου να αποφευχθούν οι συνέπειες θα πρέπει να κατανοηθούν και να εφαρμοστούν κατάλληλα μέθοδοι και τεχνολογίες που δύνανται να ενισχύσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Οι μέθοδοι και τεχνολογίες αυτές καλούνται αντίμετρα και χωρίζονται σε 4 ευρείες κατηγορίες:

i) Πρόληψη: η εφαρμογή αντιμέτρων έχει ως στόχο την ελάττωση του κινδύνου.
ii) Διασφάλιση: επιχειρείται η παροχή εγγυήσεων ότι τα εφαρμοζόμενα αντίμετρα παραμένουν αποτελεσματικά.
iii) Ανίχνευση: καταβάλλεται προσπάθεια για έγκαιρο εντοπισμό, περιστολή και αντιμετώπιση περιστατικών.
iv) Επαναφορά: μέτρα και διαδικασίες που αποσκοπούν (α) στην ταχεία επάνοδο σε ασφαλή κατάσταση κατόπιν περιστατικών διάρρηξης της ασφαλείας και (β) στη διερεύνηση των αιτίων που οδήγησαν στη διάρρηξη.

Για την αποτελεσματική υλοποίηση της πολιτικής ασφάλειας, το σχέδιο ασφάλειας οφείλει να ενσωματώνει σαφείς διαδικασίες συνεχούς παρακολούθησης και αξιολόγησης, μέσω τακτικών επισκοπήσεων και επιθεωρήσεων. Με τον τρόπο αυτό καθίσταται δυνατή η έγκαιρη αναθεώρησή του, ώστε να παραμένει διαρκώς επικαιροποιημένο σε σχέση με τις τεχνολογικές εξελίξεις και τις οργανωτικές αλλαγές.

Ένα ολοκληρωμένο σχέδιο ασφάλειας πρέπει επίσης να περιλαμβάνει αναλυτικό σχέδιο αντιμετώπισης έκτακτων καταστάσεων, το οποίο να καλύπτει τόσο την ανάκαμψη από καταστροφή (disaster recovery plan) όσο και την αποκατάσταση της λειτουργίας (contingency

action plan). Η ενσωμάτωση μηχανισμών ασφάλειας σε ένα πληροφοριακό σύστημα αποτελεί ένα σύνθετο, απαιτητικό και πολυδιάστατο έργο (Μαυρίδης, 2015).

4.4 Μεθοδολογία Υλοποίησης Πολιτικών Ασφάλειας

Η ανάπτυξη μιας ολοκληρωμένης πολιτικής ασφάλειας και η υλοποίηση ενός πλήρους συστήματος ασφάλειας πληροφοριών προϋποθέτει την ακολουθία συγκεκριμένων σταδίων, τα οποία συνολικά διακρίνονται σε πέντε φάσεις.

4.4.1 Φάση 1: «Καταγραφή υφιστάμενης κατάστασης»

Στη φάση αυτή πραγματοποιείται η αποτύπωση της υπολογιστικής και επικοινωνιακής υποδομής της επιχείρησης, δηλαδή η καταγραφή του συνόλου των περιουσιακών της στοιχείων (assets). Τα περιουσιακά στοιχεία ενός οργανισμού μπορούν να κατηγοριοποιηθούν ως εξής (Λέρα, 2012):

- **Δεδομένα (Data assets):** Περιλαμβάνουν κάθε μορφή πληροφορίας, από δεδομένα προσωπικού χαρακτήρα που αποθηκεύονται σε βάσεις δεδομένων έως και εγγραφές σε εξυπηρετητές, όπως ένας DNS server.
- **Υπηρεσίες (End User Services):** Αφορούν τις υπηρεσίες που επιτρέπουν στους τελικούς χρήστες την πρόσβαση στα δεδομένα, όπως για παράδειγμα οι υπηρεσίες πρόσβασης σε βάσεις δεδομένων.
- **Υλικά στοιχεία:** Περιλαμβάνουν τον υλικοτεχνικό εξοπλισμό του πληροφοριακού συστήματος, όπως υπολογιστές, δίκτυα και μέσα αποθήκευσης.
- **Τοποθεσίες:** Αφορούν τους φυσικούς χώρους του οργανισμού, όπως δωμάτια, κτίρια ή οικόπεδα, στους οποίους φιλοξενούνται τμήματα των πληροφοριακών συστημάτων.
- **Λογισμικό (software):** Περιλαμβάνει τις εφαρμογές και τον πηγαίο κώδικα, ιδιαίτερα σε οργανισμούς που αναπτύσσουν λογισμικό, όπου η προστασία του είναι κρίσιμης σημασίας.

Μετά την καταγραφή της υφιστάμενης κατάστασης, ακολουθεί η ανάλυση των πληροφοριακών διαδικασιών που υποστηρίζουν τη λειτουργία της επιχείρησης, καθώς και ο προσδιορισμός του ρόλου των χρηστών μέσω της κατάταξής τους σε κατηγορίες. Παράλληλα, καταγράφονται όλες οι διαδικασίες που σχετίζονται με την ασφάλεια του πληροφοριακού συστήματος και πραγματοποιείται αξιολόγηση τόσο των επιμέρους στοιχείων όσο και των υφιστάμενων μέτρων

προστασίας. Τέλος, εξετάζονται οι ιδιαιτερότητες του πληροφοριακού συστήματος, με ιδιαίτερη έμφαση στη διαχείριση και προστασία των ευαίσθητων προσωπικών δεδομένων που τηρεί η επιχείρηση.

4.4.2 Φάση 2: «Ανάλυση επικινδυνότητας»

Από τη στιγμή που στην προηγούμενη φάση έχουν καταγραφεί τα περιουσιακά στοιχεία (assets) του οργανισμού και έχει διενεργηθεί αποτίμηση της αξίας τους, προχωράμε στην παρούσα φάση στην ανάλυση της επικινδυνότητας, η οποία έχει αυξημένη σημασία αναφορικά με τη διαμόρφωση της πολιτικής ασφάλειας που θα υιοθετήσει και θα εφαρμόσει η εταιρεία προκειμένου να προστατεύσει τα πληροφορικά της συστήματα και εν γένει τα αγαθά της. Στη φάση αυτή πραγματοποιείται (α) ανάλυση των κινδύνων στους οποίους είναι εκτεθειμένο το σύστημα, (β) προσδιορισμός των ευπαθειών (vulnerabilities) και (γ) προσδιορισμός των απειλών προς το σύστημα, λαμβάνοντας υπ' όψιν το τρέχον πλαίσιο ελέγχου (control). Εξετάζοντας λεπτομερέστερα τη φάση της ανάλυσης επικινδυνότητας, έχουμε τα ακόλουθα βήματα:

- Βήμα 1ο: Προσδιορισμός των απειλών (threats) που υφίστανται έναντι του πληροφοριακού συστήματος. Για κάθε στοιχείο εντοπίζονται και καταγράφονται οι απειλές που υφίστανται γι' αυτό και θέτουν σε κίνδυνο την αξία του, ενώ καταγράφεται για κάθε στοιχείο και το σύνολο των επιπτώσεων που συσχετίζονται με κάθε απειλή.
- Βήμα 2ο: Προσδιορισμός ευπαθειών (vulnerabilities) ανά περιουσιακό στοιχείο. Ένα περιουσιακό στοιχείο μπορεί να εμφανίζει κυμαινόμενους βαθμούς ευπάθειας σε διαφορετικές απειλές. Θα πρέπει να πραγματοποιηθεί ξεχωριστή εκτίμηση των ευπαθειών και του βαθμού έκθεσης ανά στοιχείο και ανά κίνδυνο.
- Βήμα 3ο: Αναγνώριση των ενδεχόμενων ειδών απωλειών (losses) λόγω των επιπτώσεων. Η σύνταξη του καταλόγου διενεργείται με βάση τον βαθμό κινδύνου, ο οποίος, όπως αναφέρθηκε, υπολογίζεται ξεχωριστά για κάθε περιουσιακό στοιχείο και για κάθε απειλή. Στον υπολογισμό συνεκτιμάται το σύνολο των επιπτώσεων που σχετίζονται με μία απειλή, η αξία του στοιχείου, καθώς και οι ευπάθειές του που μπορεί να αξιοποιηθούν από τους παράγοντες της απειλής.
- Βήμα 4ο: Η εκτίμηση των πιθανοτήτων να προκύψουν απώλειες. Σε συνέχεια των αντιστοιχίσεων των απειλών με περιουσιακά στοιχεία, διενεργείται εκτίμηση των

πιθανοτήτων να εκδηλωθεί επίθεση σε έκαστο περιουσιακό στοιχείο. Συμπληρωματικά καταγράφεται ο βαθμός της ευπάθειας του στοιχείου προς τη συγκεκριμένη απειλή.

- Βήμα 5ο: Προσδιορισμός των προσηκόντων αντίμετρων (counter measures) προκειμένου να αντιμετωπιστούν οι κίνδυνοι. Στο πλαίσιο αυτό ο οργανισμός εξετάζει τα ακόλουθα ενδεχόμενα:
    - *Αποφυγή κινδύνου*, η οποία πραγματοποιείται με απόσυρση του πόρου από τη συγκεκριμένη επιχειρησιακή δράση/υπηρεσία (ή τη συνολική κατάργηση της υπηρεσίας)
    - *Αποδοχή κινδύνου*, ήτοι δεν λαμβάνεται κανένα μέτρο και η επιχειρησιακή δράση/υπηρεσία συνεχίζει κανονικά τη λειτουργία της,
    - *Μετριασμός κινδύνου*, με εφαρμογή αντιμέτρων. Προσδιορίζονται τα κατάλληλα αντίμετρα και το κόστος που συσχετίζεται με κάθε ένα από αυτά (οικονομικό, τεχνικό, ανθρώπινο).
- Βήμα 6ο: Κατάρτιση και εφαρμογή ενός αποτελεσματικού και οικονομικά αποδοτικού (cost effective) συστήματος ασφάλειας. Είναι ενδεχόμενο έτσι να έχουμε αποδοχή κινδύνου, π.χ. διότι ο κίνδυνος θεωρείται αμελητέος ή διότι το κόστος εφαρμογής αντιμέτρων υπερβαίνει την ωφέλεια. Επίσης είναι δυνατό να επιλεγεί μία λύση με μικρότερο βαθμό μείωσης του κινδύνου αλλά και χαμηλότερο κόστος, αν κριθεί ότι η επένδυση σε πιο αποτελεσματικές λύσεις δεν δικαιολογεί το αυξημένο κόστος τους.

Πέραν της αρχικής κατάρτισης του συστήματος ασφάλειας, απαιτείται διαρκής παρακολούθηση της εξέλιξης των κινδύνων, των απειλών, των ευπαθειών και των αγαθών, καθώς όλα αυτά τα στοιχεία τελούν υπό διαρκή αναθεώρηση. Ειδικότερα, μπορεί (ενδεικτικά) να εισαχθούν νέα αγαθά στη διαμόρφωση του συστήματος, να προκύψουν νέες απειλές, να διαγνωστούν πρόσθετες ευπάθειες, να εισαχθούν νέα είδη αποτελεσματικών αντίμετρων ή παλαιότερα αντίμετρα να αποδειχθούν αναποτελεσματικά.

Η ανάλυση επικινδυνότητας για ένα πληροφοριακό σύστημα πρέπει να χαρακτηρίζεται από πληρότητα, ήτοι να έχουν συνεκτιμηθεί όλα τα στοιχεία και οι απειλές που αφορούν την ασφάλεια του Π.Σ., συμπεριλαμβάνοντας (α) τις υπολογιστικές υποδομές, (β) τη δικτυακή υποδομή, (γ) το επίπεδο της φυσικής πρόσβασης στο σύστημα και συνακόλουθα τη φυσική ασφάλειά του. Αντίστοιχα, κατατάσσονται σε κατηγορίες οι απειλές, ανάλογα με το είδος τους/τα αποτελέσματά

τους. Ενδεικτικές κατηγορίες είναι η διείσδυση στις επικοινωνίες (communication infiltration), η διείσδυση σε επίπεδο λογικής (logical infiltration), οι αστοχίες σε επίπεδο υλικού/εξοπλισμού (equipment failure) και οι φυσικές απειλές (Physical Threats) π.χ. πυρκαγιά, σεισμός κ.τ.λ.

Ιδιαίτερο βάρος δίδεται στην κατηγορία της διείσδυσης σε επίπεδο λογικής, η οποία εξετάζει τις πληροφορίες που επεξεργάζεται και διαχειρίζεται το πληροφοριακό σύστημα και την προστασία που θα πρέπει να παρέχεται σε αυτές. Στο πλαίσιο αυτό αναλύονται τα προγράμματα/οι εφαρμογές που χρησιμοποιούνται, τα δεδομένα (αρχεία δεδομένων, βάσεις δεδομένων κ.λπ.) αλλά και οι σχετιζόμενες διαδικασίες με εμπλοκή στελεχών του οργανισμού. Η διείσδυση στις επικοινωνίες είναι επίσης σημαντική κατηγορία, καθώς μέσω του δικτύου μπορεί να υπάρχει διαρροή δεδομένων/πληροφοριών, υποκλοπή συνθηματικών, επιθέσεις στο σύστημα ή λοιπές παραβιάσεις. Τέλος, η φυσική ασφάλεια είναι σημαντική διάσταση, εξετάζοντας τη συνέχεια των υπηρεσιών σε περίπτωση δυσμενών φυσικών φαινομένων ή αστοχιών υλικού. Συνολικά, ο στόχος της ανάλυσης επικινδυνότητας είναι να προληφθούν οι ζημιές, να μειωθεί η έκθεση των πόρων σε κινδύνους και να μετριαστεί το ενδεχόμενο διακοπής της επιχειρησιακής δραστηριότητας του οργανισμού.

4.5 Φάση 3: «Πολιτική ασφαλείας»

Ο στόχος της πολιτικής ασφάλειας είναι να παρέχονται κατευθύνσεις, καθώς και κατάλληλη υποστήριξη, για θέματα που αφορούν την ασφάλεια των πληροφοριών. Ο καθορισμός της πολιτικής ασφάλειας είναι αρμοδιότητα της διοίκησης της εταιρείας/του οργανισμού, και η διοίκηση θα πρέπει να επιδεικνύει δέσμευση και αποφασιστικότητα στην εφαρμογή του. Η εμβέλεια της πολιτικής περιλαμβάνει θέματα ασφαλείας που διατέμνουν το σύνολο των επιπέδων του οργανισμού. Με άλλα λόγια, η τρέχουσα φάση ενσωματώνει δράσεις καταγραφής και κατάρτισης πλαισίων, κανονισμών, διαδικασιών και πρακτικών: το σύνολο των στοιχείων αυτών καθορίζουν τον τρόπο με τον οποίο (α) πραγματοποιείται η διαχείριση των αγαθών του οργανισμού, (β) παρέχεται προστασία για τα αγαθά του οργανισμού, και (γ) πραγματοποιείται η κατανομή των αγαθών του του οργανισμού, σε όλη την έκταση του οργανισμού. Στο πλαίσιο αυτό:

1. Διακρίνονται τα στοιχεία της πολιτικής αφ’ ενός σε *υποκείμενα* (subjects), τα οποία περιλαμβάνουν τα ενεργά στοιχεία του συστήματος, όπως για παράδειγμα χρήστες και

διεργασίες (processes) και αφ' ετέρου σε *αντικείμενα* (objects), όπως π.χ. δεδομένα, συστήματα αρχείων, κάθε είδους συσκευές (αποθήκευσης, δικτυακής επικοινωνίας κ.ο.κ.).

2. Ανατίθενται ρόλοι και αρμοδιότητες, μέσω των οποίων προκύπτουν τα δικαιώματα που τα υποκείμενα θα έχουν στα αντικείμενα, ενώ προάγεται και η αποτελεσματική διαχείριση της ανάθεσης των δικαιωμάτων.

Προκειμένου να διασφαλιστεί η πληρότητα, η συνέπεια και η αποτελεσματικότητα της πολιτικής, είναι σκόπιμο να ακολουθούνται σχετικά διεθνή πρότυπα, όπως π.χ. τα TCSEC και ITSEC. Συνοψίζοντας, μία πολιτική ασφαλείας θα ενσωματώνει τις ακόλουθες ενότητες:

- Αγαθά,
- Ρόλοι και αρμοδιότητες,
- Στόχοι της πολιτικής ασφάλειας,
- Εμβέλεια της πολιτικής ασφαλείας,
- Κατευθύνσεις, συμβουλές εφαρμογής και οδηγίες,
- Νομοθεσία, λοιπές πολιτικές και κουλτούρα ασφάλειας,
- Υλοποίηση και εφαρμογή της πολιτικής ασφάλειας, με διαδικασίες και μηχανισμούς για εγρήγορση και ενημέρωση των χρηστών, προβλέψεις για την απαρέγκλιτη εφαρμογή της πολιτικής (enforcement) και προβλέψεις για ανίχνευση και αντιμετώπιση παραβιάσεων,
- Επιθεώρηση της πολιτικής, ανασκόπηση των αποτελεσμάτων και αναθεώρηση της πολιτικής

Θεωρείται σκόπιμο οι κανόνες να διατυπώνουν ένα γενικό πλαίσιο αρχών ασφάλειας για τον οργανισμό/την εταιρεία, χωρίς να εισάγονται τεχνικοί όροι (εκτός αν είναι απαραίτητο), διατηρώντας πλήρη σαφήνεια και μεριμνώντας για την εφικτότητα της εφαρμογής τους. Επιπλέον, θα πρέπει να υπάρχει δυνατότητα γενίκευσης και επέκτασης των κανόνων. Οι κανόνες στη συνέχεια εξειδικεύονται, λαμβάνοντας υπ' όψιν τα αποτελέσματα της ανάλυσης επικινδυνότητας.

4.5.1 Φάση 4: «Καθορισμός Μέτρων Ασφαλείας»

Η φάση του καθορισμού μέτρων ασφάλειας έχει ως αντικείμενο την υλοποίηση του Σχεδίου Ασφαλείας. Στο πλαίσιο αυτό οι ειδικοί σχεδιάζουν τα μέτρα που θα ανταποκρίνονται στις απαιτήσεις ασφαλείας του συστήματος. Τα μέτρα που θα καταρτιστούν θα πρέπει να καλύπτουν τις ακόλουθες διαστάσεις (Λέρα, 2012):

- Ζητήματα οργάνωσης και διαχείρισης της ασφάλειας του συστήματος,
- Ζητήματα ασφάλειας αναφορικά με την ανάπτυξη και τη συντήρηση του συστήματος,
- Ζητήματα που άπτονται της φυσικής ασφάλειας του συστήματος,
- Ζητήματα που άπτονται της ασφάλειας των δεδομένων,
- Ζητήματα που αφορούν την υπολογιστική και τηλεπικοινωνιακή υποδομή, επί της οποίας εκτελείται το σύστημα.

Πιο αναλυτικά, τα μέτρα που άπτονται της οργάνωσης και της διαχείρισης του συστήματος εστιάζουν (α) στον σχεδιασμό της ασφάλειας του συστήματος, (β) σε κώδικες δεοντολογίας της επιχείρησης, (γ) σε μέτρα που αφορούν τον την κατόπτευση, την εξέταση της αποτελεσματικότητας και την έκταση συμμόρφωσης με την πολιτική ασφάλειας του συστήματος. Επιπλέον, στις εξεταζόμενες διαστάσεις εντάσσονται οι ρόλοι και οι αρμοδιότητες στον τομέα της διαχείρισης της ασφάλειας.

Τα μέτρα που άπτονται της ασφάλειας ανάπτυξης και της συντήρησης του συστήματος ενσωματώνουν (α) μέτρα που διέπουν την ανάπτυξη και τη συντήρησης εφαρμογών, (β) μέτρα που διέπουν τη διαχείριση καθώς και τις φάσεις υποστήριξης για το υλικό και το λογισμικό από προμηθευτές, (γ) μέτρα που άπτονται της απογραφής λογισμικού και υλικού, καθώς και της διαχείρισης των μεταβολών των διαμορφώσεων.

Εξετάζονται επίσης μέτρα για τη διάσταση της φυσικής ασφάλειας, συγκαταλέγοντας (α) μέτρα που άπτονται της φυσικής ασφάλειας των κτηρίων και άλλων κτηριολογικών εγκαταστάσεων, (β) μέτρα που άπτονται τις ασφάλειας του εξοπλισμού ICT (υποδομής υπολογιστικών και τηλεπικοινωνιακών συστημάτων). Συγκαταλέγονται επίσης μέτρα που άπτονται της προστασίας έναντι φυσικών καταστροφών.

Εξετάζονται επίσης μέτρα για τη διάσταση της ασφάλειας των δεδομένων συγκαταλέγοντας (α) μέτρα για την υλοποίηση μηχανισμών διασφάλισης της ακεραιότητας και της εμπιστευτικότητας των δεδομένων και (β) μέτρα που άπτονται της κατηγοριοποίησης και ταξινόμησης (classification) των δεδομένων.

Αναφορικά με τη διάσταση της ασφάλειας των υποδομών (υπολογιστικών και τηλεπικοινωνιακών), εδώ εντάσσονται μέτρα που αφορούν (α) διαδικασίες για τη διαχείριση

εφεδρικών αντιγράφων, (β) προσεγγίσεις για την ανίχνευση και ανάσχεση ιών, (γ) προσεγγίσεις και μέτρα για τη διαχείριση συνθηματικών και ελέγχου για την πρόσβαση στα υποσυστήματα του πληροφοριακού συστήματος, καθώς και καταλογογράφησης/τεκμηρίωσης περιστατικών ασφάλειας, (γ) μέτρα που άπτονται της ασφάλειας εφαρμογών, αποθετηρίων δεδομένων, δικτυακών συνδέσεων και υποδομών καθώς (δ) μέτρα που αφορούν την ασφάλεια των συνδέσεων στο διαδίκτυο. Ο βαθμός αποτελεσματικότητας που εμφανίζουν τα μέτρα προστασίας καθώς και α αντίμετρα εξαρτάται την ορθότητα του τρόπου χρήσης τους. Βασικά στοιχεία που λαμβάνονται υπ' όψιν σε αυτό το πλαίσιο είναι:

- Κατανόηση της έκτασης των ζητημάτων από τους χρήστες που εμπλέκονται.
- Η σχεδίαση και ο προγραμματισμός επισκοπήσεων σε περιοδική βάση, καθώς και δράσεων αξιολόγησης και αναθεώρησης των μέτρων.
- Συμπληρωματικότητα των μέτρων.
- Αλληλοεπικάλυψη των μέτρων. Ένα μείγμα μέτρων που υλοποιεί την αρχή της άμυνας σε βάθος (defense in depth) παρέχει υψηλότερα επίπεδα προστασίας για το σύστημα.
- Θέματα ευκολίας χρήσης και αποδοχής από τους χρήστες, τα οποία είναι κεφαλαιώδους σημασίας για την υιοθέτησή τους και συστηματική εφαρμογή τους.

Επιπρόσθετα, στη φάση του καθορισμού μέτρων ασφάλειας καταρτίζεται το σχέδιο υλοποίησης που ενσωματώνει και την κατανομή αρμοδιοτήτων στο πλαίσιο της εκτέλεσης συγκεκριμένων εργασιών, προκειμένου να ολοκληρωθεί η υλοποίηση του συνόλου των μέτρων ασφάλειας. Το σχέδιο υλοποίησης περιλαμβάνει και σχετικό χρονοπρογραμματισμό.

4.5.2 Φάση 5: «Σχέδιο έκτακτης ανάγκης»

Το Σχέδιο Έκτακτης Ανάγκης είναι απαραίτητο προσάρτημα του συνολικού σχεδίου ασφάλειας και περιλαμβάνει αποτύπωση των διαδικασιών που πρέπει να ακολουθηθούν σε περίπτωση εμφάνισης έκτακτης ανάγκης. Το σχέδιο αυτό αφορά τις περιπτώσεις καταστάσεων όπου η επαναφορά του συστήματος σε λειτουργική κατάσταση εντός εύλογου χρονικού πλαισίου θα είναι ανέφικτη (Λέρα, 2012).

Το σχέδιο έκτακτης ανάγκης περιλαμβάνει μέτρα για τα εξής ενδεχόμενα:

α) σοβαρή δυσλειτουργία του συστήματος (συμπεριλαμβάνοντας και μείζονες παραβιάσεις της ασφάλειας),

β) ολική καταστροφή, συμπεριλαμβάνοντας ενδεχομένως απώλεια των φυσικών υποδομών.

και για κάθε μία εκ των περιπτώσεων συγκαταλέγονται τα ακόλουθα:

- Ο προσδιορισμός ενδεχόμενων κινδύνων, καθώς και συγκεκριμένα κριτήρια που θα πρέπει να πληρούνται για να ενεργοποιηθεί το σχέδιο και η εφαρμογή των σχετικών μέτρων. Τα κριτήρια πρέπει να είναι σαφή και εγγράφως καταγεγραμμένα. Είναι σκόπιμο να υπάρχουν και κριτήρια και διαδικασίες για εγκατάλειψη της εφαρμογής του σχεδίου αλλά και την αναθεώρησή του.
- Καταγραφή των λειτουργιών του συστήματος που κρίνονται ως κεφαλαιώδους σημασίας, καθώς και προσδιορισμός των συστημάτων που τις υποστηρίζουν.
- Εναλλακτικά συστήματα/τρόποι λειτουργίας που θα υποστηρίζουν τις λειτουργιών του συστήματος που κρίνονται ως κεφαλαιώδους σημασίας.
- Ιεραρχική ταξινόμηση των λειτουργιών, ανάλογα με τη σημασία τους, και καθορισμός κριτηρίων για τη θέση τους σε λειτουργία σε εναλλακτικά συστήματα.
- Λεπτομερής καταγραφή των στρατηγικών προστασίας που εφαρμόζονται,
- Σχέδιο υλοποίησης του σχεδίου εκτάκτου ανάγκης, στο οποίο (α) καταγράφεται χρονοπρόγραμμα για τις ενέργειες και (β) κατανέμονται αρμοδιότητες ενεργειών στο προσωπικό. Στο σχέδιο πρέπει να περιλαμβάνονται όλες οι απαραίτητες πληροφορίες για την εκτέλεση των δραστηριοτήτων (στοιχεία για τους εργαζόμενους που θα εμπλακούν, αρχές που θα ειδοποιηθούν, ειδικοί, πελάτες και προμηθευτές που θα ενημερωθούν ή που θα κληθούν να συνδράμουν κ.λπ.).

Για την αντιμετώπιση μείζονων καταστροφών τυπικά χρησιμοποιείται και εφεδρική εγκατάσταση (Disaster Recovery Center), το οποίο συνήθως βρίσκεται σε απομακρυσμένη τοποθεσία για λόγους αντοχής σε φυσικές καταστροφές (Λέρα, 2012). Οι σχετικές πληροφορίες και διαδικασίες πρέπει να εντάσσονται στο σχέδιο αντιμετώπισης έκτακτης ανάγκης.

5 Απειλές-Τρωτότητες συστημάτων του πλοίου και διαδικασία ζημιογόνων γεγονότων

5.1 Απειλές και κίνδυνοι πληροφοριακών συστημάτων και ανάλυση ζημιογόνων γεγονότων

Η εκτίμηση κινδύνου για την ασφάλεια των πληροφοριακών συστημάτων ενσωματώνει διαδικασίες, οι οποίες συγκεκριμενοποιούνται για κάθε οργανισμό. Τυπικά, οι οργανισμοί κατά την φάση της αξιολόγησης του κινδύνου εξετάζουν πιθανά περιστατικά ασφαλείας. Στη ναυτιλία, εν αντιθέσει με άλλους τομείς, δεν υπάρχουν διαθέσιμα ιστορικά και στατιστικά στοιχεία που αφορούν ανάλογα περιστατικά ή υπάρχουν σε πολύ περιορισμένη έκταση.

Η ανάλυση των περιστατικών επιθέσεων στον τομέα της ναυτιλίας αλλά και σε άλλους επιχειρηματικούς τομείς έχει αναδείξει ότι αρκεί μία επιτυχημένη επίθεση για να οδηγηθούμε σε απώλεια σημαντικών υπηρεσιών που παρέχει μία εταιρεία/ένας οργανισμός. Προκειμένου για τον έλεγχο (control) των κινδύνων αλλά και της λειτουργίας ενός συστήματος πληροφοριών, οι διαχειριστές και οι χρήστες πρέπει να τελούν εν γνώσει των τρωτών σημείων του συστήματος και των απειλών που ενδέχεται να τις αξιοποιήσουν.

5.2 Τύποι επιθέσεων

Γενικά, διακρίνονται δύο τύποι επιθέσεων, που ενδέχεται να επηρεάσουν τη λειτουργία μιας εταιρείας ή ενός πλοίου, ως εξής:

α) επιθέσεις χωρίς στόχευση, όπου τα συστήματα, οι υπηρεσίες και τα δεδομένα μιας ναυτιλιακής εταιρείας ή ενός πλοίου είναι πιθανοί στόχοι που επιλέγονται χωρίς συγκεκριμένα κριτήρια.

β) επιθέσεις με στόχευση, όπου τα συστήματα, οι υπηρεσίες και τα δεδομένα μιας ναυτιλιακής εταιρείας ή ενός οργανισμού επιλέγονται επί τούτου ως στόχοι.

Οι συχνότεροι παράγοντες απειλής για τα πληροφοριακά συστήματα ενός πλοίου συνοψίζονται στις ακόλουθες παραγράφους.

5.2.1 Δυσαρεστημένοι Εργαζόμενοι

Εργαζόμενοι που έχουν δυσαρεστηθεί ενδέχεται να επιφέρουν ζημιές σε ένα σύστημα. Οι εργαζόμενοι διαθέτουν υψηλό βαθμό εξοικειωσης με τα συστήματα και τα προγράμματα της εταιρείας που τους απασχολεί, και συνακόλουθα έχουν αυξημένη πιθανότητα να γνωρίζουν τις ενέργειες που δυνητικά θα προξενούσαν αυξημένη ζημιά.

Οι δυσαρεστημένοι εργαζόμενοι διαθέτουν πρόσβαση σε ευαίσθητες πληροφορίες και συστήματα, γεγονός που τους καθιστά επικίνδυνους αν επιλέξουν να ενεργήσουν κακόβουλα. Μπορούν να διαγράψουν σημαντικά δεδομένα, να εγκαταστήσουν κακόβουλες εφαρμογές ή να παραχωρήσουν πρόσβαση σε εξωτερικούς επιτιθέμενους, προκαλώντας σοβαρές ζημιές στη λειτουργία του πλοίου και στην ασφάλεια των πληροφοριών. Λόγω αυτής της απειλής, είναι ουσιώδες οι ναυτιλιακές εταιρείες να θέτουν σε εφαρμογή αυστηρά μέτρα ασφαλείας, όπως ελεγχόμενη πρόσβαση σε κρίσιμα συστήματα, διαρκή παρακολούθηση των ενεργειών των υπαλλήλων και διαδικασίες άμεσης αντίδρασης σε περίπτωση ανίχνευσης ύποπτης δραστηριότητας.

5.2.2 Κακόβουλοι Χάκερς

Οι χάκερς αποτελούν μια αληθινή και υπαρκτή απειλή με αυξημένη γνώση σε δικτυακά διασυνδεδεμένα συστήματα πληροφορικής. Οι χάκερ μπορούν να εισέλθουν μέσω του δικτύου σε υπολογιστικά συστήματα και να απειλήσουν την ιδιωτικότητα και την ακεραιότητα των δεδομένων προτού καν ανιχνευθεί η μη εξουσιοδοτημένη πρόσβαση.

Οι κακόβουλοι χάκερς συχνά αξιοποιούν προηγμένες μεθόδους για να παρακάμψουν τα μέτρα ασφάλειας, όπως επιθέσεις phishing, κοινωνική μηχανική και εκμετάλλευση κενών ασφαλείας λογισμικού. Αφού αποκτήσουν πρόσβαση, είναι ικανοί να υποκλέψουν ευαίσθητα δεδομένα, να διαταράξουν τη σωστή λειτουργία των συστημάτων ή να μπλοκάρουν την πρόσβαση και να απαιτήσουν λύτρα για την αποκατάστασή της. Η παραπάνω απειλή ενισχύει την ανάγκη για αποτελεσματικές άμυνες στον κυβερνοχώρο, όπως τακτική ανανέωση του λογισμικού, χρήση ισχυρών κωδικών πρόσβασης και αδιάλειπτη παρακολούθηση των δικτύων για ενέργειες πέραν των συνηθισμένων, ώστε να προλαμβάνονται και να αντιμετωπίζονται έγκαιρα οι επιθέσεις αυτές.

5.2.3 Βιομηχανική Κατασκοπεία

Η βιομηχανική κατασκοπεία πραγματοποιείται με τη συγκέντρωση στοιχείων βιομηχανικής ιδιοκτησίας από ιδιωτικές εταιρείες ή δημόσιους φορείς προς όφελος άλλης επιχείρησης ή οργανισμού.

Η βιομηχανική κατασκοπεία μπορεί να γίνει με διάφορους τρόπους, όπως η είσοδος σε υπολογιστικά δίκτυα για την κλοπή εμπορικών μυστικών, ή παράνομη απόκτηση σχεδίων και τεχνικών πληροφοριών, ή ακόμη και η στρατολόγηση υπαλλήλων που διαθέτουν πρόσβαση σε ευαίσθητες πληροφορίες. Αυτή η μορφή παρακολούθησης μπορεί να προκαλέσει σοβαρή απώλεια ανταγωνιστικού πλεονεκτήματος, δεδομένου ότι οι πληροφορίες που συλλέγονται μπορεί να αξιοποιηθούν για την παραγωγή ανταγωνιστικών προϊόντων ή για τη λήψη στρατηγικών αποφάσεων που βλάπτουν την επιχείρηση-στόχο. Η αποτροπή αυτών των κινδύνων απαιτεί αποτελεσματικά μέτρα ασφάλειας, όπως η κρυπτογράφηση πληροφοριών, η αυστηρή ρύθμιση πρόσβασης και η τακτική εξέταση των συστημάτων ασφαλείας για ανίχνευση πιθανών παραβιάσεων.

5.2.4 Εξωτερική Κυβερνητική Κατασκοπεία

Σε ορισμένες περιπτώσεις υφίστανται απειλές που προέρχονται από κυβερνητικές υπηρεσίες άλλων κρατών. Πέρα από την πιθανή οικονομική κατασκοπεία, ξένες υπηρεσίες έχουν τη δυνατότητα να στοχεύουν συστήματα για να επεκτείνουν τη γνώση τους για τον στόχο.

Η εξωτερική κυβερνητική κατασκοπεία συνήθως περιλαμβάνει τη χρησιμοποίηση εξελιγμένων τεχνικών και πόρων, που είναι διαθέσιμοι μόνον σε κρατικούς φορείς, για την παρακολούθηση, την κλοπή δεδομένων ή την παρέμβαση σε βασικές υποδομές. Οι επιθέσεις αυτές μπορεί να είναι δυσχερές να ανιχνευθούν και να αποτραπούν, εξαιτίας της τεχνολογικής υπεροχής και της πολυπλοκότητας των εργαλείων που αξιοποιούνται. Επιπλέον, οι συγκεκριμένες επιχειρήσεις συχνά επιδιώκουν όχι μόνο άμεσο κέρδος, αλλά και στρατηγική αξιοποίηση πληροφοριών, παράμετρος που μπορεί να οδηγήσει σε μακροπρόθεσμες συνέπειες στην εθνική ασφάλεια ή στη γεωπολιτική σταθερότητα. Η διαχείριση αυτών των κινδύνων προϋποθέτει διεθνή συνεργασία, αυστηρά μέτρα κυβερνοασφάλειας και συνεχή εκπαίδευση του προσωπικού στις βέλτιστες πρακτικές για την ασφάλεια των πληροφοριακών συστημάτων.

5.2.5 Σφάλματα και Παραλείψεις

Οι χρήστες, οι εργαζόμενοι που καταχωρούν δεδομένα, οι διαχειριστές του συστήματος και οι προγραμματιστές, συχνά κάνουν ακουσίως σφάλματα που συμβάλλουν άμεσα ή/και έμμεσα στην εμφάνιση ζητημάτων ασφαλείας.

Τα σφάλματα και οι παραλείψεις λόγω ανθρώπινου παράγοντα μπορούν να προκαλέσουν σοβαρές αδυναμίες στα πληροφοριακά συστήματα ενός πλοίου. Τα σφάλματα μπορεί να αφορούν λανθασμένη εισαγωγή πληροφοριών, αδυναμία εντοπισμού και επίλυσης ενός τεχνικού ζητήματος, ή ακόμα και εσφαλμένες ρυθμίσεις ασφάλειας κ.λπ. Σε κάθε περίπτωση, τα ανθρώπινα σφάλματα μπορούν να δημιουργήσουν ευκαιρίες για κακόβουλες επιθέσεις ή να προκαλέσουν σοβαρές βλάβες στη λειτουργία. Αυτά τα σφάλματα, αν και μη εσκεμμένα, μπορεί να προκαλέσουν απώλεια πληροφοριών, διακοπή στις διαδικασίες ή ακόμα και οικονομικές ζημίες. Αυτός είναι ο λόγος που είναι απαραίτητο να υπάρχει διαρκής εκπαίδευση και ενημέρωση των υπαλλήλων, καθώς και να τηρούνται διαδικασίες ελέγχου και επιθεώρησης που περιορίζουν την πιθανότητα διάπραξης τέτοιων σφαλμάτων.

5.2.6 Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό είναι λογισμικό που είναι προγραμματισμένο να προβαίνει σε ενέργειες που προκαλούν ζημιά στα πληροφοριακά συστήματα. Οι κυριότερες κατηγορίες είναι:

- Ιός: Κώδικας που μεριμνά για την αυτό-αναπαραγωγή του προσαρτώντας αντίγραφα του εαυτού του σε εκτελέσιμα προγράμματα και μετατρέποντάς τα σε ξενιστές. Η εκτέλεση ενός προγράμματος-ξενιστή οδηγεί σε εκτέλεση του ιού και την περαιτέρω διάδοσή του.
- Δούρειος Ίππος: Ένα πρόγραμμα που έχει ως διακηρυγμένο στόχο την υλοποίηση μιας επιθυμητής λειτουργικότητας, αλλά ενσωματώνει μία μη κοινοποιημένη ανεπιθύμητη λειτουργία που οδηγεί σε βλάβες.
- Σκουλήκι: Ένα πρόγραμμα το οποίο αυτό-αναπαράγεται. Διαφέρει από τον ιό στο ότι είναι αυτόνομο και δεν χρειάζεται ξενιστή. Το σκουλήκι δημιουργεί αντίγραφα του εαυτού του, τα οποία εκτελούνται χωρίς την παρέμβαση του χρήστη. Τυπικά διαδίδεται μέσω υπηρεσιών του διαδικτύου.

Το κακόβουλο λογισμικό (malware) αποτελεί μία από τις σημαντικές απειλές για τα συστήματα ενός πλοίου. Πέραν των βασικών τύπων που αναφέρθηκαν ανωτέρω, το κακόβουλο λογισμικό μπορεί να λαμβάνει και πρόσθετες μορφές, όπως:

- Ransomware, το οποίο κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί λύτρα για την αποκατάσταση της πρόσβασης,
- Spyware, το οποίο παρακολουθεί κρυφίως τις δραστηριότητες των χρηστών και συλλέγει πληροφορίες χωρίς αυτοί να το γνωρίζουν ή να συγκατατίθενται σε αυτό,
- Adware, το οποίο εμφανίζει ανεπιθύμητες διαφημίσεις.

Η διαχείριση αυτών των κινδύνων προϋποθέτει ένα ολοκληρωμένο σύστημα ασφάλειας, το οποίο περιλαμβάνει τη χρήση σύγχρονου λογισμικού προστασίας, συστηματικούς ελέγχους, καθώς και εκπαίδευση των χρηστών για την αναγνώριση και αποφυγή ύποπτων εφαρμογών και συνημμένων.

5.2.7 Ηλεκτρονικό ψάρεμα

Η τεχνολογία των πληροφοριών χρησιμοποιείται όλο και περισσότερο για τη ηλεκτρονικό ψάρεμα (phishing). Αυτό αφορά συνήθως την αποστολή emails σε μεγάλο αριθμό από πιθανούς στόχους, αποσκοπώντας στην άντληση ευαίσθητων ή διαβαθμισμένων πληροφοριών (π.χ. συνθηματικών).

Το phishing είναι μία από τις πιο κοινές μορφές ηλεκτρονικής απάτης και θεωρείται ιδιαίτερα επικίνδυνο, αφού εκμεταλλεύεται την εμπιστοσύνη ή/και την άγνοια των χρηστών. Οι επιτιθέμενοι συχνά αποστέλλουν μηνύματα που φαίνονται να έρχονται από αξιόπιστες πηγές, όπως τράπεζες, συνεργάτες ή κυβερνητικούς φορείς, ενθαρρύνοντας τους παραλήπτες να αποκαλύψουν προσωπικές πληροφορίες, κωδικούς πρόσβασης ή άλλες ευαίσθητες λεπτομέρειες. Αυτές οι πληροφορίες μπορεί να αξιοποιηθούν για οικονομική απάτη, κλοπή ταυτότητας ή διάφορες κακόβουλες πράξεις. Η ασφάλεια απέναντι σε τέτοιου είδους επιθέσεις προϋποθέτει προσοχή από τους χρήστες, εκπαίδευση στην αναγνώριση ύποπτων μηνυμάτων, και τη χρήση ψηφιακών εργαλείων ασφαλείας που μπορούν να εντοπίζουν και να εμποδίζουν ύποπτα emails πριν εισέλθουν στα εισερχόμενα των χρηστών (Αλβέρτης, 2016).

5.2.8 Watering Hole Attack

Τα watering hole attacks τυπικά εξαπολύονται προς εταιρείες και οργανισμούς. Αυτό το είδος της επίθεσης, εκμεταλλεύεται μια ιστοσελίδα, οδηγώντας σε λήψη από εργαζόμενους κακόβουλου κώδικα, και καταλήγοντας σε μόλυνση από κακόβουλο λογισμικό. Ο στόχος είναι ο διαμοιρασμός του malware σε όσα περισσότερα συστήματα είναι δυνατόν.

Στις επιθέσεις τύπου Watering Hole, οι επιτιθέμενοι στοχεύουν ιστοσελίδες που είναι γνωστό ότι επισκέπτονται συχνά οι εργαζόμενοι μιας συγκεκριμένης εταιρείας ή οργανισμού. Μόλις η ιστοσελίδα έχει μολυνθεί με κακόβουλο κώδικα, κάθε επισκέπτης της μπορεί να γίνει στόχος, χωρίς καν να αντιληφθεί ότι έχει μολυνθεί το σύστημά του. Αυτός ο τύπος επίθεσης είναι ιδιαίτερα επικίνδυνος επειδή μπορεί να πλήξει πολλαπλά θύματα ταυτόχρονα και να διαδώσει το malware σε δίκτυα υψηλής αξίας. Οι επιθέσεις αυτές απαιτούν προηγμένα μέτρα άμυνας, όπως η συνεχής παρακολούθηση της διαδικτυακής κίνησης, η τακτική ενημέρωση λογισμικού ασφαλείας και η εκπαίδευση των εργαζομένων να αναγνωρίζουν και να αποφεύγουν επισφαλείς ιστότοπους.

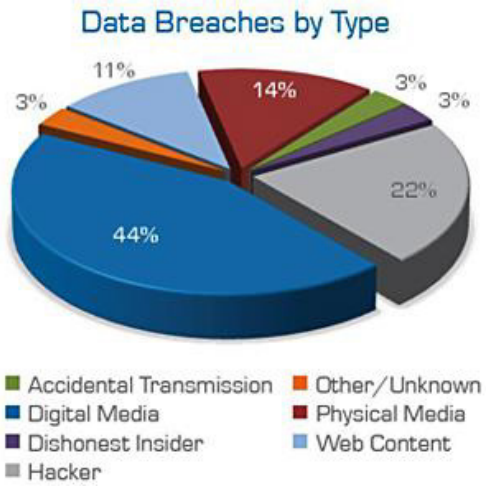
5.2.9 Φυσικές υποδομές

Η πρόκληση βλάβης σε υποδομές περιλαμβάνει τη διακοπή παροχής ρεύματος (συγκαταλέγονται οι παρατεταμένες ή σύντομες διακοπές, αιχμές καθώς και βυθίσεις τάσης), απώλεια επικοινωνιών, διαρροή υδάτων/πλημμύρα, ζητήματα αποχέτευσης, πυρκαγιές και ούτω καθεξής.

Οι φυσικές καταστροφές και οι αποτυχίες υποδομών δύνανται να έχουν καταστροφικές συνέπειες για τα συστήματα ενός πλοίου, διακόπτοντας την κανονική λειτουργία και θέτοντας σε κίνδυνο την ασφάλεια των δεδομένων αλλά και του συνόλου της οντότητας του πλοίου. Διακοπές ρεύματος μπορούν να οδηγήσουν σε απώλεια δεδομένων και διακοπή κρίσιμων υπηρεσιών/συστημάτων, ενώ καταστροφές όπως πυρκαγιές ή πλημμύρες μπορούν να προκαλέσουν φυσική βλάβη στον εξοπλισμό. Η έλλειψη κατάλληλων επικοινωνιών μπορεί να οδηγήσει στην απομόνωση του πλοίου, καθιστώντας δύσκολη την ανταπόκριση σε έκτακτες καταστάσεις. Για την αντιμετώπιση αυτών των κινδύνων, είναι απαραίτητο να υπάρχουν σχέδια συνέχειας λειτουργίας (business continuity plans) και συστήματα εφεδρείας που να διασφαλίζουν ότι οι βασικές λειτουργίες μπορούν να διατηρηθούν ακόμη και σε περίπτωση φυσικών καταστροφών ή άλλων καταστάσεων έκτακτης ανάγκης.

5.2.10 Προστασία Προσωπικών Δεδομένων

Το γεγονός ότι συσσωρεύονται μεγάλες ποσότητες ψηφιακών πληροφοριών που αφορούν φυσικά πρόσωπα σε πληροφοριακά συστήματα που λειτουργούν για λογαριασμό πιστωτικών ιδρυμάτων και ιδιωτικών εταιρειών, σε συνδυασμό με την αυξημένη δυνατότητα των υπολογιστικών συστημάτων για καταγραφή, αποθήκευση, ανάλυση και συσχέτιση πληροφοριών, οδηγούν σε μεγάλους κινδύνους για την ιδιωτικότητα των προσωπικών δεδομένων.



Εικόνα 7. Συχνότητα Τύπων απειλών – επιθέσεων κατά των Πληροφοριακών Συστημάτων (Identity Finder, 2009)

5.3 Ευπάθειες (Vulnerabilities) και Ευάλωτα Συστήματα Πλοίου

Η λειτουργία των σύγχρονων πλοίων στηρίζεται σε μεγάλο βαθμό σε ψηφιακά συστήματα. Σε ένα πλοίο, κατά τη διαδικασία ελέγχου της ασφάλειας των συστημάτων του αρχικά εξετάζονται οι τρωτότητες αυτών των συστημάτων.

Τα αυτόνομα συστήματα παρουσιάζουν χαμηλότερη ευπάθεια σε σύγκριση με εκείνα που είναι συνδεδεμένα σε δίκτυο ή στο Διαδίκτυο. Τα συστήματα των πλοίων, ωστόσο, καθίστανται ολοένα και πιο εξαρτημένα από αυτά που υπάρχουν στην ηπειρωτική χώρα. Η σύνδεση με το Διαδίκτυο είναι απαραίτητη για την υλοποίηση διαφόρων νόμιμων διαδικασιών που σχετίζονται με το πλοίο, όπως (Homeland Security, 2016):

- **Συστήματα Διαχείρισης Φορτίου:** χρησιμοποιούνται για την ηλεκτρονική παρακολούθηση της φόρτωσης, της διαχείρισης και του ελέγχου του φορτίου (τα οποία μπορεί να είναι και επικίνδυνα).

- **Συστήματα Γέφυρας:** Η αυξανόμενη χρήση δικτυακών συστημάτων πλοήγησης, παρέχει πρόσθετα σημεία ευαλωτότητας για τα πλοία, τα οποία μπορούν να αξιοποιηθούν για επιθέσεις. Ακόμη και απομονωμένα συστήματα γέφυρας, τα οποία δεν διασυνδέονται με άλλα συστήματα ή δίκτυα ενδέχεται να παρουσιάζουν αντίστοιχη ευαλοτότητα, καθώς η ενημέρωση αυτών των συστημάτων σε προγράμματα ή δεδομένα συχνά διενεργείται μέσω αφαιρούμενων μέσων (removable media) ή με κατά περίσταση εγκαθιδρυόμενες δικτυακές συνδέσεις, πηγές που δεν ελέγχονται συνήθως επαρκώς (Homeland Security, 2016).

- **Συστήματα πρόωσης και διαχείρισης μηχανημάτων και ελέγχου ενέργειας:** Τα ψηφιακά συστήματα παρακολούθησης και ελέγχου των μηχανημάτων που περιλαμβάνει τις κύριες μηχανές πρόωσης, τις μηχανές παραγωγής ηλεκτρικής ενέργειας αλλά και ηλεκτρικά και ηλεκτρονικά συστήματα, είναι επίσης σημεία που δύναται να εμφανιστούν ευαλωτότητες.
- **Συστήματα Ελέγχου Πρόσβασης:** είναι τα ψηφιακά συστήματα που εξασφαλίζουν την φυσική ασφάλεια του πλοίου, του πληρώματος, των επιβατών και του φορτίου. Περιλαμβάνει συστήματα παρακολούθησης με κάμερες, συστήματα προειδοποίησης κινδύνου κ.ά.
- **Συστήματα Διαχείρισης και Εξυπηρέτησης Επιβατών:** Τα ηλεκτρονικά συστήματα που εφαρμόζονται στο πλαίσιο της διαχείρισης, της επιβίβασης και του ελέγχου των επιβατών είναι πιθανό να διαχειρίζονται προσωπικά δεδομένα, για τα οποία υπάρχει κίνδυνος διαρροής, καταστροφής ή παραφθοράς.
- **Δημόσια Δίκτυα Εξυπηρέτησης Επιβατών:** σταθερά ή ασύρματα δίκτυα που παρέχουν σύνδεση στο Διαδίκτυο για τους επιβάτες εν πλω, θα πρέπει να είναι πλήρως απομονωμένα, φυσικά αλλά και στην ψηφιακή τους διάσταση, σε σχέση με κρίσιμα συστήματα ασφάλειας του σκάφους.
- **Συστήματα Διαχείρισης και Εξυπηρέτησης Πληρώματος:** δίκτυα που χρησιμοποιούνται από το πλήρωμα του πλοίου τόσο για διοικητικούς λόγους όσο και για λόγους ψυχαγωγίας, εφ' όσον παρέχουν πρόσβαση στο Διαδίκτυο ή σε συστήματα

ηλεκτρονικού ταχυδρομείου, θα πρέπει να θεωρούνται συστήματα αυξημένης ευαλωτότητας.

- **Συστήματα Επικοινωνιών:** ασύρματες επικοινωνίες που πραγματοποιούνται μέσω δορυφόρων ή και με άλλους ασύρματους τρόπους συνεισφέρουν στην αύξηση της ευαλωτότητας των συστημάτων του πλοίου.

5.4 Ανάλυση Επικινδυνότητας

Αφού ολοκληρωθεί η καταγραφή των ευπαθειών και των ευάλωτων σημείων ενός πλοίου ή οργανισμού, ακολουθεί η ανάλυση επικινδυνότητας για τα πληροφοριακά συστήματα. Προς την κατεύθυνση αυτή, αξιοποιούνται πρότυπα για τη διαχείριση της ασφάλειας που παρέχουν καθοδήγηση για την κατάρτιση μελέτης για την ανάλυση της επικινδυνότητας (Risk Analysis).

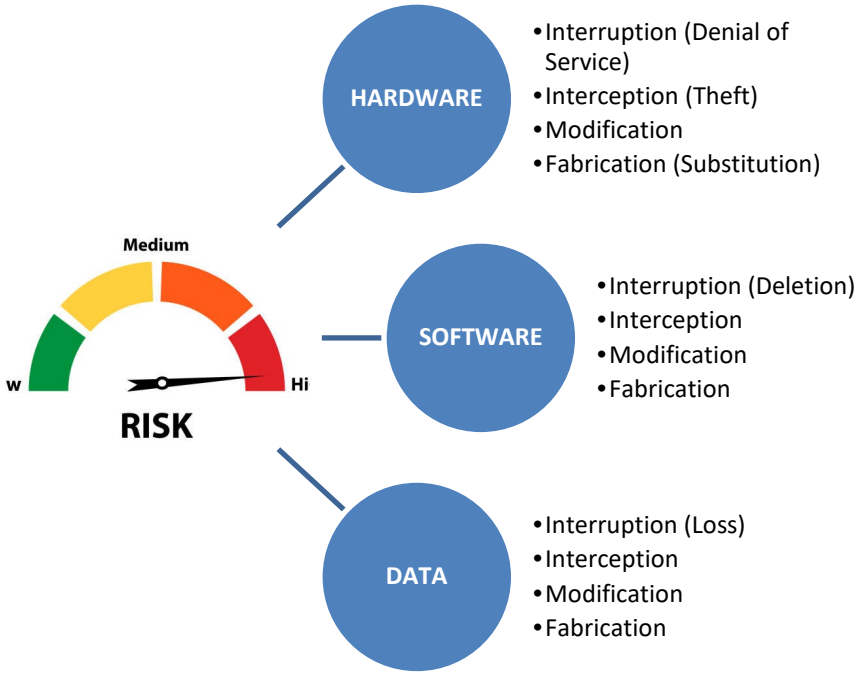
Για διευκόλυνση του αναγνώστη, αρχικά παρατίθενται οι ορισμοί των βασικών εννοιών που εμπλέκονται στην ανάλυση κινδύνων:

- Ως **απειλή** (threat) νοείται η περίσταση που ενέχει την πιθανότητα να προκληθούν απώλειες ή ζημιές, συμπεριλαμβάνοντας την **υποκλοπή** (interception), τη διαρροή δεδομένων, την τροποποίηση ή καταστροφή, την πλαστογράφηση, ή την παύση της λειτουργίας.
- Μία **ευπάθεια** (vulnerability) είναι ένα κενό στην ασφάλεια του συστήματος, το οποίο δύναται να οφείλεται σε κακή ρύθμιση, παρωχημένο/ευάλωτο αλγόριθμο ή μηχανισμό κ.λπ.
- Ως **επίθεση** (attack) ορίζεται το περιστατικό όπου μία απειλή επιχειρεί να αξιοποιήσει (εκούσια ή ακούσια) μία ή περισσότερες ευπάθειες. Μία επίθεση μπορεί να είναι επιτυχής, συνεπώς να καταλήξει σε παραβίαση, ή όχι. Η πιθανότητα παραβίασης υπολογίζεται ως εξής:

  Πιθανότητα παραβίασης = πιθανότητα απειλής x πιθανότητα επιτυχίας επίθεσης
- Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια.
- Αντίμετρο: Ως αντίμετρο ορίζεται ένα μέτρο που τίθεται σε εφαρμογή προκειμένου να αντιμετωπιστούν οι απειλές και να προστατευτεί το σύστημα. Τα μέτρα μπορεί να

συντελούν στην πρόληψη της παραβίασης, στην ανίχνευσή της ή στην απομείωση των απωλειών που προκύπτουν σε περίπτωση παραβίασης (Μπιλάλης, 2016).

Η Εικόνα 8 παρουσιάζει τις διαστάσεις της ανάλυσης επικινδυνότητας,

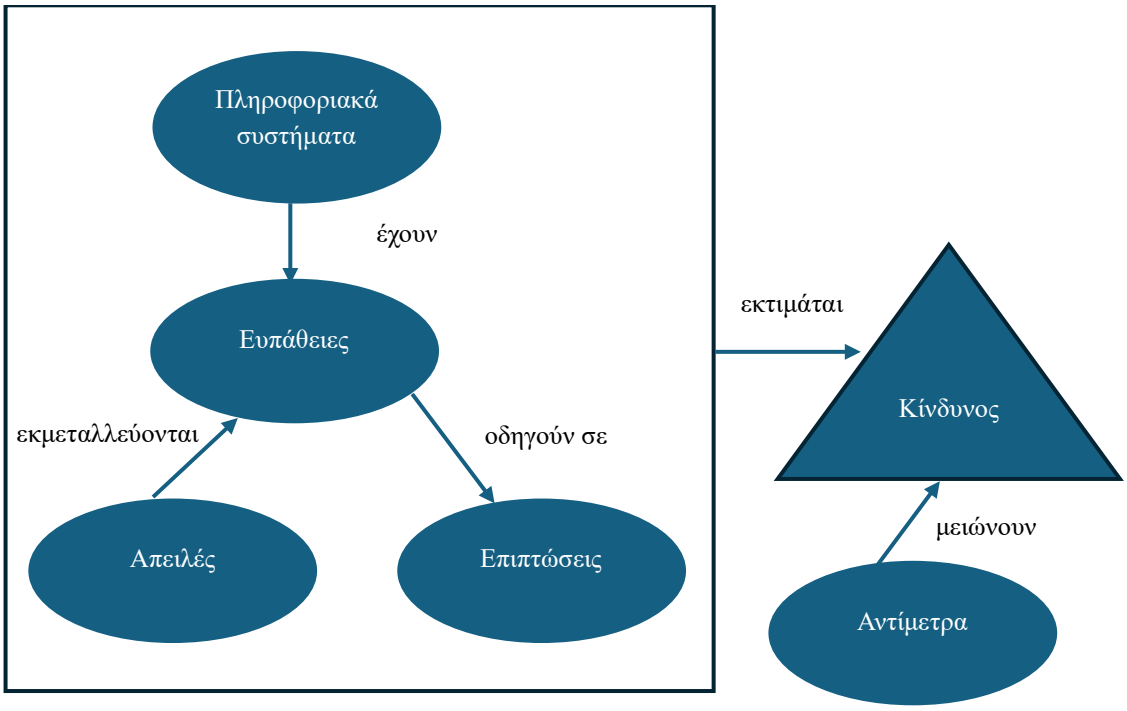


Εικόνα 8. Ανάλυση Επικινδυνότητας (με πληροφορίες από Pfleeger, Pfleeger & Coles-Kemp, 2023)

Μέσω της διαδικασίας ανάλυσης επικινδυνότητας, ο οργανισμός αποκομίζει τις εξής ωφέλειες:

- Κατανοείται το σύστημα σε μεγαλύτερη έκταση και βάθος
- Εμπεδώνεται η κατανόηση της ανάγκης διασφάλισης του συστήματος
- Παρέχεται η δυνατότητα βελτιωμένης στοχοθέτησης των μέτρων που αφορούν την ασφάλεια
- Μπορούν να δικαιολογηθούν ευχερέστερα και πληρέστερα οι δαπάνες για την ασφάλεια
- Βελτιώνεται συνολικά η ασφάλεια του συστήματος.

Η Εικόνα 9 παρουσιάζει την αλληλεξάρτηση των εννοιών που σχετίζονται με την ανάλυση επικινδυνότητας.



Εικόνα 9. Ανάλυση Επικινδυνότητας Επιπτώσεις και Αντίμετρα (Σαλτσίδης, 2018).

Μέσω της ανάλυση επικινδυνότητας, πέραν των ανωτέρω ωφελειών, αναβαθμίζει τις δυνατότητες για πρόβλεψη και αποτροπή μελλοντικών απειλών. Καθώς οδηγεί τους ειδικούς στη συστηματική εξέταση και ανάλυση των πιθανών κινδύνων, ο σχετιζόμενος οργανισμός έχει τη δυνατότητα να αναπτύξει στρατηγικές αυξημένης αποδοτικότητας προκειμένου να αντιμετωπίσει απρόσμενες καταστάσεις, να περιορίσει τα κόστη που προκύπτουν συνεπεία περιστατικών ασφάλειας, και να διαμορφώσουν έναν κύκλο σχεδιασμού-υλοποίησης-ελέγχου-ενεργειών. Επιπρόσθετα, μέσω της ανάλυσης καθίσταται δυνατή η προσαρμογή των μέτρων ασφάλειας στις ανάγκες του οργανισμού, προάγοντας την αποδοτική και αποτελεσματική κατανομή των πόρων.

5.4.1 Μέθοδοι ανάλυσης επικινδυνότητας

Προκειμένου να εκτιμηθεί το τρέχον επίπεδο ασφάλειας ενός πληροφοριακού συστήματος χρησιμοποιούνται μέθοδοι για την ανάλυση της επικινδυνότητας. Τρεις ευρέως διαδεδομένες μέθοδοι είναι οι:

- Security Behavior Analysis (SBA)

- Marion (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau, or Methodology of Analysis of Computer Risks Directed by Levels), η οποία έχει αναπτυχθεί από το Club de la Sécurité de l'Information Français (French Information Security Club).
- CCTA Risk Analysis and Management Method (CRAMM), η οποία αναπτύχθηκε αρχικά από την κυβέρνηση του Ηνωμένου Βασιλείου (CCTA - Central Computer and Telecommunications Agency).

Τα αποτελέσματα της ανάλυσης επικινδυνότητας καθοδηγούν στη συνέχεια τις διαδικασίες διαμόρφωσης της πολιτικής ασφάλειας

Η επιλογή της κατάλληλης μεθόδου ανάλυσης επικινδυνότητας εξαρτάται από τις συγκεκριμένες ανάγκες και το προφίλ κινδύνου του οργανισμού ή της επιχείρησης. Για παράδειγμα, η μέθοδος SBA εστιάζει στην ανάλυση των απειλών και των τρωτών σημείων για την ανάπτυξη μιας στρατηγικής ασφάλειας προσαρμοσμένης στις ιδιαίτερες απαιτήσεις του συστήματος. Η μέθοδος MARION προσφέρει μια πιο δομημένη και συστηματική προσέγγιση, ενώ η CRAMM παρέχει ένα ολοκληρωμένο πλαίσιο που καλύπτει τόσο την ανάλυση των κινδύνων όσο και τη διαχείριση αυτών. Η χρήση αυτών των μεθόδων επιτρέπει την ανάπτυξη μιας πολιτικής ασφάλειας που είναι τεκμηριωμένη, σαφής και προσαρμοσμένη στις πραγματικές συνθήκες και απειλές που αντιμετωπίζει το πληροφοριακό σύστημα, ενισχύοντας έτσι τη συνολική ασφάλεια και ανθεκτικότητα του οργανισμού.

5.5 Ανάλυση επικινδυνότητας

Αναλυτικότερα η ανάλυση επικινδυνότητας (Risk Analysis) του πληροφοριακού συστήματος αποτελείται από τα εξής βήματα (πρβλ. ενότητα 4.4.2):

- Βήμα 1^{ο}: Προσδιορισμός των απειλών (threats) που υφίστανται έναντι του πληροφοριακού συστήματος. Για κάθε στοιχείο εντοπίζονται και καταγράφονται οι απειλές που υφίστανται γι' αυτό και θέτουν σε κίνδυνο την αξία του, ενώ καταγράφεται για κάθε στοιχείο και το σύνολο των επιπτώσεων που συσχετίζονται με κάθε απειλή.
- Βήμα 2^{ο}: Προσδιορισμός ευπαθειών (vulnerabilities) ανά περιουσιακό στοιχείο. Ένα περιουσιακό στοιχείο μπορεί να εμφανίζει κυμαινόμενους βαθμούς ευπάθειας σε

διαφορετικές απειλές. Θα πρέπει να πραγματοποιηθεί ξεχωριστή εκτίμηση των ευπαθειών και του βαθμού έκθεσης ανά στοιχείο και ανά κίνδυνο.

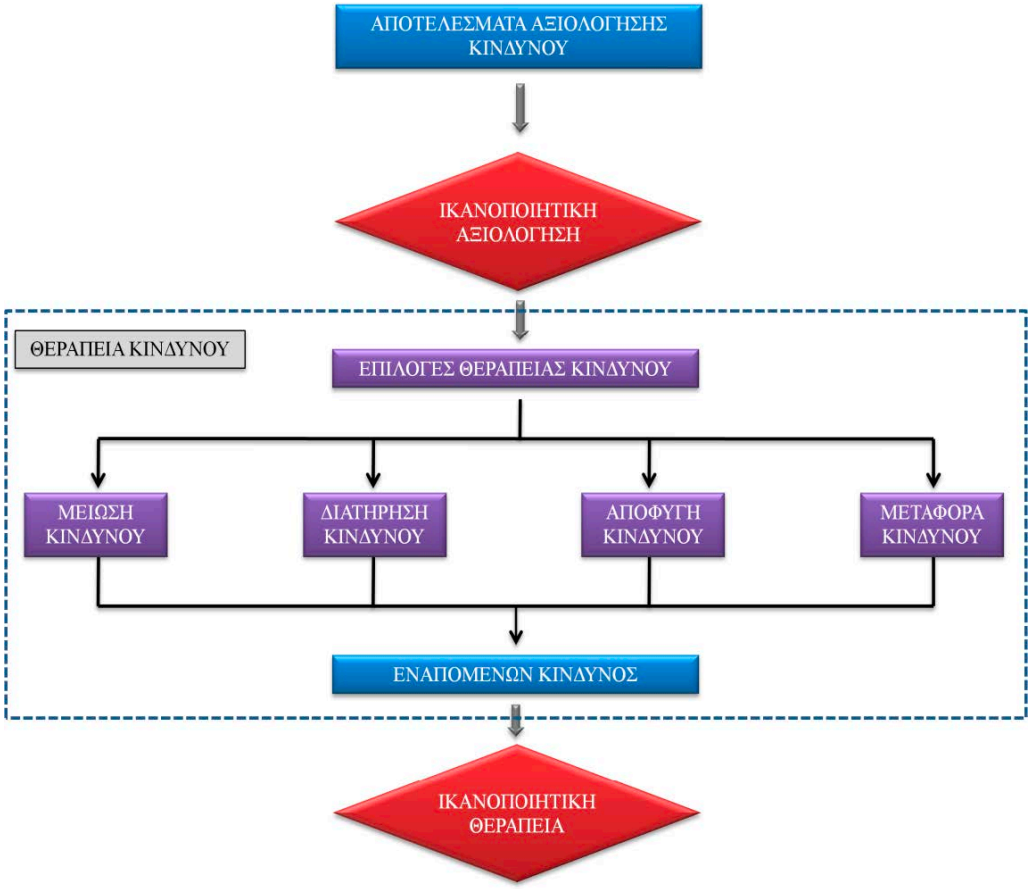
- Βήμα 3ο: Αναγνώριση των ενδεχόμενων ειδών απωλειών (losses) λόγω των επιπτώσεων. Η σύνταξη του καταλόγου διενεργείται με βάση τον βαθμό κινδύνου, ο οποίος, όπως αναφέρθηκε, υπολογίζεται ξεχωριστά για κάθε περιουσιακό στοιχείο και για κάθε απειλή. Στον υπολογισμό συνεκτιμάται το σύνολο των επιπτώσεων που σχετίζονται με μία απειλή, η αξία του στοιχείου, καθώς και οι ευπάθειές του που μπορεί να αξιοποιηθούν από τους παράγοντες της απειλής.
- Βήμα 4ο: Η εκτίμηση των πιθανοτήτων να προκύψουν απώλειες. Σε συνέχεια των αντιστοιχίσεων των απειλών με περιουσιακά στοιχεία, διενεργείται εκτίμηση των πιθανοτήτων να εκδηλωθεί επίθεση σε έκαστο περιουσιακό στοιχείο. Συμπληρωματικά καταγράφεται ο βαθμός της ευπάθειας του στοιχείου προς τη συγκεκριμένη απειλή.
- Βήμα 5ο: Προσδιορισμός των προσηκόντων αντίμετρων (counter measures) προκειμένου να αντιμετωπιστούν οι κίνδυνοι. Στο πλαίσιο αυτό ο οργανισμός εξετάζει τα ακόλουθα ενδεχόμενα:
    - *Αποφυγή κινδύνου*, η οποία πραγματοποιείται με απόσυρση του πόρου από τη συγκεκριμένη επιχειρησιακή δράση/υπηρεσία (ή τη συνολική κατάργηση της υπηρεσίας)
    - *Αποδοχή κινδύνου*, ήτοι δεν λαμβάνεται κανένα μέτρο και η επιχειρησιακή δράση/υπηρεσία συνεχίζει κανονικά τη λειτουργία της,
    - Μετριασμός κινδύνου, με εφαρμογή αντιμέτρων. Προσδιορίζονται τα κατάλληλα αντίμετρα και το κόστος που συσχετίζεται με κάθε ένα από αυτά (οικονομικό, τεχνικό, ανθρώπινο).
- Βήμα 6ο: Κατάρτιση και εφαρμογή ενός αποτελεσματικού και οικονομικά αποδοτικού (cost effective) συστήματος ασφάλειας. Είναι ενδεχόμενο έτσι να έχουμε αποδοχή κινδύνου, π.χ. διότι ο κίνδυνος θεωρείται αμελητέος ή διότι το κόστος εφαρμογής αντιμέτρων υπερβαίνει την ωφέλεια. Επίσης είναι δυνατό να επιλεγεί μία λύση με μικρότερο βαθμό μείωσης του κινδύνου αλλά και χαμηλότερο κόστος, αν κριθεί ότι η επένδυση σε πιο αποτελεσματικές λύσεις δεν δικαιολογεί το αυξημένο κόστος τους.
- Η ανάλυση επικινδυνότητας για ένα πληροφοριακό σύστημα πρέπει να χαρακτηρίζεται από πληρότητα, ήτοι να έχουν συνεκτιμηθεί όλα τα στοιχεία και οι απειλές που αφορούν

την ασφάλεια του Π.Σ., συμπεριλαμβάνοντας (α) τις υπολογιστικές υποδομές, (β) τη δικτυακή υποδομή, (γ) το επίπεδο της φυσικής πρόσβασης στο σύστημα και συνακόλουθα τη φυσική ασφάλειά του. Αντίστοιχα, κατατάσσονται σε κατηγορίες οι απειλές, ανάλογα με το είδος τους/τα αποτελέσματά τους. Ενδεικτικές κατηγορίες είναι η διείσδυση στις επικοινωνίες (communication infiltration), η διείσδυση σε επίπεδο λογικής (logical infiltration), οι αστοχίες σε επίπεδο υλικού/εξοπλισμού (equipment failure) και οι φυσικές απειλές (Physical Threats) π.χ. πυρκαγιά, σεισμός κ.τ.λ.

- Ιδιαίτερο βάρος δίδεται στην κατηγορία της διείσδυσης σε επίπεδο λογικής, η οποία εξετάζει τις πληροφορίες που επεξεργάζεται και διαχειρίζεται το πληροφοριακό σύστημα και την προστασία που θα πρέπει να παρέχεται σε αυτές. Στο πλαίσιο αυτό αναλύονται τα προγράμματα/οι εφαρμογές που χρησιμοποιούνται, τα δεδομένα (αρχεία δεδομένων, βάσεις δεδομένων κ.λπ.) αλλά και οι σχετιζόμενες διαδικασίες με εμπλοκή στελεχών του οργανισμού. Η διείσδυση στις επικοινωνίες είναι επίσης σημαντική κατηγορία, καθώς μέσω του δικτύου μπορεί να υπάρχει διαρροή δεδομένων/πληροφοριών, υποκλοπή συνθηματικών, επιθέσεις στο σύστημα ή λοιπές παραβιάσεις. Τέλος, η φυσική ασφάλεια είναι σημαντική διάσταση, εξετάζοντας τη συνέχεια των υπηρεσιών σε περίπτωση δυσμενών φυσικών φαινομένων ή αστοχιών υλικού. Συνολικά, ο στόχος της ανάλυσης επικινδυνότητας είναι να προληφθούν οι ζημιές, να μειωθεί η έκθεση των πόρων σε κινδύνους και να μετριαστεί το ενδεχόμενο διακοπής της επιχειρησιακής δραστηριότητας του οργανισμού.

5.6 Θεραπεία κινδύνου

Σύμφωνα με τα προαναφερθέντα, προκειμένου να αντιμετωπισθούν οι κίνδυνοι που δύνανται να απειλήσουν ένα πληροφοριακό σύστημα εντάσσονται στις κάτωθι κατηγορίες:



Εικόνα 10. Θεραπεία κινδύνου (Καρατζάς, 2013)

- **Μετριασμός κινδύνου:** Πρόκειται για την επιλογή των κατάλληλων μέτρων με στόχο τη μείωση του επιπέδου του κινδύνου σε επιθυμητά/ανεκτά/διαχειρίσιμα επίπεδα ούτως ώστε ο κίνδυνος που εναπομένει να δύναται να κριθεί ως αποδεκτός.

  Επιπρόσθετα, αν υιοθετηθεί η λύση της απομείωσης του κινδύνου, θα πρέπει να συνυπολογιστούν και τυχόν περιορισμοί σε χρονικό, τεχνικό, οικονομικό, επιχειρησιακό και ηθικό επίπεδο οι οποίοι θα επηρεάσουν το σύστημα.

- **Αποφυγή του κινδύνου:** Σε ενδεχόμενο που το επίπεδο του κινδύνου είναι πολύ υψηλό ή το κόστος για την εφαρμογή των κατάλληλων αντίμετρων δεν φτάνει ένα ικανοποιητικό επίπεδο κόστους/οφέλους, τότε μπορεί να αποφασιστεί η εξ ολοκλήρου αποφυγή του κινδύνου, π.χ. με απόσυρση υπηρεσίας.

- **Αποδοχή κινδύνου:** Επιλέγεται όταν το επίπεδο επικινδυνότητας πληροί τις προϋποθέσεις και τα κριτήρια για την αποδοχή του κινδύνου. Στην προκειμένη περίπτωση, δεν υπάρχει λήψη αντιμέτρων και κατά προέκταση ο κίνδυνος διατηρείται.
- **Μεταφορά του κινδύνου:** Σύμφωνα με αυτή την προσέγγιση, ο κίνδυνος μεταφέρεται σε εξωτερικό φορέα, ο οποίος έχει τη δυνατότητα να τον χειριστεί αποτελεσματικά. Η μεταφορά μπορεί να δημιουργήσει νέους κινδύνους (π.χ. κίνδυνοι στη διασύνδεση εταιρικών συστημάτων στο εσωτερικό δίκτυο με το εξωτερικό σύστημα που φιλοξενεί την υπηρεσία που μεταφέρθηκε), και συνεπώς μπορεί να εισάγεται η ανάγκη για λήψη νέων μέτρων.

6 Πολιτικές Ασφαλείας και μέτρα προστασίας

6.1 Πολιτικές Ασφαλείας και Διαδικασίες

Το προσωπικό μιας εταιρείας/ενός οργανισμού αποτελεί ένα ιδιαίτερα σημαντικό περιουσιακό στοιχείο. Οι πολιτικές ασφαλείας, σε συνδυασμό με τις διαδικασίες, παρέχουν στο προσωπικό τα εργαλεία που υποστηρίζουν την πραγμάτωση του σημαντικού ρόλου που αυτό επιτελεί, ωστόσο τα εφόδια αυτά δεν είναι αφ' εαυτών αρκετά. Είναι απαραίτητο να υπάρχει μέριμνα για ευαισθητοποίηση του προσωπικού και καλλιέργεια κουλτούρας για την ασφάλεια συστημάτων. Τα έγγραφα που σχετίζονται με τις πολιτικές ασφαλείας και τις σχετιζόμενες διαδικασίες θα πρέπει να καθίστανται προσβάσιμα στο προσωπικό και να υπάρχουν ενημερώσεις για τυχόν αλλαγές και επικαιροποιήσεις. Θα πρέπει να υπάρχει σαφήνεια ως προς τον τρόπο εφαρμογής των προβλέψεων που αφορούν την ασφάλεια, καθώς και τις επιπτώσεις που θα επέλθουν σε περίπτωση που υπάρξουν παρεκκλίσεις από τα οριζόμενα. Οι πολιτικές και οι διαδικασίες θα πρέπει να επανεξετάζονται συχνά ώστε να διασφαλίζεται ότι παρέχουν πλήρη κάλυψη λαμβάνοντας υπ' όψιν τις εκάστοτε τεχνολογικές εξελίξεις. Το ελάχιστο σύνολο ζητημάτων που θα πρέπει να καλύπτουν και να ρυθμίζουν οι πολιτικές έχει ως ακολούθως (Γεωργιάδης, 2018):

- Δυνατότητα ανάκτησης δεδομένων, δημιουργία αντιγράφων ασφαλείας, πλεονασμός (redundancy), συνέχιση της επιχειρησιακής λειτουργίας και σχέδιο αποκατάστασης μετά από καταστροφή,
- Προνόμια διαχειριστή, καθορισμός καθηκόντων για τους χρήστες και μηχανισμοί παραχώρησης και ανάκλησης πρόσβασης,
- Έλεγχο απομακρυσμένης πρόσβασης, χρήση εικονικών ιδιωτικών δικτύων (VPN) καθώς και μηχανισμών κρυπτογράφησης,
- Περιορισμοί και κανόνες στη φυσική πρόσβαση, πολιτικές χρήσης αφαιρούμενων αποθηκευτικών μέσων, πολιτικές για χρήση προσωπικών συσκευών ("Bring Your Own Device – BYOD"),
- Τα όρια της χρήσης της εταιρικής υποδομής για προσωπικούς λόγους (π.χ. χρήση του εταιρικού email για προσωπική αλληλογραδά),
- Πολιτικές και κανονισμοί χρήσης ηλεκτρονικού ταχυδρομείου, κανόνες κωδικών πρόσβασης, ενημέρωση και ευαισθητοποίηση για το ηλεκτρονικό ψάρεμα ("phishing"),

- Θέματα αναβάθμισης λογισμικού, διαδικασία προγραμματισμού και εγκατάστασης ενημερώσεων και χρονοπρογραμματισμός συντηρήσεων,
- Προμήθεια, εγκατάσταση, ρύθμιση και χρήση λογισμικού προστασίας από ιούς, καθώς και θέματα ενημέρωσης υπογραφών και μηχανών εντοπισμού ιών,
- Χαρακτηρισμός και χρήση λογισμικού τρίτων (σύνταξη λευκής και μαύρης λίστας),
- Διάθεση ή πώληση εξοπλισμού και μέτρα για την προστασία/καταστροφή των δεδομένων που αποθηκεύεται στον εξοπλισμό.

6.2 Μέτρα για την ενίσχυση της επί του πλοίου ασφάλειας στον Κυβερνοχώρο

Καθώς ο βαθμός εξάρτησης από το λογισμικό, το διαδίκτυο και τις τεχνολογίες βαίνει αυξανόμενος, γίνεται αντίστοιχα ολοένα και πιο σημαντική η ασφάλεια στον κυβερνοχώρο. Στον τομέα της ναυτιλίας, διαμορφώνονται κατευθυντήριες γραμμές και οδηγίες για την πιο αποτελεσματική προστασία έναντι των απειλών που υφίστανται, τόσο εδραιωμένων όσο και νεοεμφανιζομένων, την καλύτερη αντιμετώπιση ευαλωτοτήτων/τρωτών σημείων, καθώς και έναντι επιθέσεων εναντίον των αγαθών. Συνακόλουθα, απαιτείται η Εισαγωγή κατάλληλων τεχνικών και διαδικαστικών ελέγχων για την προστασία των επιχειρήσεων των εργασιών που εκτελούνται στο πλοίο, καθώς και των πληροφοριών και των δεδομένων που σχετίζονται με τα πλοία και τα πληρώματά τους, τους επιβάτες τους και τα φορτία τους (Ρόδιος, 2017).

6.3 Εμπλεκόμενοι στην Ανάπτυξη Πολιτικών Ασφάλειας

Η ανάπτυξη πολιτικών ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού, προϋποθέτει την καταγραφή των απαιτήσεων ασφάλειας. Με βάση τα αποτελέσματα της καταγραφής διαμορφώνεται η στόχευση της ασφάλειας και προσδιορίζεται ο τρόπος για την επίτευξη της στόχευσης αυτής. Οι απαιτήσεις που αφορούν την ασφάλεια είναι δυνατόν να συλλέγονται από μία πληθώρα πηγών όπως για παράδειγμα:

- Οι τελικοί χρήστες των συστημάτων,
- Η διοίκηση της εταιρείας ή του οργανισμού, η οποία έχει ως στόχο τη διασφάλιση απρόσκοπτης χρήσης για τα πληροφοριακά συστήματα που υποστηρίζουν τις λειτουργίες του οργανισμού,

- Οι οι πελάτες του οργανισμού καθώς και οι συναλασσόμενοι με αυτόν, καθώς τα πληροφοριακά συστήματα του οργανισμού περιλαμβάνουν δεδομένα που τους αφορούν και εκτελούν υπηρεσίες που σχετίζονται με εκείνους,
- Τα νομικά ρυθμιστικά και κανονιστικά πλαίσια τα οποία διέπουνε τη λειτουργία του οργανισμού.

Πολιτική ασφάλειας θα πρέπει να έχει έκταση και βάθος που να είναι επαρκή για την ικανοποίηση όλων των απαιτήσεων ασφάλειας που καταγράφονται για τα συστήματα του οργανισμού. Οι προβλέψεις μάλιστα θα πρέπει να τηρούν προδιαγραφές αναλογικότητας, δηλαδή το επίπεδο ασφάλειας που επιτυγχάνεται για έκαστο σύστημα ή υπηρεσία να είναι ανάλογο της κρισιμότητας του συστήματος για τον οργανισμό, χωρίς παράλληλα να υπάρχει υπέρμετρη επιβάρυνση των χρηστών λόγω της εισαγωγής των μηχανισμών ασφαλείας.

6.4 Βέλτιστη πρόταση μέτρων ασφάλειας

Η διαμόρφωση της τελικής βέλτιστης πρότασης για υιοθέτηση και εφαρμογή μέτρων ασφαλείας πραγματοποιείται λαμβάνοντας υπ' όψιν το σύνολο των αποτελεσμάτων της διαδικασίας αξιολόγησης κινδύνου του οργανισμού. Το τελικό εξαγόμενο θα πρέπει να διασφαλίζει τον μετριασμό του κινδύνου σε επίπεδα που κρίνονται ως αποδεκτά. Επιπρόσθετα θα πρέπει να περιλαμβάνονται συγκεκριμένες αναθέσεις αρμοδιοτήτων στους αξιωματικούς του πλοίου αλλά και στους υπαλλήλους που είναι επιφορτισμένη με την τήρηση της ασφάλειας από πλευράς της ναυτιλιακής εταιρείας. Τέλος, είναι επιθυμητό, για κάθε ανάθεση αρμοδιοτήτων να παρέχονται συγκεκριμένες οδηγίες για τον τρόπο εκτέλεσης των καθηκόντων που απορρέουν από τους κανονισμούς ασφάλειας.

6.5 Υλοποίηση Μέτρων Ασφαλείας στην Πράξη

Η προστασία κρίσιμων συστημάτων τα οποία υποστηρίζουν την επιχειρησιακή λειτουργία, τη λήψη αποφάσεων σε ένα πλοίο καθώς και τη διαχείριση του πλοίου, αλλά και τα σχετιζόμενα δεδομένα, θα πρέπει να προστατεύονται αποτελεσματικά με εφαρμογή πολλαπλών επιπέδων μέτρων προστασίας. Στο πλαίσιο αυτό θα πρέπει να λαμβάνεται υπόψη ο ρόλος του προσωπικού, των διαδικασιών και της τεχνολογίας προκειμένου:

- Να αυξάνονται οι πιθανότητες για την ανίχνευση ενός περιστατικού ασφαλείας,

- Να διατίθενται επαρκείς τεχνολογική και ανθρώπινοι πόροι προκειμένου για την επίτευξη του απαραίτητου επίπεδου ασφαλείας.

Η υλοποίηση των μέτρων ασφαλείας πρέπει να είναι μια ολιστική διαδικασία που ενσωματώνει τεχνολογικά εργαλεία, αυστηρές διαδικασίες και εκπαίδευση του προσωπικού. Είναι σημαντικό να εφαρμόζονται τεχνικά μέτρα όπως η κρυπτογράφηση δεδομένων, η χρήση firewall και συστημάτων ανίχνευσης εισβολών (IDS), καθώς και η τακτική ενημέρωση των συστημάτων αυτών για την προστασία από νέες απειλές. Παράλληλα, οι διαδικασίες θα πρέπει να περιλαμβάνουν σαφείς κατευθυντήριες γραμμές για την ασφαλή διαχείριση των δεδομένων και την αντιμετώπιση περιστατικών ασφαλείας. Η εκπαίδευση του προσωπικού αποτελεί επίσης κρίσιμο στοιχείο, καθώς η επίγνωση των πιθανών απειλών και η γνώση των βέλτιστων πρακτικών δύναται να μειώσει σημαντικά την πιθανότητα ανθρώπινου λάθους το οποίο θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια του πλοίου και των πληροφοριακών του συστημάτων.

6.6 «Άμυνα σε βάθος» (“defense in depth”)

Όπως προαναφέρθηκε, η προστασία κρίσιμων συστημάτων τα οποία υποστηρίζουν την επιχειρησιακή λειτουργία, τη λήψη αποφάσεων σε ένα πλοίο καθώς και τη διαχείριση του πλοίου, αλλά και τα σχετιζόμενα δεδομένα, θα πρέπει να προστατεύονται αποτελεσματικά με εφαρμογή πολλαπλών επιπέδων μέτρων προστασίας. Η προσέγγιση αυτή καλείται «άμυνα σε βάθος» και για την υλοποίησή της αξιοποιείται συνδυασμός μέτρων και διαδικασιών που αφορούν:

- Τη φυσική ασφάλεια του πλοίου,
- Την προστασία των δικτύων με πλήρη λειτουργική κατάτμηση (network segregation),
- Την ανίχνευση εισβολλών
- Τη διενέργεια περιοδικών ελέγχων και σαρώσεων για ευπάθειες στην πληροφοριακή καθώς και τη δικτυακή υποδομή,
- Σύνταξη λευκής λίστας που θα περιλαμβάνει τις εφαρμογές των οποίων η χρήση επιτρέπεται,
- Ελέγχους αναθέσεων δικαιωμάτων, σε αντιπαραβολή με την πολιτική ασφάλειας,
- τις πολιτικές που σχετίζονται με τη χρήση αφαιρούμενων μέσων και την πολυπλοκότητα των κωδικών ασφάλειας,

- Την ενημέρωση και ευαισθητοποίηση του ανθρώπινου δυναμικού σχετικά με τους υφιστάμενους κινδύνους καθώς και την εκπαίδευση στις διαδικασίες.

Η «άμυνα σε βάθος» έχει ως αποτέλεσμα την καλύτερη προστασία του εξοπλισμού των πληροφοριακών συστημάτων και των δεδομένων. Αυτό εξασφαλίζεται μέσω μέτρων τα οποία τοποθετούνται σε επάλληλα επίπεδα διαμορφώνοντας έτσι ένα πιο αποτελεσματικό σύστημα άμυνας.

6.7 «Άμυνα σε πλάτος» (“ defense in breadth”)

Καθώς στη σύγχρονη ναυτιλία το επίπεδο της ολοκλήρωσης μεταξύ των συστημάτων που είναι τοποθετημένα επί του πλοίου είναι πολύ υψηλό, και αντίστοιχα υψηλός είναι ο βαθμός αλληλεξάρτησης μεταξύ των συστημάτων, Η επίτευξη του επιθυμητού επιπέδου ασφάλειας προϋποθέτει την εφαρμογή κατάλληλων μηχανισμών και μέτρων προστασίας σε όλη την έκταση των συστημάτων του πλοίου. Αυτό καλείται «Άμυνα σε Πλάτος» και χρησιμοποιείται για να περιορίσει τον βαθμό ευαλωτότητας των συστημάτων του πλοίου, αποτρέποντας τη διάδοση των επιπτώσεων από την ύπαρξη ευπάθειας σε ένα σύστημα, στα υπόλοιπα.

Η «Άμυνα σε Πλάτος» απαιτεί την εφαρμογή ενός πολυεπίπεδου και διασυνδεδεμένου πλέγματος μέτρων ασφαλείας που καλύπτει κάθε πιθανό σημείο εισόδου και αλληλεπίδρασης μεταξύ των συστημάτων του πλοίου. Αυτό σημαίνει ότι δεν πρέπει να βασίζεται μόνο σε μεμονωμένα μέτρα προστασίας, αλλά να εξασφαλίζει ότι κάθε επίπεδο άμυνας υποστηρίζει και ενισχύει τα υπόλοιπα. Για παράδειγμα, ένα σύστημα ελέγχου πρόσβασης πρέπει να συνεργάζεται με συστήματα παρακολούθησης δικτύου και εντοπισμού ανωμαλιών, ώστε οποιαδήποτε παραβίαση σε ένα επίπεδο να μπορεί να εντοπιστεί και να αντιμετωπιστεί προτού επηρεάσει άλλα κρίσιμα συστήματα. Αυτή η προσέγγιση μειώνει τον κίνδυνο μιας αποτυχίας ασφαλείας να εξαπλωθεί και να προκαλέσει εκτεταμένες ζημιές, διασφαλίζοντας τη συνεχή λειτουργία και την ασφάλεια όλων των συστημάτων του πλοίου.

6.8 Προστασία και Αποτροπή Επιθέσεων

Τα μέτρα προστασίας χωρίζονται σε δύο κατηγορίες άμυνας, (α) στα Τεχνικά (Technical) και (β) στα Διαδικαστικά (Procedural). Η πρώτη κατηγορία αφορά τον σχεδιασμό, την ανθεκτικότητα του εξοπλισμού και τον τρόπο διασύνδεσης των συστημάτων. Η δεύτερη αφορά θέματα όπως οι

διαδικασίες εργασίας, πολιτικές διαχείρισης ανθρώπινων πόρων, διαδικασίες ασφαλείας και ελέγχους πρόσβασης. Οι δύο κατηγορίες δεν λειτουργούν αυτόνομα αλλά είναι αλληλοεξαρτώμενες.

Η αποτελεσματική προστασία και αποτροπή επιθέσεων επιτυγχάνεται όταν τα μέτρα των δύο κατηγοριών (διαδικαστικά και τεχνικά) συνεργάζονται αποτελεσματικά, διαμορφώνοντας ένα ολιστικό και συνεκτικό αμυντικό σύστημα. Στο πλαίσιο αυτό, τα τεχνικά μέτρα (π.χ. κρυπτογράφηση δεδομένων, συστήματα firewall και δίκτυα VPN) υλοποιούν πρώτη γραμμή άμυνας έναντι εξωτερικών επιθέσεων και ευαλωτοτήτων των συστημάτων. Συμπληρωματικά τα διαδικαστικά μέτρα παρέχουν τα εχέγγυα ότι ο ανθρώπινος παράγοντας που εμπλέκεται στη διαδικασία υλοποίησης της ασφάλειας τηρεί απαρέγκλιτα τα πρότυπα και τις διαδικασίες που προβλέπονται από το κανονιστικό πλαίσιο, με αποτέλεσμα τη μείωση του κινδύνου εμφάνισης σφαλμάτων που οφείλονται στο ανθρώπινο παράγοντα. Η συνδυαστική λειτουργία των δύο προσεγγίσεων, σε συνδυασμό με τη διαρκή εκπαίδευση του προσωπικού και την τακτική επικαιροποίηση των πολιτικών και διαδικασιών, ενισχύει την ανθεκτικότητα του πλοίου απέναντι σε πιθανές απειλές και διασφαλίζει την απρόσκοπτη λειτουργία των κρίσιμων συστημάτων του.

6.9 Τεχνικά Μέτρα Προστασίας

Τα τεχνικά μέτρα προστασίας που εφαρμόζονται στο πλαίσιο της ναυτιλίας περιλαμβάνουν τα κάτωθι:

- Περιορισμός και έλεγχος των δικτυακών θυρών (ports), των πρωτοκόλλων και των υπηρεσιών: για την εφαρμογή των πολιτικών ασφαλείας της εταιρείας μπορούν να χρησιμοποιηθούν οι λίστες πρόσβασης στα συστήματα του δικτύου. Έτσι, διασφαλίζεται ότι μέσω ενός ελεγχόμενου δικτύου διέρχεται μόνον η επιτρεπόμενη κίνηση.
- Ρύθμιση και παραμετροποίηση των δικτυακών συσκευών όπως τα firewalls, routers και switches: πρέπει να καθοριστεί ποια συστήματα μπορούν να συνδέονται σε ελεγχόμενα δίκτυα και ποια όχι. Δίκτυα Με πιο ελαστικό πλαίσιο ελέγχου (όπως για παράδειγμα δίκτυα για την εξυπηρέτηση των επιβατών του πλοίου) δεν θα πρέπει να διασυνδέονται με δίκτυα ελεγχόμενης πρόσβασης, καθώς η δυνατότητα των δικτύων της πρώτης κατηγορίας για σύνδεση με το Διαδίκτυο τα καθιστά επιρρεπή στην διείσδυση κακόβουλου λογισμικού. Δίκτυα που (α) είναι κρίσιμα για την επιχειρησιακή λειτουργία του πλοίου, (β) παρέχουν

απομακρυσμένη πρόσβαση σε χρήστες με αυξημένα προνόμια, (γ) επεξεργάζονται στοιχεία του φορτίου, θα πρέπει να παρέχουν υψηλό επίπεδο ασφάλειας

- Φυσική ασφάλεια: αποτελεί μια αποτελεσματική «άμυνα σε βάθος», εξασφαλίζοντας ότι περιοχές με ευαίσθητα εξαρτήματα θα πρέπει να ασφαλίζονται και ο εξοπλισμός και τα καλώδια του δικτύου να μην είναι προσβάσιμα από μη εξουσιοδοτημένα άτομα. Επιπρόσθετα, δεν πρέπει να υπάρχει δυνατότητα φυσικής πρόσβασης σε ευαίσθητο εξοπλισμό και η τοποθέτηση αφαιρούμενων μέσων ή εξωτερικών συσκευών σε κρίσιμα συστήματα (π.χ. σε θύρες USB στα συστήματα της γέφυρας).
- Ανίχνευση, αποκλεισμός και ειδοποιήσεις: η ανίχνευση εισβολών και μολύνσεων αποτελεί κρίσιμο σημείο των διαδικασιών ελέγχου. Για να μπορέσουν να καθοριστούν τα κατώτατα όρια συναγερμού σε περίπτωση περιστατικού ασφαλείας, θα πρέπει οι ρόλοι των χρηστών να είναι διακριτοί και να υπάρχει επιμερισμός αρμοδιοτήτων και ευθύνης. Επιπρόσθετα, οι εταιρείες μπορούν να επιλέξουν να ενσωματώσουν ένα Σύστημα Ανίχνευσης Εισβολών (IDS) ή ένα Σύστημα Πρόληψης Εισβολών (IPS) στο δίκτυο ή ως μέρος του τείχους προστασίας.
- Για τις δορυφορικές και λοιπές ραδιοκυματικές επικοινωνίες, θα πρέπει η ασφάλεια να καθοριστεί σε συνεργασία με τον πάροχο της υπηρεσίας. Οι προδιαγραφές της δορυφορικής σύνδεσης θα πρέπει να ληφθούν υπόψη κατά τον καθορισμό των απαιτήσεων προστασίας του δικτύου.
- Έλεγχος ασύρματης πρόσβασης: η ασύρματη πρόσβαση στα δίκτυα του πλοίου, θα πρέπει να περιορίζεται μόνο σε συσκευές που προορίζονται για αυτό τον σκοπό. Θα πρέπει να χρησιμοποιούνται ισχυρά κλειδιά κρυπτογράφησης, τα οποία θα ανανεώνονται τακτικά.
- Εντοπισμός κακόβουλου λογισμικού (Malware): Θα πρέπει να χρησιμοποιείται λογισμικό σάρωσης που μπορεί να εντοπίσει και να αντιμετωπίσει αυτόματα την παρουσία κακόβουλου λογισμικού σε συστήματα. Ως γενική κατευθυντήρια οδηγία, οι ηλεκτρονικοί υπολογιστές που είναι τοποθετημένοι στα κεντρικά γραφεία και οι οποίοι επικοινωνούν άμεσα ή έμμεσα με τα συστήματα του πλοίου, θα πρέπει να προστατεύονται το ίδιο με αυτούς που βρίσκονται στο πλοίο.
- Ασφαλής ρύθμιση υλικού και λογισμικού: Προνόμια επιπέδου διαχειριστή θα πρέπει να απονέμονται μόνο σε ανώτερα στελέχη τα οποία θα είναι απόλυτα έμπιστα. Τα στελέχη αυτά θα μπορούν εν συνεχεία να διαχειρίζονται και να ελέγχουν τους λογαριασμούς και τα

προνόμια των απλών χρηστών. Οι χρήστες δεν θα πρέπει να έχουνε τη δυνατότητα να εγκαθιστούν νέα προγράμματα ή να τροποποιούν τη διαμόρφωση του υλικού.

- Προστασία εφαρμογών πλοήγησης (browsers) και ηλεκτρονικού ταχυδρομείου: η επικοινωνία μεταξύ πλοίου και συστημάτων επί της ακτής είναι κρίσιμη για τη λειτουργία του πλοίου. Συνακόλουθα διαδικτυακές (web-based) εφαρμογές και συστήματα ηλεκτρονικού ταχυδρομείου θα πρέπει να προστατεύονται κατάλληλα έτσι ώστε:
  - Να αποτρέπεται η διαρροή των ευαίσθητων πληροφοριών που διακινούνται μέσω του ηλεκτρονικού ταχυδρομείου,
  - Να εξασφαλίζεται η εμπιστευτικότητας και η ακεραιότητας των δεδομένων που ανταλλάσσονται με το ηλεκτρονικό ταχυδρομείο,
  - Να αποτρέπεται η εκτέλεση κακόβουλων σεναρίων (scripts) μέσα στα προγράμματα περιήγησης ιστού και ηλεκτρονικού ταχυδρομείου.
- Δυνατότητα επαναφοράς δεδομένων: Θα πρέπει να παρέχεται η δυνατότητα για επαναφορά του συστήματος ή/και των δεδομένων από ένα ασφαλές και «καθαρό» αντίγραφο, επιτρέποντας την αποκατάσταση τους, σε περιπτώσεις προβλημάτων.
- Ασφάλεια λογισμικού εφαρμογών: θα πρέπει να παρέχονται ενημερώσεις ασφαλείας στα ενσωματωμένα συστήματα.

6.10 Διαδικαστικά Μέτρα Προστασίας

Τα διαδικαστικά μέτρα προστασίας που εφαρμόζονται στο πλαίσιο της ναυτιλίας περιλαμβάνουν τα κάτωθι:

- Εκπαίδευση και ευαισθητοποίηση: Η κατάρτιση και η ευαισθητοποίηση του προσωπικού αποτελούν τα βασικά υποστηρικτικά στοιχεία μιας αποτελεσματικής προσέγγισης της διαχείρισης κινδύνου. Το προσωπικό διαδραματίζει πρωταρχικό ρόλο στην προστασία των πληροφοριακών συστημάτων και των δεδομένων, καθώς ακόμη και μια απλή απροσεξία μπορεί να οδηγήσει σε εμφάνιση μείζονος περιστατικού ασφαλείας. Η εκπαίδευση και ενημέρωση στο προσωπικό θα πρέπει να προσαρμοσμένη στα κατάλληλα επίπεδα για:
  - Το προσωπικό του πλοίου, συμπεριλαμβανομένων του πλοιάρχου, των αξιωματικών και του πληρώματος,

- Το προσωπικό που εργάζεται σε θέσης υποστήριξης εκτός πλοίου, όπως στην διαχείριση, την φόρτωση και την λειτουργία του πλοίου.

- Πρόσβαση σε επισκέπτες: Άνθρωποι εκτός του περιβάλλοντος του πλοίου ή της εταιρείας, όπως τεχνικοί, αξιωματικοί λιμένων, εκπρόσωποι, θα πρέπει να έχουν περιορισμένη πρόσβαση σε πληροφοριακά συστήματα του πλοίου. Σε κάθε πρόσωπο, πρέπει να παραχωρούνται μόνον τα δικαιώματα που προβλέπονται στην πολιτική για τον συγκεκριμένο ρόλο που έχει ανατεθεί στο πρόσωπο αυτό.
- Αναβαθμίσεις και συντήρηση λογισμικού: Ιδιαίτερη μέριμνα θα πρέπει να λαμβάνεται για τις ενημερώσεις υλικού και λογισμικού που σχετίζονται με την ασφάλεια: οι ενημερώσεις αυτές θα πρέπει να εγκαθίστανται το συντομότερο δυνατόν, πάντα με τα εχέγγυα της ορθής λειτουργικότητας και με στόχο την ελαχιστοποίηση του ρίσκου. Υλικό ή λογισμικό που δεν υποστηρίζεται πλέον από τον κατασκευαστή ή από τον προγραμματιστή δεν θα δέχεται πλέον ενημερώσεις και θα πρέπει να εξεταστεί η αναβάθμισή του.
- Εργαλεία ενημερώσεων λογισμικού κατά των ιών και κακόβουλου λογισμικού: Πρέπει να θεσπιστούν διαδικασίες ώστε να διασφαλιστεί ότι οι ενημερώσεις θα διανέμονται εγκαίρως στα πλοία και ότι ενημερώνονται απρόσκοπτα και έγκαιρα όλα τα συστήματα του πλοίου.
- Απομακρυσμένη πρόσβαση: Πρέπει να θεσπιστούν πολιτικές και διαδικασίες για τον έλεγχο της απομακρυσμένης πρόσβασης στα πληροφοριακά συστήματα του πλοίου. Θα πρέπει να καθορίζεται πλήρως (α) ποιος έχει πρόσβαση, (β) σε ποιες χρονικές περιόδους επιτρέπεται στον καθένα η πρόσβαση και (γ) σε ποιους πόρους και υπηρεσίες μπορεί ο κάθε χρήστης/υποκείμενο να έχει πρόσβαση.
- Απονομή δικαιωμάτων διαχειριστή: Η απονομή δικαιωμάτων διαχειριστή επιτρέπει τυπικά την πλήρη πρόσβαση στις ρυθμίσεις διαμόρφωσης ενός συστήματος αλλά και στο σύνολο των δεδομένων και συνακόλουθα πρέπει να πραγματοποιείται με προσοχή.
- Έλεγχοι φυσικών και αφαιρούμενων μέσων: Κατά τη μεταφορά δεδομένων από διαφορετικά δίκτυα ή συστήματα, υπάρχει κίνδυνος εισαγωγής κακόβουλου λογισμικού ή υπεξαγωγής δεδομένων. Για τον λόγο αυτό θα πρέπει να αποφεύγεται η χρήση τους.
- Καταστροφή δεδομένων σε εξοπλισμό που πωλείται, αποσύρεται ή διατίθεται: καθώς τα δεδομένα που περιέχονται στον εξοπλισμό μπορεί είναι ευαίσθητα ή εμπιστευτικά, θα

πρέπει να διασφαλίζεται ότι έχουν καταστραφεί με τρόπο που να μην επιτρέπεται η ανάκτησή τους.

- Λήψη υποστήριξης από τα κεντρικά γραφεία και σχέδια έκτακτης ανάγκης: Τα πλοία πρέπει να διαθέτουν πρόσβαση σε τεχνική υποστήριξη σε περίπτωση επιθέσεων ή συμβάντων ασφαλείας που αφορούν πληροφοριακά συστήματα.

7 Ενεργειακή Αποδοτικότητα κατά τη διάρκεια Κυβερνοεπιθέσεων

7.1 Επιπτώσεις κυβερνοεπιθέσεων στην ενεργειακή κατανάλωση των πλοίων

7.1.1 Κυβερνοεπιθέσεις και αποσταθεροποίηση των συστημάτων ελέγχου ενέργειας

Οι κυβερνοεπιθέσεις μπορούν να επηρεάσουν σοβαρά την ενεργειακή απόδοση των πλοίων, αποσταθεροποιώντας τα συστήματα ελέγχου ενέργειας που διαχειρίζονται κρίσιμες λειτουργίες όπως η πρόωση, οι μηχανές και τα ηλεκτρονικά συστήματα. Τα σύγχρονα πλοία εξαρτώνται σε μεγάλο βαθμό από προηγμένα συστήματα αυτοματισμού και διαχείρισης ενέργειας, τα οποία βελτιστοποιούν τη λειτουργία των μηχανών και μειώνουν την κατανάλωση καυσίμων. Ωστόσο, όταν αυτά τα συστήματα δέχονται επίθεση, η αποτελεσματικότητά τους μειώνεται δραστικά, καθώς οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε κρίσιμα δεδομένα ή να τροποποιήσουν τις παραμέτρους λειτουργίας των συστημάτων. Αυτό μπορεί να οδηγήσει σε υπερβολική κατανάλωση ενέργειας, απώλειες δεδομένων, ή ακόμη και διακοπές λειτουργίας (Alzate et al, 2024).

Η αποσταθεροποίηση των συστημάτων ελέγχου ενέργειας μπορεί να έχει άμεσες επιπτώσεις στην κατανάλωση καυσίμου, καθώς η ελάττωση της ακρίβειας στη διαχείριση των μηχανών οδηγεί σε υποβέλτιστη απόδοση. Επιπλέον, η απώλεια ελέγχου του συστήματος μπορεί να αναγκάσει το πλήρωμα να καταφύγει σε χειροκίνητες διαδικασίες, οι οποίες συχνά είναι λιγότερο αποδοτικές από τις αυτοματοποιημένες λύσεις. Οι κυβερνοεπιθέσεις μπορούν επίσης να αποσυντονίσουν τις επικοινωνίες μεταξύ διαφορετικών συστημάτων στο πλοίο, όπως τα συστήματα διαχείρισης καυσίμου και τα συστήματα πρόωσης, επιδεινώνοντας περαιτέρω την ενεργειακή αναποτελεσματικότητα (Alzate et al, 2024).

Σε περίπτωση επιτυχημένης επίθεσης, η αποκατάσταση της ενεργειακής αποδοτικότητας μπορεί να αποδειχθεί δύσκολη και χρονοβόρα, ειδικά όταν τα συστήματα ελέγχου έχουν παραβιαστεί σε

μεγάλη έκταση ή/και βάθος. Οι κυβερνοεπιθέσεις μπορούν να στοχεύσουν όχι μόνο την άμεση λειτουργία του πλοίου, αλλά και τα συστήματα λήψης αποφάσεων για την ενεργειακή διαχείριση. Οι διαταραχές αυτές μπορούν να προκαλέσουν καταστροφικές συνέπειες, όχι μόνο από οικονομική άποψη, αλλά και από την άποψη της ασφάλειας, θέτοντας σε κίνδυνο τόσο το πλήρωμα όσο και το περιβάλλον (Jaramillo Jimenez et al, 2022).

7.1.2 Διακοπές λειτουργίας και αύξηση ενεργειακού κόστους

Οι διακοπές λειτουργίας που προκαλούνται από κυβερνοεπιθέσεις στα πληροφοριακά συστήματα των πλοίων μπορούν να οδηγήσουν σε σημαντική αύξηση του ενεργειακού κόστους. Όταν οι κρίσιμες λειτουργίες του πλοίου, όπως η διαχείριση πρόωσης, οι μηχανές και τα συστήματα ελέγχου καυσίμων, τεθούν εκτός λειτουργίας λόγω κυβερνοεπίθεσης, η αποκατάσταση των συστημάτων μπορεί να απαιτεί χρόνο και εξειδικευμένες λύσεις. Αυτό έχει ως αποτέλεσμα όχι μόνο την αύξηση της κατανάλωσης καυσίμου, καθώς το πλοίο δεν λειτουργεί με την απαραίτητη ενεργειακή αποδοτικότητα, αλλά και την αύξηση του λειτουργικού κόστους λόγω των καθυστερήσεων ή ακόμα και των έκτακτων συντηρήσεων που απαιτούνται (Tam et al, 2016).

Οι διακοπές αυτές συχνά αναγκάζουν τα πληρώματα να στραφούν σε χειροκίνητες διαδικασίες, οι οποίες δεν είναι τόσο ακριβείς όσο τα αυτοματοποιημένα συστήματα ελέγχου, οδηγώντας σε σπατάλη ενέργειας. Τα αυτόματα συστήματα διαχείρισης ενέργειας είναι σχεδιασμένα να προσαρμόζουν τη λειτουργία του πλοίου σε πραγματικό χρόνο για βέλτιστη απόδοση, ενώ σε συνθήκες χειροκίνητου ελέγχου, οι χειρισμοί γίνονται με λιγότερη ακρίβεια και χωρίς δυνατότητα άμεσης προσαρμογής στις ανάγκες του πλοίου (Jaramillo Jimenez et al, 2022).

Επιπλέον, οι κυβερνοεπιθέσεις που διαταράσσουν την παροχή δεδομένων και πληροφοριών για την ενεργειακή κατανάλωση μπορεί να έχουν ως αποτέλεσμα τη λήψη εσφαλμένων αποφάσεων από τα πληρώματα ή τα συστήματα υποστήριξης στη στεριά. Αυτό μπορεί να αυξήσει την κατανάλωση καυσίμου, καθώς και τις πιθανότητες για πιο εκτεταμένες βλάβες που απαιτούν επισκευές, αυξάνοντας περαιτέρω τα κόστη. Τέτοιες επιθέσεις μπορούν να έχουν μακροπρόθεσμες συνέπειες, καθώς η αποκατάσταση της λειτουργίας των συστημάτων και η βελτιστοποίηση της ενεργειακής κατανάλωσης ενδέχεται να απαιτεί επιπλέον χρόνο και κόστος, επηρεάζοντας τη συνολική απόδοση του πλοίου και τον προϋπολογισμό της επιχείρησης (Jaramillo Jimenez et al, 2022).

7.1.3 Επιπτώσεις στις λειτουργίες των μηχανών και της πρόωσης

Οι επιπτώσεις των κυβερνοεπιθέσεων στις λειτουργίες των μηχανών και της πρόωσης ενός πλοίου μπορεί να είναι ιδιαίτερα σημαντικές, επηρεάζοντας άμεσα την επιχειρησιακή ικανότητα και την ενεργειακή απόδοση. Τα συστήματα που ελέγχουν τις μηχανές και την πρόωση είναι υπεύθυνα για τη ρύθμιση της ταχύτητας, την κατανομή ισχύος και την ομαλή λειτουργία του πλοίου. Σε περίπτωση κυβερνοεπίθεσης, αυτά τα κρίσιμα συστήματα μπορεί να παραβιαστούν ή να διακοπεί/διαταραχθεί η λειτουργία τους, προκαλώντας δυσλειτουργίες που επηρεάζουν τη συνολική απόδοση του πλοίου (Potamos et al, 2024).

Όταν τα συστήματα πρόωσης δεν λειτουργούν σωστά, μπορεί να εμφανιστεί ως συνέπεια η αυξημένη κατανάλωση καυσίμων, καθώς οι μηχανές δεν θα λειτουργούν με την απαραίτητη αποδοτικότητα. Επιπλέον, η υποβέλτιστη λειτουργία στις μηχανές μπορεί να προκαλέσει αυξημένες δονήσεις και φθορά, με αποτέλεσμα την ανάγκη για περισσότερες συντηρήσεις και επισκευές, κάτι που αυξάνει τα λειτουργικά κόστη και επηρεάζει τη συνολική ενεργειακή αποδοτικότητα του πλοίου (Tam et al, 2016).

Επίσης, οι κυβερνοεπιθέσεις μπορούν να επηρεάσουν την ικανότητα ελέγχου της ταχύτητας και της πορείας του πλοίου, προκαλώντας ανισορροπίες στην πρόωση και αναγκάζοντας το πλήρωμα να καταφύγει σε χειροκίνητες διαδικασίες. Αυτές οι διαδικασίες, συχνά λιγότερο ακριβείς και αποδοτικές από τα αυτόματα συστήματα, μπορεί να οδηγήσουν σε περαιτέρω σπατάλη καυσίμου και σε αύξηση της διάρκειας του ταξιδιού (Potamos et al, 2024).

Η αποσταθεροποίηση των συστημάτων μηχανών και πρόωσης λόγω κυβερνοεπίθεσης μπορεί να προκαλέσει, επίσης, καθυστερήσεις και να επιφέρει δυσκολίες στη διατήρηση του χρονοδιαγράμματος των δρομολογίων. Αυτές οι καθυστερήσεις επιβαρύνουν τόσο το ενεργειακό κόστος όσο και τη συνολική λειτουργία του πλοίου, καθιστώντας απαραίτητη την ανάπτυξη πιο ανθεκτικών συστημάτων προστασίας από κυβερνοεπιθέσεις για την αποφυγή τέτοιων επιπτώσεων (Tam et al, 2016).

Πίνακας 2. Επιπτώσεις των κυβερνοεπιθέσεων στις λειτουργίες των μηχανών και της πρόωσης

Επιπτώσεις Κυβερνοεπιθέσεων	Περιγραφή
Δυσλειτουργία συστημάτων πρόωσης	Προκαλεί ανεξέλεγκτη κατανάλωση καυσίμων και μειωμένη ενεργειακή απόδοση.
Αυξημένες συντηρήσεις και επισκευές	Οι μηχανές υπόκεινται σε αυξημένη φθορά λόγω δονήσεων και προβλημάτων απόδοσης.
Χειροκίνητες διαδικασίες	Μειωμένη ακρίβεια και αποδοτικότητα κατά τον έλεγχο της ταχύτητας και πορείας.
Καθυστέρηση δρομολογίων	Προβλήματα στον έλεγχο της πρόωσης οδηγούν σε καθυστερήσεις και αυξημένο κόστος.
Αύξηση Λειτουργικού κόστους	Απαιτούνται περισσότερα καύσιμα και συντηρήσεις, αυξάνοντας τα συνολικά κόστη.

7.1.4 Η ενεργειακή αποδοτικότητα υπό καθεστώς απώλειας επικοινωνιών

Η ενεργειακή αποδοτικότητα σε συνθήκες απώλειας επικοινωνιών είναι ένα κρίσιμο θέμα για τη ναυτιλία, καθώς οι διακοπές στην επικοινωνία μπορούν να επηρεάσουν σοβαρά τη λειτουργία των πλοίων και την ικανότητά τους να διαχειρίζονται αποτελεσματικά την ενέργεια. Σε περιπτώσεις απώλειας επικοινωνιών, τα πλοία αντιμετωπίζουν προκλήσεις όπως η αδυναμία πρόσβασης σε πληροφορίες σχετικά με τις συνθήκες της θάλασσας, τα φορτία και τις ρυθμίσεις των συστημάτων πρόωσης. Αυτό μπορεί να οδηγήσει σε λιγότερο αποτελεσματική διαχείριση των πόρων και σε αυξημένη κατανάλωση καυσίμου (Potamos et al, 2024).

Η έλλειψη επικοινωνίας καθιστά δύσκολη την παρακολούθηση των συστημάτων ενέργειας σε πραγματικό χρόνο, περιορίζοντας τη δυνατότητα των πληρωμάτων να ανιχνεύσουν τυχόν ανωμαλίες και να προσαρμόσουν τις ρυθμίσεις για βέλτιστη απόδοση. Όταν τα πλοία δεν μπορούν να συνδεθούν με κεντρικά συστήματα ελέγχου ή με άλλα πλοία, η ικανότητά τους να

ανταλλάσσουν πληροφορίες και να προσαρμόζονται σε μεταβαλλόμενες συνθήκες υποβαθμίζονται (Zhu et al., 2022).

Για να αντιμετωπιστούν αυτές οι προκλήσεις, τα πλοία μπορούν να εφαρμόσουν προληπτικές στρατηγικές, όπως η εκπαίδευση του πληρώματος για τη λειτουργία των συστημάτων ενέργειας χωρίς υποστήριξη επικοινωνίας. Η αυτονομία στη διαχείριση των πόρων και η λήψη αποφάσεων βασισμένων σε προκαθορισμένες διαδικασίες μπορεί να βελτιώσουν την ενεργειακή απόδοση σε περιόδους κρίσης. Επίσης, η εφαρμογή τοπικών συστημάτων παρακολούθησης που λειτουργούν ανεξάρτητα από κεντρικά δίκτυα μπορεί να βοηθήσει στη διατήρηση της παρακολούθησης της κατανάλωσης ενέργειας και της απόδοσης των μηχανών, ακόμη και υπό καθεστώς απώλειας επικοινωνιών (Koutroumpa et al., 2023).

Εν κατακλείδι, η προετοιμασία και η ευελιξία των πληρωμάτων είναι καθοριστικές για τη διασφάλιση της ενεργειακής αποδοτικότητας σε καταστάσεις επικοινωνιακής κρίσης, επιτρέποντας στα πλοία να συνεχίζουν να λειτουργούν με αποδοτικότητα παρά τις προκλήσεις.

7.1.5 Παράδειγμα ενεργειακής αναποτελεσματικότητας λόγω κυβερνοεπίθεσης

Ένα χαρακτηριστικό παράδειγμα μειωμένης ενεργειακής αποτελεσματικότητας λόγω κυβερνοεπίθεσης αφορά μια επίθεση σε συστήματα ελέγχου της πρόωσης ενός μεγάλου εμπορικού πλοίου. Σε αυτή την περίπτωση, οι χάκερ κατάφεραν να παραβιάσουν το σύστημα διαχείρισης της μηχανής, αλλοιώνοντας τις παραμέτρους που ρυθμίζουν την ταχύτητα και την ισχύ του κινητήρα. Ως αποτέλεσμα, οι χειριστές δεν μπορούσαν να διατηρήσουν τη βέλτιστη απόδοση του κινητήρα, με την κατανάλωση καυσίμων να αυξάνεται δραματικά. Το πλοίο συνέχισε τη διαδρομή του με χαμηλότερη απόδοση, καταναλώνοντας σημαντικά περισσότερα καύσιμα από το προβλεπόμενο (Erbas et al, 2024).

Η επίθεση αυτή είχε πολλαπλές συνέπειες. Η αυξημένη κατανάλωση ενέργειας οδήγησε σε υπερβολική χρήση καυσίμων, αυξάνοντας το λειτουργικό κόστος του πλοίου. Παράλληλα, η αναποτελεσματική λειτουργία του κινητήρα είχε αρνητικές επιπτώσεις και στις συνολικές επιδόσεις του πλοίου, καθώς η ταχύτητα και η σταθερότητα της πλεύσης μειώθηκαν, γεγονός που προκάλεσε καθυστερήσεις στο χρονοδιάγραμμα παράδοσης του φορτίου. Η επίθεση δημιούργησε

επίσης αυξημένη ανάγκη για τη συντήρηση του πλοίου, καθώς η παρατεταμένη λειτουργία υπό αυτές τις συνθήκες θα μπορούσε να προκαλέσει φθορά στα εξαρτήματα του κινητήρα και ανάγκη για επιπλέον επισκευές (Erbas et al, 2024).

Το συγκεκριμένο παράδειγμα υπογραμμίζει πόσο ευάλωτο μπορεί να είναι ένα πλοίο απέναντι σε κυβερνοεπιθέσεις, ειδικά όσον αφορά την ενεργειακή του αποδοτικότητα. Οι επιθέσεις αυτές όχι μόνο επιβαρύνουν το κόστος λειτουργίας λόγω της αυξημένης κατανάλωσης καυσίμων, αλλά μπορούν επίσης να θέσουν σε κίνδυνο την ασφάλεια του πλοίου και να προκαλέσουν μακροχρόνια ζημιά στα συστήματα του. Αυτή η περίπτωση αναδεικνύει την ανάγκη για αυστηρότερα μέτρα προστασίας και ενεργειακή διαχείριση σε περιπτώσεις κυβερνοεπιθέσεων (Potamos et al, 2024).

7.2 Στρατηγικές εξοικονόμησης ενέργειας σε περίπτωση επίθεσης

7.2.1 Άμεσες παρεμβάσεις για αποκατάσταση ενεργειακής ισορροπίας

Σε περίπτωση κυβερνοεπίθεσης που επηρεάζει την ενεργειακή αποδοτικότητα ενός πλοίου, οι άμεσες παρεμβάσεις είναι κρίσιμες για την αποκατάσταση της ενεργειακής ισορροπίας και τη μείωση των αρνητικών συνεπειών. Η πρώτη και πιο άμεση δράση είναι η απομόνωση των προσβεβλημένων συστημάτων, έτσι ώστε να σταματήσει η περαιτέρω εξάπλωση της επίθεσης. Οι διαχειριστές των συστημάτων θα πρέπει να επαναφέρουν τις λειτουργίες του πλοίου σε χειροκίνητη λειτουργία όπου αυτό είναι εφικτό, διατηρώντας έτσι τον έλεγχο των βασικών μηχανών και της πρόωσης, με στόχο την ελαχιστοποίηση της ενεργειακής κατανάλωσης (Tam et al, 2016).

Μια ακόμη κρίσιμη παρέμβαση αφορά τη χρήση εφεδρικών συστημάτων και διαδικασιών που μπορούν να υποκαταστήσουν τα κύρια συστήματα ελέγχου, τα οποία έχουν υποστεί ζημιά. Για παράδειγμα, τα εφεδρικά ενεργειακά συστήματα και οι μηχανισμοί ελέγχου της πρόωσης μπορούν να ενεργοποιηθούν προκειμένου να διατηρηθεί η ενεργειακή απόδοση του πλοίου σε ασφαλή επίπεδα. Παράλληλα, η άμεση αξιολόγηση της κατάστασης από τις τεχνικές ομάδες θα επιτρέψει τη λήψη στοχευμένων μέτρων για την αντιμετώπιση των ζημιών στα συστήματα ελέγχου, βοηθώντας έτσι στην αποκατάσταση της ενεργειακής ισορροπίας (Yang et al, 2023).

Επιπλέον, οι μηχανικοί και οι αξιωματικοί του πλοίου θα πρέπει να εφαρμόσουν στρατηγικές εξοικονόμησης ενέργειας, όπως η μείωση της ταχύτητας πλεύσης και η βελτιστοποίηση της

πορείας του πλοίου, ώστε να μειωθεί η κατανάλωση καυσίμων κατά τη διάρκεια της κρίσης. Τέτοιες αντιμετωπίσεις όχι μόνο θα συμβάλουν στη διατήρηση της ενεργειακής ισορροπίας, αλλά θα περιορίσουν και τις οικονομικές επιπτώσεις της αυξημένης κατανάλωσης (Yang et al, 2023).

Τέλος, είναι σημαντικό να παρακολουθείται συνεχώς η κατάσταση των ενεργειακών αναγκών του πλοίου, προκειμένου να αναπροσαρμόζονται οι στρατηγικές και να λαμβάνονται έγκαιρες αποφάσεις, που θα βοηθήσουν στην επαναφορά της ενεργειακής αποδοτικότητας και στην εξομάλυνση της λειτουργίας του πλοίου.

7.2.2 Ρόλος των εφεδρικών συστημάτων στη διαχείριση ενέργειας

Τα εφεδρικά συστήματα διαδραματίζουν κρίσιμο ρόλο στη διαχείριση της ενέργειας, ιδιαίτερα κατά τη διάρκεια κρίσεων, όπως οι κυβερνοεπιθέσεις, που επηρεάζουν την κανονική λειτουργία των πλοίων. Αυτά τα συστήματα έχουν σχεδιαστεί για να υποστηρίζουν τις βασικές λειτουργίες του πλοίου, όταν τα κύρια συστήματα ελέγχου καταστούν αδρανή ή δυσλειτουργούν. Η ενεργοποίησή τους αποτελεί άμεση και απαραίτητη ενέργεια, η οποία μπορεί να διασφαλίσει την αδιάλειπτη λειτουργία των βασικών μηχανών, της πρόωσης και των άλλων ενεργειακών αναγκών του πλοίου, ενώ συμβάλλουν καθοριστικά στη μείωση των κινδύνων που σχετίζονται με τη συνολική ενεργειακή αναποτελεσματικότητα (Erbas et al, 2024).

Ένα από τα βασικά πλεονεκτήματα των εφεδρικών συστημάτων είναι η ικανότητά τους να παρέχουν γρήγορη εναλλακτική λύση σε περίπτωση δυσλειτουργίας, διασφαλίζοντας ότι το πλοίο θα συνεχίσει να λειτουργεί με επαρκή ενεργειακή απόδοση, ακόμα και υπάρχει αστοχία στα κύρια συστήματα. Για παράδειγμα, οι εφεδρικές γεννήτριες μπορούν να αναλάβουν την παροχή ενέργειας, ενώ τα συστήματα ελέγχου της πρόωσης μπορούν να ρυθμιστούν χειροκίνητα ή αυτόματα για να εξασφαλιστεί η ασφαλής πλεύση (Jaramillo Jimenez et al, 2022).

Επιπλέον, τα εφεδρικά συστήματα διαδραματίζουν σημαντικό ρόλο στη διατήρηση της ευστάθειας του πλοίου σε ενεργειακά κρίσιμες στιγμές, προσφέροντας χρόνο στους διαχειριστές για να επιδιορθώσουν τις βλάβες ή να αναβαθμίσουν τα κύρια συστήματα. Η ύπαρξη ενός καλά σχεδιασμένου συστήματος εφεδρείας μειώνει τις πιθανότητες πλήρους ενεργειακής κατάρρευσης και εξασφαλίζει την αποτελεσματική λειτουργία του πλοίου σε συνθήκες έκτακτης ανάγκης. Συνεπώς, η σωστή συντήρηση και η τακτική δοκιμή των εφεδρικών συστημάτων είναι ουσιώδη

στοιχεία για τη συνολική ενεργειακή αποδοτικότητα του πλοίου, ιδίως σε καταστάσεις που θέτουν σε κίνδυνο την ασφάλεια και τη λειτουργία του (Jaramillo Jimenez et al, 2022).

7.2.3 Οικονομικές στρατηγικές για μείωση του κόστους ενέργειας κατά την επίθεση

Οι οικονομικές στρατηγικές για τη μείωση του κόστους ενέργειας κατά τη διάρκεια μιας κυβερνοεπίθεσης διαδραματίζουν καθοριστικό ρόλο στη διατήρηση της βιωσιμότητας και της λειτουργικότητας του πλοίου. Θα πρέπει αρχικά να πραγματοποιηθεί άμεση αξιολόγηση της κατάστασης και ελαχιστοποίηση της κατανάλωσης ενέργειας μέσω περιορισμού των μη κρίσιμων λειτουργιών. Αυτό μπορεί να επιτευχθεί με την προσωρινή απενεργοποίηση των συστημάτων που δεν είναι απαραίτητα για την ασφαλή πλεύση ή τις επιχειρησιακές ανάγκες, εξοικονομώντας ενέργεια για τις πιο κρίσιμες διεργασίες (Dimakopoulou & Rantos, 2024).

Ένα άλλο σημαντικό μέτρο είναι η χρήση εναλλακτικών πηγών ενέργειας, όπως τα εφεδρικά συστήματα ή οι μπαταρίες, που μπορούν να διατηρήσουν την ενεργειακή ισορροπία χωρίς να επιβαρύνουν τα κύρια συστήματα. Η υιοθέτηση αυτών των συστημάτων μπορεί να περιορίσει την ενεργειακή κατανάλωση και το κόστος, ενώ παράλληλα εξασφαλίζει την απρόσκοπτη λειτουργία των βασικών μηχανών και συστημάτων. Επιπλέον, η χρήση καινοτόμων τεχνολογιών που προσφέρουν ενεργειακή αποδοτικότητα, όπως έξυπνα συστήματα διαχείρισης ενέργειας, μπορεί να βελτιώσει την απόδοση κατά τη διάρκεια μιας επίθεσης (Dimakopoulou & Rantos, 2024).

Μακροπρόθεσμα, οι επενδύσεις σε τεχνολογίες που βελτιστοποιούν τη χρήση της ενέργειας και μειώνουν την εξάρτηση από τα παραδοσιακά καύσιμα μπορούν να βοηθήσουν στη μείωση του κόστους. Για παράδειγμα, η μετάβαση σε πιο αποδοτικά καύσιμα, όπως τα βιοκαύσιμα ή οι τεχνολογίες ανανεώσιμων πηγών ενέργειας, μπορεί να μειώσει την επιβάρυνση των συστημάτων και το κόστος λειτουργίας σε κρίσιμες στιγμές (Poulsen et al, 2022)

Τέλος, η εκπαίδευση του προσωπικού στη διαχείριση κρίσεων και ενεργειακής αποδοτικότητας, σε συνδυασμό με την εφαρμογή ολοκληρωμένων πολιτικών ασφάλειας, συμβάλλει στη μείωση των κινδύνων και του ενεργειακού κόστους κατά τη διάρκεια μιας επίθεσης.

7.2.4 Ενεργειακά αποδοτικές επιλογές διαδρομής σε συνθήκες έκτακτης ανάγκης

Σε συνθήκες έκτακτης ανάγκης, όπως μια κυβερνοεπίθεση που επηρεάζει τα συστήματα πλοήγησης και ενέργειας, η επιλογή ενεργειακά αποδοτικών διαδρομών είναι κρίσιμη για τη διατήρηση της ασφάλειας και της λειτουργικότητας του πλοίου. Η ενεργειακή αποδοτικότητα σε τέτοιες καταστάσεις προϋποθέτει τη χρήση τεχνολογιών που μπορούν να αναλύουν και να υποδεικνύουν εναλλακτικές διαδρομές με βάση τις τρέχουσες συνθήκες. Αυτές οι επιλογές πρέπει να συνυπολογίζουν παράγοντες όπως η ταχύτητα του ανέμου, τα θαλάσσια ρεύματα και η κατανάλωση καυσίμων, έτσι ώστε να μειωθεί η κατανάλωση ενέργειας και να παραταθεί η διάρκεια της αυτονομίας του πλοίου (Tam et al, 2016).

Ένας από τους πιο αποδοτικούς τρόπους για την εξοικονόμηση ενέργειας είναι η επιλογή μιας διαδρομής που ελαχιστοποιεί τις αντιξοότητες, όπως οι περιοχές με αντίθετα ρεύματα ή έντονες καιρικές συνθήκες. Αυτές οι παράμετροι μπορούν να επηρεάσουν σημαντικά την κατανάλωση καυσίμου, ιδιαίτερα όταν το πλοίο βρίσκεται υπό περιορισμούς λόγω μιας κυβερνοεπίθεσης. Η χρήση εναλλακτικών συστημάτων πλοήγησης, τα οποία είναι λιγότερο ευάλωτα σε επιθέσεις, μπορεί να βοηθήσει στην εξεύρεση ασφαλών και ενεργειακά αποδοτικών διαδρομών (Deloitte, 2022).

Παράλληλα, η προσαρμογή της ταχύτητας του πλοίου είναι ένας πρόσθετος σημαντικός παράγοντας. Σε πολλές περιπτώσεις, η μείωση της ταχύτητας μπορεί να οδηγήσει σε σημαντική μείωση της κατανάλωσης ενέργειας, χωρίς να θέτει σε κίνδυνο την ασφάλεια. Η συνεργασία μεταξύ του προσωπικού πλοήγησης και των μηχανικών για την αξιολόγηση των δεδομένων σε πραγματικό χρόνο είναι μεγάλης σημασίας, ώστε να λαμβάνονται οι καλύτερες αποφάσεις σχετικά με την κατεύθυνση και την ταχύτητα του πλοίου (Poulsen et al, 2022)

Συνολικά, η ενεργειακά αποδοτική επιλογή διαδρομής σε συνθήκες έκτακτης ανάγκης απαιτεί ταχύτητα αντίδρασης, ακριβή δεδομένα και σωστή ανάλυση των επικρατουσών συνθηκών, με σκοπό τη μεγιστοποίηση της ενεργειακής αποδοτικότητας και την ελαχιστοποίηση του ρίσκου.

7.2.5 Συνεργασία με παρόχους τεχνολογίας για άμεσες λύσεις εξοικονόμησης

Η συνεργασία με παρόχους τεχνολογίας είναι σημαντική για την ανάπτυξη άμεσων λύσεων εξοικονόμησης ενέργειας σε περιπτώσεις κυβερνοεπιθέσεων. Οι εταιρείες αυτές διαθέτουν την τεχνογνωσία και τα εργαλεία που μπορούν να ενισχύσουν τη διαχείριση της ενέργειας στα πλοία, επιτρέποντας τη γρήγορη αποκατάσταση της λειτουργικότητας και την προσαρμογή σε έκτακτες συνθήκες. Η τεχνολογία διαχείρισης ενέργειας (Energy Management Systems - EMS) μπορεί να ενσωματωθεί στα πλοία για την παρακολούθηση και τη βελτιστοποίηση της κατανάλωσης ενέργειας σε πραγματικό χρόνο (Deloitte, 2022).

Η εφαρμογή καινοτόμων τεχνολογιών, όπως οι αλγόριθμοι πρόβλεψης κατανάλωσης, μπορεί να βοηθήσει τους πλοιάρχους και τους μηχανικούς να λάβουν πιο ορθές και ενημερωμένες αποφάσεις κατά τη διάρκεια μιας κρίσης. Οι πάροχοι τεχνολογίας μπορούν να παρέχουν υποστήριξη και καθοδήγηση στην εφαρμογή λύσεων που βελτιώνουν την ενεργειακή αποδοτικότητα, όπως είναι τα συστήματα αυτόματης ρύθμισης καυσίμου ή τα συστήματα ανάκτησης ενέργειας από τις μηχανές. Αυτές οι λύσεις μπορούν να μειώσουν την εξάρτηση από εξωτερικούς πόρους, ελαχιστοποιώντας την κατανάλωση ενέργειας και τα λειτουργικά κόστη (Tam et al, 2016).

Επιπλέον, οι συνεργασίες αυτές μπορούν να περιλαμβάνουν τη συνεχή εκπαίδευση του πληρώματος σχετικά με την αποτελεσματική χρήση των συστημάτων διαχείρισης ενέργειας. Με την κατάλληλη εκπαίδευση και υποστήριξη, το πλήρωμα μπορεί να είναι σε θέση να αντεπεξέλθει γρηγορότερα σε προβλήματα που σχετίζονται με την ενέργεια, εφαρμόζοντας άμεσα στρατηγικές εξοικονόμησης (Deloitte, 2022).

Εν τέλει, η συνεργασία με παρόχους τεχνολογίας είναι θεμελιώδους σημασίας για τη διαχείριση των προκλήσεων που προκύπτουν από κυβερνοεπιθέσεις, προκειμένου να διασφαλιστεί η ενεργειακή αποδοτικότητα και η ασφάλεια των πλοίων σε κρίσιμες καταστάσεις.

7.3 Αναδυόμενες τεχνολογίες για την ενεργειακή αποδοτικότητα υπό συνθήκες έκτακτης ανάγκης

Στις ενότητες που ακολουθούν εξετάζεται η χρήση αναδυόμενων τεχνολογιών για την ενεργειακή αποδοτικότητα υπό συνθήκες έκτακτης ανάγκης. Ειδικότερα αναλύεται (α) η χρήση της τεχνητής

νοημοσύνης για ανάλυση ενεργειακής κατανάλωσης σε πραγματικό χρόνο, (β) η αυτοματοποίηση συστημάτων πρόωσης για βέλτιστη ενεργειακή διαχείριση, (γ) τα έξυπνα συστήματα παρακολούθησης καυσίμου σε περιπτώσεις κυβερνοεπίθεσης, (δ) τα δικτυακά ενεργειακά συστήματα για τη μείωση των απωλειών και (ε) η χρήση Blockchain για ασφαλή διαχείριση δεδομένων ενέργειας.

7.3.1 Τεχνητή νοημοσύνη για ανάλυση ενεργειακής κατανάλωσης σε πραγματικό χρόνο

Η τεχνητή νοημοσύνη (ΤΝ) έχει αναδιαρθρώσει τη διαδικασία ανάλυσης της κατανάλωσης ενέργειας των πλοίων, προσφέροντας τη δυνατότητα παρακολούθησης και αξιολόγησης σε πραγματικό χρόνο. Μέσω προηγμένων αλγορίθμων μηχανικής μάθησης, οι εφαρμογές ΤΝ είναι σε θέση να επεξεργάζονται μεγάλα σύνολα δεδομένων από διάφορες πηγές, όπως αισθητήρες και συστήματα διαχείρισης ενέργειας, και να αναγνωρίζουν πρότυπα και τάσεις στη χρήση ενέργειας (Tam et al, 2016).

Η ικανότητα της ΤΝ να εντοπίζει ανωμαλίες στην κατανάλωση ενέργειας είναι εξαιρετικά χρήσιμη, ιδιαίτερα σε περιπτώσεις κυβερνοεπιθέσεων ή τεχνικών προβλημάτων. Για παράδειγμα, εάν εντοπιστεί μια ξαφνική αύξηση στην κατανάλωση ενέργειας, οι αλγόριθμοι μπορούν να αποστείλουν άμεσα ειδοποιήσεις για να εξεταστεί η κατάσταση, βοηθώντας στην άμεση κινητοποίηση και αποκατάσταση τυχόν ζημιών. Αυτό επιτρέπει την ταχεία αντίδραση και την ελαχιστοποίηση των επιπτώσεων που μπορεί να προκύψουν από διακοπές λειτουργίας ή ενεργειακή αναποτελεσματικότητα (Tam et al, 2016).

Επιπλέον, η ΤΝ μπορεί να προτείνει στρατηγικές βελτιστοποίησης της κατανάλωσης ενέργειας, προσαρμόζοντας τις ρυθμίσεις των συστημάτων με βάση τις πραγματικές συνθήκες και απαιτήσεις. Αυτό περιλαμβάνει τη βελτίωση των διαδικασιών ελέγχου μηχανών, την προσαρμογή των επιπέδων ισχύος και τη διαχείριση των φορτίων. Η ενσωμάτωση της Τ.Ν. στα πληροφοριακά συστήματα καθιστά δυνατή τη συνεχή βελτίωση των ενεργειακών επιδόσεων, συμβάλλοντας σε μια πιο βιώσιμη και αποδοτική ναυτιλία (Tam et al, 2016).

Τέλος, η δυνατότητα προβλέψεων για μελλοντική κατανάλωση ενέργειας βασισμένη σε ιστορικά δεδομένα και προσαρμοσμένα μοντέλα μπορεί να βοηθήσει τις ναυτιλιακές εταιρείες να

προγραμματίζουν καλύτερα τις ανάγκες τους, μειώνοντας το συνολικό κόστος και τις περιβαλλοντικές επιπτώσεις. Η αξιοποίηση της ΤΝ στην ανάλυση της ενεργειακής κατανάλωσης είναι, επομένως, καθοριστικής σημασίας για την επίτευξη ενός πιο αποδοτικού και ασφαλούς ναυτιλιακού τομέα.

7.3.2 Αυτοματοποίηση συστημάτων πρόωσης για βέλτιστη ενεργειακή διαχείριση

Η αυτοματοποίηση των συστημάτων πρόωσης στα πλοία είναι κρίσιμη για τη βέλτιστη ενεργειακή διαχείριση, ιδίως σε περιόδους αυξημένων προκλήσεων όπως κυβερνοεπιθέσεις. Οι σύγχρονες τεχνολογίες αυτοματισμού επιτρέπουν τη συνεχή παρακολούθηση και ρύθμιση των παραμέτρων λειτουργίας των μηχανών και των συστημάτων πρόωσης, εξασφαλίζοντας ότι η ενέργεια χρησιμοποιείται με τον πιο αποδοτικό τρόπο (NIST, 2023).

Μέσω προηγμένων αισθητήρων και συστημάτων ελέγχου, οι αυτοματοποιημένες λύσεις μπορούν να αναλύουν σε πραγματικό χρόνο δεδομένα σχετικά με την κατανάλωση ενέργειας, την κατάσταση των μηχανών και τις εξωτερικές συνθήκες. Αυτή η πληροφορία επιτρέπει την αυτόματη ρύθμιση των ρυθμών πρόωσης και της κατανάλωσης καυσίμου, εξασφαλίζοντας ότι οι μηχανές λειτουργούν πάντα στην πιο αποδοτική τους κατάσταση. Με τον τρόπο αυτό, μειώνεται η κατανάλωση καυσίμου και οι εκπομπές ρύπων, συμβάλλοντας στη βιωσιμότητα της ναυτιλίας (NIST, 2023).

Επιπλέον, οι αυτοματοποιημένες λύσεις μπορούν να ενσωματώσουν αλγορίθμους πρόβλεψης, οι οποίοι αναλύουν τα ιστορικά δεδομένα για να προσαρμόσουν τη λειτουργία των συστημάτων πρόωσης σε πραγματικό χρόνο, με στόχο τη μέγιστη ενεργειακή αποδοτικότητα. Η δυνατότητα έγκαιρης αντίδρασης σε ανωμαλίες, όπως η αύξηση της κατανάλωσης ενέργειας ή η δυσλειτουργία των μηχανών, μπορεί να αποτρέψει σοβαρές επιπτώσεις που μπορεί να προκύψουν από κυβερνοεπιθέσεις ή τεχνικά προβλήματα (Afenyo & Caesar, 2023).

Η υιοθέτηση τέτοιων αυτοματοποιημένων συστημάτων πρόωσης επιτρέπει στις ναυτιλιακές εταιρείες να ενισχύσουν την ενεργειακή τους αποδοτικότητα και να βελτιώσουν τη συνολική απόδοση των πλοίων τους. Η διαρκής παρακολούθηση και προσαρμογή των συνθηκών λειτουργίας είναι σημαντική για την επιτυχία των επιχειρήσεων στη σύγχρονη ναυτιλία,

προσφέροντας ταυτόχρονα και οικονομικά οφέλη μέσω της μείωσης του κόστους καυσίμου και της αύξησης της αξιοπιστίας των συστημάτων πρόωσης.

7.3.3 Έξυπνα συστήματα παρακολούθησης καυσίμου σε περιπτώσεις κυβερνοεπίθεσης

Η ανάπτυξη έξυπνων συστημάτων παρακολούθησης καυσίμου είναι κρίσιμη για τη διασφάλιση της ενεργειακής αποδοτικότητας και της ασφάλειας των πλοίων, ιδίως σε περιπτώσεις κυβερνοεπίθεσης. Αυτά τα συστήματα χρησιμοποιούν προηγμένες τεχνολογίες, όπως αισθητήρες, IoT (Internet of Things) και τεχνητή νοημοσύνη, για να παρακολουθούν και να αναλύουν σε πραγματικό χρόνο την κατανάλωση καυσίμου, παρέχοντας σημαντικές πληροφορίες σχετικά με τη λειτουργία των μηχανών και την αποδοτικότητα της πρόωσης (Afenyo & Caesar, 2023).

Μέσω της συλλογής δεδομένων από πολλαπλές πηγές, τα έξυπνα συστήματα παρακολούθησης μπορούν να εντοπίζουν ανωμαλίες στη χρήση καυσίμου, οι οποίες μπορεί να υποδεικνύουν διαρροές ή κακόβουλες επιθέσεις. Εάν ένα πλοίο υποστεί κυβερνοεπίθεση, αυτά τα συστήματα μπορούν να ειδοποιούν αμέσως το πλήρωμα για τις ασυνήθιστες διακυμάνσεις στην κατανάλωση καυσίμου, επιτρέποντας την ταχεία αντίδραση και τη λήψη μέτρων, προκειμένου για την αποκατάσταση της κανονικότητας (Afenyo & Caesar, 2023).

Επιπλέον, η ανάλυση των δεδομένων καυσίμου μπορεί να συμβάλει στη βελτιστοποίηση των διαδρομών πλοίων, επιλέγοντας εκείνες που απαιτούν λιγότερη ενέργεια. Μέσω αλγορίθμων μηχανικής μάθησης, οι υπολογιστικές πλατφόρμες των έξυπνων συστημάτων μπορούν να προσαρμόζουν τις στρατηγικές διαχείρισης καυσίμου βάσει των αναγκών και των προκλήσεων που προκύπτουν κατά τη διάρκεια μιας κυβερνοεπίθεσης (Yang et al, 2023).

Η υιοθέτηση αυτών των έξυπνων συστημάτων δεν ενισχύει μόνο την ασφάλεια των πλοίων, αλλά και τη βιωσιμότητα των λειτουργιών τους. Στη σύγχρονη ναυτιλία, η ενσωμάτωση έξυπνων τεχνολογιών παρακολούθησης καυσίμου αποτελεί αναγκαία στρατηγική για τη διασφάλιση της αποδοτικής και ασφαλούς λειτουργίας των πλοίων, ιδίως σε περιόδους αυξημένης απειλής από κυβερνοεπιθέσεις.

7.3.4 Δικτυακά ενεργειακά συστήματα για τη μείωση των απωλειών

Η ανάπτυξη δικτυακών ενεργειακών συστημάτων είναι κρίσιμη για τη μείωση των απωλειών ενέργειας στα πλοία, ειδικά κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης όπως οι κυβερνοεπιθέσεις. Αυτά τα συστήματα αξιοποιούν την τεχνολογία του διαδικτύου και την επικοινωνία μεταξύ των διαφόρων υποσυστημάτων του πλοίου (Dimakopoulou & Rantos, 2024).

Η παρακολούθηση των ενεργειακών ροών και η ανάλυση των δεδομένων που σχετίζονται με τη χρήση ενέργειας προσφέρουν τη δυνατότητα εντοπισμού αναποτελεσματικών διαδικασιών και εξοπλισμού. Με αυτόν τον τρόπο, οι διαχειριστές του πλοίου μπορούν να προβαίνουν σε άμεσες παρεμβάσεις για τη βελτίωση της αποδοτικότητας και τη μείωση των απωλειών. Επιπλέον, η συγκέντρωση και ανάλυση των δεδομένων επιτρέπει την ανάπτυξη στρατηγικών πρόληψης και απόκρισης σε κυβερνοεπιθέσεις, ελαχιστοποιώντας τις συνέπειές τους στην κατανάλωση ενέργειας (Tam et al, 2016).

Η εφαρμογή δικτυακών ενεργειακών συστημάτων παρέχει τη δυνατότητα διαχείρισης των ενεργειακών πόρων με περισσότερη ακρίβεια και αποτελεσματικότητα. Με τη βοήθεια αισθητήρων και τεχνολογιών IoT, οι διαχειριστές μπορούν να ελέγχουν και να ρυθμίζουν αυτόματα τα συστήματα πρόωσης και ενέργειας του πλοίου, προσαρμόζοντας τις λειτουργίες τους σε πραγματικό χρόνο ανάλογα με τις ανάγκες (Dimakopoulou & Rantos, 2024).

Αυτή η προσαρμοστικότητα είναι ιδιαίτερα σημαντική σε περιπτώσεις κυβερνοεπίθεσης, όπου οι συσκευές και τα δίκτυα μπορεί να υποστούν επιθέσεις που επηρεάζουν την ενεργειακή τους απόδοση. Η ικανότητα των δικτυακών ενεργειακών συστημάτων να αντιδρούν άμεσα και να προσαρμόζονται σε νέα δεδομένα μπορεί να συμβάλλει καθοριστικά στη διασφάλιση της αποδοτικής και ασφαλούς λειτουργίας των πλοίων.

7.3.5 Blockchain για ασφαλή διαχείριση δεδομένων ενέργειας

Η τεχνολογία blockchain αναδεικνύεται ως μια καινοτόμος λύση για την ασφαλή διαχείριση των δεδομένων ενέργειας, προσφέροντας αξιοπιστία και διαφάνεια σε ένα πεδίο που συχνά πλήττεται από κυβερνοεπιθέσεις και επιπλέον έχει αυξημένες ανάγκες για αξιόπιστη καταγραφή και ανάλυση. Λόγω της αποκεντρωμένης φύσης του δικτύου, το blockchain επιτρέπει την καταγραφή των δεδομένων σε πολλές θέσεις ταυτόχρονα, διασφαλίζοντας ότι καμία μεμονωμένη οντότητα

δεν έχει πλήρη έλεγχο ή πρόσβαση σε όλα τα δεδομένα. Αυτό το χαρακτηριστικό είναι σημαντκό για τη δημιουργία εμπιστοσύνης μεταξύ των χρηστών, των παρόχων ενέργειας και των ρυθμιστικών αρχών (Fu et al, 2019).

Η ασφάλεια που παρέχει το blockchain οφείλεται στη χρήση κρυπτογραφικών αλγορίθμων, οι οποίοι καθιστούν τις καταχωρίσεις πρακτικά αδύνατο να τροποποιηθούν ή να διαγραφούν. Σε περιπτώσεις κυβερνοεπίθεσης, αυτή η χαρακτηριστική ακεραιότητα των δεδομένων προστατεύει τις πληροφορίες σχετικά με την κατανάλωση και τη διανομή ενέργειας, διασφαλίζοντας ότι οι χρήστες έχουν πρόσβαση μόνο σε έγκυρα και αξιόπιστα δεδομένα (Fu et al, 2019).

Επιπλέον, η χρήση blockchain διευκολύνει την παρακολούθηση της ενέργειας από την παραγωγή έως την κατανάλωση, παρέχοντας μια καθαρή εικόνα της ενεργειακής ροής. Αυτό μπορεί να ενισχύσει την αποδοτικότητα και να μειώσει τις σπατάλες, καθώς οι χρήστες μπορούν να δουν τις ενεργειακές τους συνήθειες σε πραγματικό χρόνο και να προσαρμόσουν τη συμπεριφορά τους ανάλογα (Liu et al, 2019).

Η ενσωμάτωση έξυπνων συμβολαίων (smart contracts) στο blockchain προσφέρει επίσης τη δυνατότητα αυτοματοποίησης διαδικασιών, όπως η διαχείριση συμβολαίων και οι πληρωμές, μειώνοντας έτσι τα κόστη και την ανάγκη για μεσάζοντες. Αυτές οι δυνατότητες καθιστούν το blockchain ένα αναγκαίο εργαλείο για την ασφαλή και αποτελεσματική διαχείριση των δεδομένων ενέργειας, προάγοντας τη βιωσιμότητα και την ασφάλεια στον τομέα της ενέργειας (Liu et al, 2019).

7.4 Παραδείγματα εφαρμογής συστημάτων εξοικονόμησης ενέργειας σε πραγματικές συνθήκες κυβερνοεπίθεσης

Στις ακόλουθες παραγράφους παρατίθενται συγκεκριμένα παραδείγματα/μελέτες περίπτωσης που αφορούν την εξοικονόμηση ενέργειας σε πραγματικές συνθήκες κυβερνοεπίθεσης.

7.4.1 Μελέτη περίπτωσης: Εφαρμογή αυτόματου ελέγχου ενέργειας σε πλοία

Η εφαρμογή αυτόματου ελέγχου ενέργειας στα πλοία έχει επιφέρει σημαντικές μεταβολές στη διαχείριση των ενεργειακών πόρων, προσφέροντας σημαντικά οφέλη αναφορικά με τη λειτουργία και την αποδοτικότητα. Με την ανάπτυξη και την εφαρμογή συστημάτων αυτοματισμού, οι

πλοιοκτήτες μπορούν να παρακολουθούν και να διαχειρίζονται την κατανάλωση ενέργειας σε πραγματικό χρόνο, βελτιώνοντας την απόδοση και μειώνοντας τα λειτουργικά έξοδα (Yang, 2023).

Στην περίπτωση των πλοίων, η ενσωμάτωση συστημάτων αυτόματου ελέγχου επιτρέπει τη ρύθμιση των μηχανών και των ηλεκτρικών συστημάτων ανάλογα με τις απαιτήσεις φορτίου και τις συνθήκες πλεύσης. Για παράδειγμα, σε πλοία που χρησιμοποιούν σύγχρονα συστήματα ελέγχου, οι αισθητήρες παρακολουθούν συνεχώς τις παραμέτρους απόδοσης, όπως η ταχύτητα, η κατανάλωση καυσίμου και οι περιβαλλοντικές συνθήκες. Αυτά τα δεδομένα αναλύονται σε πραγματικό χρόνο, επιτρέποντας την προσαρμογή των ρυθμίσεων των μηχανών ώστε να επιτυγχάνεται η μέγιστη ενεργειακή αποδοτικότητα (Tam et al, 2016).

Ένα παράδειγμα επιτυχούς εφαρμογής αυτόματου ελέγχου ενέργειας είναι η υλοποίηση του συστήματος Energy Management System (EMS) σε εμπορικά πλοία. Το EMS αξιοποιεί αλγορίθμους μηχανικής μάθησης για να προβλέψει τις ενεργειακές ανάγκες βάσει ιστορικών δεδομένων και μοντέλων κίνησης. Η αυτοματοποίηση αυτής της διαδικασίας μειώνει την ανθρώπινη παρέμβαση, ελαχιστοποιώντας τα σφάλματα και βελτιώνοντας την αντίδραση του πλοίου σε μεταβαλλόμενες συνθήκες (Yang, 2023).

Οι πλοιοκτήτες αναγνωρίζουν τα οφέλη της υιοθέτησης τέτοιων τεχνολογιών, καθώς η βελτιωμένη ενεργειακή αποδοτικότητα συνεισφέρει στη μείωση του περιβαλλοντικού αποτυπώματος των πλοίων και ενισχύει τη συμμόρφωση με τις κανονιστικές ρυθμίσεις. Η εφαρμογή αυτόματου ελέγχου ενέργειας όχι μόνο προσφέρει οικονομικά οφέλη, αλλά και προάγει τη βιωσιμότητα στον τομέα της ναυτιλίας.

7.4.2 Υποβάθμιση ενεργειακής απόδοσης κατά την κυβερνοεπίθεση σε δεξαμενόπλοιο

Η υποβάθμιση της ενεργειακής απόδοσης κατά την κυβερνοεπίθεση σε ένα δεξαμενόπλοιο αναδεικνύει σοβαρές αδυναμίες στα συστήματα διαχείρισης ενέργειας και ασφάλειας. Όταν οι κυβερνοεπιθέσεις στοχεύουν στη διακοπή ή την κακόβουλη τροποποίηση της λειτουργίας των συστημάτων πρόωσης και ελέγχου, οι συνέπειες είναι άμεσες και καταστροφικές. Πρώτον, οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση σε κρίσιμες πληροφορίες σχετικά με τη

λειτουργία των μηχανών, με αποτέλεσμα τη σπατάλη ενέργειας και την αυξημένη κατανάλωση καυσίμου. Η εμφάνιση προβλημάτων στον έλεγχο των μηχανών οδηγούν σε υποβέλτιστες ρυθμίσεις, οι οποίες καθιστούν ανέφικτη την επίτευξη βέλτιστης ενεργειακής απόδοσης (ISO, 2022).

Δεύτερον, οι κυβερνοεπιθέσεις συχνά προκαλούν διακοπές στη λειτουργία των συστημάτων, οι οποίες ενδέχεται να δημιουργήσουν ανάγκες για επανεκκίνηση ή ακόμα και φυσική παρέμβαση. Αυτές οι καθυστερήσεις συνεπάγονται πρόσθετο κόστος και σπατάλη ενέργειας. Όταν οι διακοπές συνδυάζονται με την ανάγκη για επείγουσες επισκευές ή αλλαγές στη διαχείριση της ενέργειας, οι ελλείψεις και οι καθυστερήσεις μπορούν να οδηγήσουν σε σημαντική αύξηση των λειτουργικών δαπανών (Liu et al, 2019).

Συμπληρωματικά, οι συνέπειες των κυβερνοεπιθέσεων επηρεάζουν και την αξιοπιστία του σκάφους. Η αδυναμία εφαρμογής στρατηγικών ενεργειακής εξοικονόμησης καθιστά τα πλοία πιο ευάλωτα σε οικονομικές κρίσεις και αυξάνουν τις πιθανότητες να υπάρξουν παραβιάσεις των περιβαλλοντικών κανονισμών. Η επένδυση σε τεχνολογίες ανθεκτικότητας, όπως η τεχνητή νοημοσύνη και τα αυτόματα συστήματα ελέγχου, είναι επιτακτική για την ενίσχυση της ασφάλειας και της αποδοτικότητας των ενεργειακών διαδικασιών σε περιπτώσεις κυβερνοεπιθέσεων (Tam et al, 2016).

Αυτή η ανάλυση τονίζει την ανάγκη για συνδυασμένες στρατηγικές που περιλαμβάνουν την ασφάλεια, την τεχνολογία και τη συνεχιζόμενη εκπαίδευση του πληρώματος, ώστε να διασφαλιστεί η βιωσιμότητα και η αποτελεσματικότητα της ενεργειακής διαχείρισης στη ναυτιλία.

7.4.3 Σενάρια ανασυγκρότησης ενεργειακών συστημάτων μετά από κυβερνοεπίθεση

Η ανασυγκρότηση ενεργειακών συστημάτων μετά από μια κυβερνοεπίθεση είναι κρίσιμη για τη διασφάλιση της λειτουργικής συνέχειας και της ασφάλειας των πλοίων. Μετά την εκδήλωση μιας κυβερνοεπίθεσης, οι διαδικασίες αποκατάστασης πρέπει να είναι άμεσες και καλά σχεδιασμένες. Ένα από τα βασικά σενάρια περιλαμβάνει την εκτίμηση της έκτασης της ζημίας και την αναγνώριση των επηρεαζόμενων συστημάτων. Αυτό απαιτεί τη συνεργασία ειδικών σε θέματα

κυβερνοασφάλειας και τεχνικών ομάδων για τη διεξαγωγή μιας λεπτομερούς ανάλυσης των εσωτερικών και εξωτερικών συστημάτων που έχουν υποστεί βλάβη (DNV, 2023).

Στη συνέχεια, η επαναφορά της λειτουργικότητας μπορεί να γίνει μέσω της επανεγκατάστασης ή της αποκατάστασης των λογισμικών που έχουν πληγεί, καθώς και της εφαρμογής ενημερώσεων ασφαλείας που είναι απαραίτητες για την αποφυγή μελλοντικών επιθέσεων. Ταυτόχρονα, έχει ιδιαίτερη σημασία να πραγματοποιηθούν ανασχεδιασμοί στις υποδομές, ενσωματώνοντας προηγμένες τεχνολογίες που προσφέρουν καλύτερη ανθεκτικότητα στις κυβερνοεπιθέσεις (DNV, 2023).

Επιπλέον, η εκπαίδευση του πληρώματος είναι καίριας σημασίας. Η επιμόρφωση του προσωπικού στις διαδικασίες έκτακτης ανάγκης και στην αναγνώριση επιθέσεων μπορεί να μειώσει το αντίκτυπο της επόμενης κυβερνοεπίθεσης και να ενισχύσει τη συνολική ανθεκτικότητα του σκάφους. Σε κάθε βήμα της ανασυγκρότησης, οι επικοινωνίες πρέπει να διατηρούνται ανοιχτές και διαφανείς, προκειμένου να εξασφαλιστεί ότι όλα τα μέλη της ομάδας είναι ενημερωμένα για τις τρέχουσες διαδικασίες και τα πρωτόκολλα (IBM, 2022).

Τέλος, η καταγραφή και ανάλυση των δεδομένων κατά τη διάρκεια και μετά από την επίθεση είναι ιδιαίτερης σημασίας για τη διαμόρφωση στρατηγικών αποκατάστασης που θα μπορούσαν να εφαρμοστούν σε μελλοντικές περιπτώσεις. Η συλλογή πληροφοριών από προηγούμενες επιθέσεις θα συμβάλει στη δημιουργία προγνωστικών μοντέλων, τα οποία θα ενισχύσουν τη συνολική ικανότητα αντίστασης και την αποτελεσματικότητα των ενεργειακών συστημάτων σε περιπτώσεις έκτακτης ανάγκης (IBM, 2022).

7.4.4 Συνδυασμός φυσικής και κυβερνοασφάλειας για ενίσχυση ενεργειακής απόδοσης

Ο συνδυασμός φυσικής ασφάλειας και κυβερνοασφάλειας αποτελεί κρίσιμη στρατηγική για την ενίσχυση της ενεργειακής απόδοσης των πλοίων και των ενεργειακών συστημάτων τους. Η φυσική ασφάλεια περιλαμβάνει τις διαδικασίες και τις τεχνολογίες που προστατεύουν τις υποδομές και τους πόρους από φυσικές απειλές, όπως οι φυσικές καταστροφές και τα ατυχήματα. Αντίστοιχα, η κυβερνοασφάλεια εστιάζει στην προστασία των ψηφιακών συστημάτων και των

δεδομένων από επιθέσεις που θα μπορούσαν να διαταράξουν τη λειτουργία των πλοίων (Ben Farah et al, 2022).

Η αποτελεσματική συνεργασία αυτών των δύο διαστάσεων μπορεί να βελτιώσει σημαντικά την ενεργειακή απόδοση. Για παράδειγμα, η εφαρμογή συστημάτων φυσικής ασφάλειας μπορεί να προστατεύσει τους σταθμούς ενέργειας και τους αισθητήρες που παρακολουθούν την κατανάλωση ενέργειας από φυσικές ζημιές, ενώ η κυβερνοασφάλεια διασφαλίζει ότι οι πληροφορίες που σχετίζονται με την ενεργειακή κατανάλωση είναι αξιόπιστες και διαθέσιμες. Επιπλέον, η συνδυασμένη προσέγγιση βοηθά στην αποφυγή απωλειών ενέργειας που μπορεί να προκύψουν λόγω κακόβουλων επιθέσεων, φυσικών καταστροφών (Ben Farah et al, 2022) ή και συνδυασμών αυτών.

Επίσης, οι προγραμματισμένες στρατηγικές αναβάθμισης των συστημάτων ασφαλείας πρέπει να περιλαμβάνουν προληπτικά μέτρα για την ανίχνευση και την αντοχή σε κυβερνοεπιθέσεις, ενισχύοντας έτσι τη συνολική ανθεκτικότητα των ενεργειακών συστημάτων. Η ενσωμάτωση τεχνολογιών IoT (Internet of Things) και τεχνητής νοημοσύνης μπορεί να βελτιώσει την παρακολούθηση και τον έλεγχο των συστημάτων ενέργειας, επιτρέποντας στους διαχειριστές να εντοπίζουν ανωμαλίες και να αντιδρούν άμεσα σε πιθανές απειλές (Tam et al, 2016).

Συνολικά, ο συνδυασμός φυσικής και κυβερνοασφάλειας όχι μόνο προστατεύει τα ενεργειακά συστήματα αλλά και προάγει την ενεργειακή αποδοτικότητα, μειώνοντας ταυτόχρονα το κόστος και τον κίνδυνο ζημιών σε περιπτώσεις έκτακτης ανάγκης.

7.4.5 Βέλτιστες πρακτικές για ολοκληρωμένα συστήματα ενεργειακής διαχείρισης και ασφάλειας

Η ολοκληρωμένη διαχείριση ενέργειας σε συνδυασμό με την ασφάλεια των συστημάτων είναι θεμελιώδης για την αποδοτικότητα και την ασφάλεια των ενεργειακών υποδομών. Οι βέλτιστες πρακτικές περιλαμβάνουν τις κατάλληλες μελέτες ασφάλειας, την ενσωμάτωση προηγμένων τεχνολογιών, την προληπτική αναγνώριση κινδύνων και τη συνεχή εκπαίδευση του προσωπικού. Πρώτον, η εφαρμογή έξυπνων συστημάτων παρακολούθησης ενέργειας επιτρέπει τη συλλογή δεδομένων σε πραγματικό χρόνο, προσφέροντας τη δυνατότητα ανάλυσης της ενεργειακής

κατανάλωσης και ανίχνευσης ανωμαλιών που ενδέχεται να υποδηλώνουν κυβερνοεπιθέσεις (NIST, 2023).

Δεύτερον, η ανάπτυξη στρατηγικών κυβερνοασφάλειας είναι απαραίτητη. Αυτές οι στρατηγικές περιλαμβάνουν την εφαρμογή πολυεπίπεδης ασφάλειας, όπου οι ευπάθειες των συστημάτων αναγνωρίζονται και αποκαθίστανται προτού καταστεί δυνατό για τους επιτιθέμενους να τις εκμεταλλευτούν. Είναι σημαντικό να πραγματοποιούνται τακτικοί έλεγχοι και ανανεώσεις στις μελέτες, τις πολιτικές και τους μηχανισμούς ασφαλείας για να διασφαλιστεί ότι το πλαίσιο παραμένει επίκαιρο και οι τεχνολογίες παραμένουν ενημερωμένες και αποτελεσματικές (ISO, 2022).

Επιπλέον, η δημιουργία κουλτούρας ασφάλειας στον οργανισμό ενθαρρύνει τους εργαζομένους να συμμετέχουν ενεργά στη διαδικασία διαχείρισης κινδύνων και μπορεί να μειώσει σημαντικά τις πιθανότητες επιτυχίας μιας κυβερνοεπίθεσης. Εκπαιδευτικά προγράμματα και ασκήσεις προσομοίωσης βοηθούν το προσωπικό να κατανοήσει καλύτερα τους κινδύνους και να μάθει πώς να αντιδρά σε περίπτωση επιθέσεων (NIST, 2023).

Τέλος, η συνεργασία με ειδικούς στον τομέα της κυβερνοασφάλειας και της ενεργειακής διαχείρισης, καθώς και η συμμετοχή σε δίκτυα που μοιράζονται πληροφορίες σχετικά με απειλές και επιθέσεις, είναι κρίσιμη για την ενίσχυση της ασφάλειας και της απόδοσης των ενεργειακών συστημάτων. Με την υιοθέτηση αυτών των βέλτιστων πρακτικών, οι οργανισμοί μπορούν να διασφαλίσουν τη βιωσιμότητα και την ανθεκτικότητα των ενεργειακών υποδομών τους.

7.5 Οικονομική αποτίμηση της ενεργειακής αποδοτικότητας κατά τη διάρκεια κυβερνοεπιθέσεων

Στις ακόλουθες παραγράφους μελετάται η οικονομική αποτίμηση της ενεργειακής αποδοτικότητας κατά τη διάρκεια κυβερνοεπιθέσεων.

7.5.1 Κόστος και οφέλη της άμεσης ενεργειακής απόκρισης σε κυβερνοεπιθέσεις

Η άμεση απόκριση σε κυβερνοεπιθέσεις είναι κρίσιμη για την προστασία των ενεργειακών υποδομών, αλλά συνοδεύεται από σημαντικά κόστη και οφέλη. Αρχικά, το κόστος για την

επίτευξη της άμεσης απόκρισης περιλαμβάνει τις επενδύσεις σε προηγμένες τεχνολογίες ασφαλείας και τη συνεχιζόμενη εκπαίδευση του προσωπικού. Η ανάγκη για εξειδικευμένο προσωπικό και η εγκατάσταση συστημάτων παρακολούθησης και ελέγχου απαιτούν χρηματοδότηση, η οποία μπορεί να είναι δυσβάσταχτη, ειδικά για μικρότερες επιχειρήσεις (Tam et al, 2016).

Ωστόσο, τα οφέλη της άμεσης ενεργειακής απόκρισης είναι πολλά και εκτιμάται ότι υπερβαίνουν τα κόστη. Κατ' αρχάς, η ταχεία αντίδραση σε κυβερνοεπιθέσεις μπορεί να περιορίσει τις επιπτώσεις τους, μειώνοντας τον κίνδυνο μεγάλων οικονομικών ζημιών ή ακόμα και την πλήρη αναστολή λειτουργίας της επιχείρησης. Μελέτες έχουν καταδείξει ότι οι επιχειρήσεις που επενδύουν στην άμεση απόκριση και σε στρατηγικές κυβερνοασφάλειας μειώνουν το μέσο κόστος των επιθέσεων, καθώς μπορούν να αποτρέψουν την εξάπλωση των ζημιών και την απώλεια δεδομένων (IBM, 2022).

Επιπλέον, η ενίσχυση της ασφάλειας μπορεί να βελτιώσει την εμπιστοσύνη των πελατών και των συνεργατών, παράμετρος που είναι κρίσιμη για τη βιωσιμότητα και την ανάπτυξη της επιχείρησης. Οι εταιρείες που επιδεικνύουν ισχυρές πρακτικές ασφάλειας συχνά προσελκύουν περισσότερους πελάτες, καθώς οι καταναλωτές γίνονται ολοένα και πιο ευαισθητοποιημένοι σχετικά με την ασφάλεια των δεδομένων και την προστασία τους (Ben Farah et al, 2022).

Εν κατακλείδι, η άμεση απόκριση σε κυβερνοεπιθέσεις απαιτεί αρχικά σημαντική επένδυση, αλλά τα οφέλη από την αποτελεσματική προστασία και την αύξηση της εμπιστοσύνης μπορούν να αποδειχθούν εξαιρετικά πολύτιμα για τις επιχειρήσεις.

7.5.2 Μακροπρόθεσμες οικονομικές επιπτώσεις των ενεργειακών απωλειών λόγω κυβερνοεπιθέσεων

Οι μακροπρόθεσμες οικονομικές επιπτώσεις των ενεργειακών απωλειών λόγω κυβερνοεπιθέσεων είναι σοβαρές και εκτεταμένες, επηρεάζοντας όχι μόνο τις άμεσες χρηματοοικονομικές πτυχές αλλά και τη συνολική βιωσιμότητα των επιχειρήσεων. Οι κυβερνοεπιθέσεις συχνά οδηγούν σε διακοπή λειτουργίας των συστημάτων, προκαλώντας σημαντικές ζημιές και κόστη αποκατάστασης. Οι ενεργειακές απώλειες μπορεί να είναι ιδιαίτερα δαπανηρές, καθώς απαιτούν

επενδύσεις για την αποκατάσταση των συστημάτων και την επανεκπαίδευση του προσωπικού (Deloitte, 2022).

Επιπρόσθετα, οι συνέπειες της απώλειας ενέργειας δεν περιορίζονται μόνο στα άμεσα κόστη αποκατάστασης. Οι επενδυτές και οι μέτοχοι είναι πιθανό να απωλέσουν την εμπιστοσύνη τους σε εταιρείες που πλήττονται από κυβερνοεπιθέσεις, με αποτέλεσμα την πτώση της τιμής των μετοχών και συνακόλουθα τη μείωση της αξίας της επιχείρησης στο χρηματιστήριο. Οι μακροπρόθεσμες οικονομικές συνέπειες μπορούν επίσης να περιλαμβάνουν την αύξηση του κόστους ασφάλισης και την ανάγκη για περισσότερους πόρους στον τομέα της κυβερνοασφάλειας (Ben Farah et al, 2022).

Οι κυβερνοεπιθέσεις επηρεάζουν επίσης την ανταγωνιστικότητα των επιχειρήσεων. Οι εταιρείες που δεν διαχειρίζονται αποτελεσματικά τις κυβερνοαπειλές ενδέχεται να χάνουν πελάτες και αγορές, μειώνοντας τα έσοδά τους και επηρεάζοντας αρνητικά την ανάπτυξή τους (Ben Farah et al, 2022). Αυτό μπορεί να έχει μακροχρόνιες συνέπειες στην καινοτομία και την επένδυση, περιορίζοντας τη δυνατότητα των εταιρειών να επενδύσουν σε νέες τεχνολογίες και υποδομές που θα μπορούσαν να βελτιώσουν την ενεργειακή αποδοτικότητα και ασφάλεια.

7.5.3 Επιπτώσεις της απώλειας ενεργειακής αποδοτικότητας στη ναυτιλιακή αγορά

Η απώλεια ενεργειακής αποδοτικότητας στη ναυτιλιακή αγορά έχει σημαντικές επιπτώσεις, επηρεάζοντας την οικονομική βιωσιμότητα των πλοίων, την ανταγωνιστικότητα των εταιρειών και το περιβάλλον. Όταν ένα πλοίο λειτουργεί με χαμηλή ενεργειακή αποδοτικότητα, οι δαπάνες για καύσιμα αυξάνονται, οδηγώντας σε μεγαλύτερα λειτουργικά κόστη. Αυτό είναι ιδιαίτερα επιζήμιο σε περιόδους υψηλών τιμών καυσίμων, καθώς οι ναυτιλιακές εταιρείες πρέπει να προσαρμόσουν τις τιμές τους, γεγονός που μπορεί να τις καθιστά λιγότερο ανταγωνιστικές στην αγορά (Alzate et al, 2024).

Η αυξημένη κατανάλωση καυσίμου δεν επηρεάζει μόνο την οικονομία των εταιρειών, αλλά έχει και σοβαρές περιβαλλοντικές συνέπειες. Η μεγαλύτερη κατανάλωση καυσίμου συνδέεται με αυξημένες εκπομπές CO_2 και άλλων ρύπων, κάτι που έρχεται σε αντίθεση με τους παγκόσμιους στόχους για μείωση των εκπομπών και την καταπολέμηση της κλιματικής αλλαγής (Alzate et al,

2024). Αυτό μπορεί να οδηγήσει σε αυστηρότερες κανονιστικές ρυθμίσεις και ποινές για τις εταιρείες που δεν συμμορφώνονται με τις απαιτήσεις για τη μείωση των εκπομπών.

Επιπλέον, οι πλοιοκτήτες και οι διαχειριστές που δεν επενδύουν στην τεχνολογία ενεργειακής αποδοτικότητας μπορεί να χάσουν τις ευκαιρίες τους στην αγορά, καθώς οι πελάτες και οι συνεργάτες τους αναζητούν εταιρείες που προωθούν την αειφορία και τη μείωση του ανθρακικού αποτυπώματος (Potamos et al, 2024). Η απώλεια ενεργειακής αποδοτικότητας μπορεί να μειώσει την αξιοπιστία της εταιρείας, πλήττοντας τις στρατηγικές ανάπτυξης και επένδυσης.

7.6 Κυβερνοασφάλεια και ενεργειακή αποδοτικότητα: Μια ολοκληρωμένη προσέγγιση

7.6.1 Συνεργασία κυβερνοασφάλειας και ενεργειακής διαχείρισης

Η συνεργασία μεταξύ κυβερνοασφάλειας και ενεργειακής διαχείρισης είναι κρίσιμη στη σύγχρονη εποχή, καθώς οι κυβερνοεπιθέσεις γίνονται όλο και πιο εξελιγμένες και συχνές. Στο πλαίσιο της ναυτιλίας, η συνδυασμένη προσέγγιση αυτών των δύο τομέων μπορεί να οδηγήσει σε καλύτερη προστασία των ενεργειακών συστημάτων από επιθέσεις που στοχεύουν στην αποσταθεροποίηση των λειτουργιών των πλοίων. Η αποτελεσματική ενεργειακή διαχείριση περιλαμβάνει τη συνεχή παρακολούθηση και βελτιστοποίηση της κατανάλωσης ενέργειας, ενώ η κυβερνοασφάλεια διασφαλίζει ότι τα συστήματα παρακολούθησης και ελέγχου παραμένουν ασφαλή από εξωτερικές επιθέσεις (Erbas et al, 2024).

Η συνεργασία αυτή απαιτεί τη δημιουργία ολοκληρωμένων στρατηγικών που συνδυάζουν την ανάλυση κινδύνων από κυβερνοεπιθέσεις με την αξιολόγηση των επιπτώσεών τους στην ενεργειακή αποδοτικότητα. Η εφαρμογή τεχνολογιών όπως η τεχνητή νοημοσύνη και το blockchain μπορεί να ενισχύσει την ικανότητα των εταιρειών να αναγνωρίζουν και να αντιμετωπίζουν απειλές σε πραγματικό χρόνο, διασφαλίζοντας παράλληλα την ομαλή λειτουργία των ενεργειακών συστημάτων (Erbas et al, 2024).

Η συνεργασία κυβερνοασφάλειας και ενεργειακής διαχείρισης μπορεί επίσης να οδηγήσει σε σημαντική εξοικονόμηση χρημάτων. Με τη μείωση των ενεργειακών απωλειών που προκύπτουν από κυβερνοεπιθέσεις, οι εταιρείες μπορούν να μειώσουν τα λειτουργικά τους κόστη και να

βελτιώσουν την ανταγωνιστικότητα τους στην αγορά. Επιπλέον, η εφαρμογή καινοτόμων λύσεων για την ενεργειακή διαχείριση μπορεί να ενισχύσει την αξιοπιστία και την καλή φήμη των εταιρειών στον τομέα της ναυτιλίας, προσφέροντας τους πλεονεκτήματα έναντι των ανταγωνιστών τους.

7.6.2 Προσαρμογή πολιτικών ασφάλειας για αύξηση της ενεργειακής αποδοτικότητας

Η προσαρμογή των πολιτικών ασφάλειας είναι κρίσιμη για την αύξηση της ενεργειακής αποδοτικότητας, ιδίως στον τομέα της ναυτιλίας. Οι σύγχρονες προκλήσεις που προέρχονται από κυβερνοεπιθέσεις απαιτούν μια στρατηγική που ενσωματώνει την κυβερνοασφάλεια με τις πολιτικές ενεργειακής διαχείρισης. Αυτή η προσέγγιση όχι μόνο διασφαλίζει την ακεραιότητα των ενεργειακών συστημάτων αλλά και βελτιώνει τη συνολική απόδοση των πλοίων.

Η ενσωμάτωση ισχυρών πολιτικών ασφάλειας ενισχύει την αξιοπιστία των ενεργειακών διαδικασιών, καθώς οι ευπάθειες στα συστήματα ελέγχου ενέργειας μπορούν να οδηγήσουν σε σημαντικές απώλειες. Για παράδειγμα, η εφαρμογή πρωτοκόλλων κρυπτογράφησης και ελέγχου πρόσβασης μπορεί να μειώσει την πιθανότητα επιθέσεων και να προστατεύσει τα κρίσιμα δεδομένα της ενεργειακής διαχείρισης (Jaramillo Jimenez et al, 2022).

Η συνεργασία μεταξύ των τομέων κυβερνοασφάλειας και ενεργειακής διαχείρισης μπορεί επίσης να οδηγήσει σε τη βελτίωση της ενεργειακής αποδοτικότητας μέσω της ανάπτυξης στρατηγικών ανάλυσης δεδομένων. Η αξιοποίηση τεχνητής νοημοσύνης για την παρακολούθηση της ενεργειακής κατανάλωσης σε πραγματικό χρόνο μπορεί να εντοπίσει ανωμαλίες που μπορεί να υποδεικνύουν κακόβουλες επιθέσεις. Επιπλέον, οι πολιτικές που προωθούν την εκπαίδευση του προσωπικού σχετικά με τους κινδύνους κυβερνοασφάλειας συμβάλλουν στη δημιουργία μιας κουλτούρας ασφαλούς πρακτικής και ενεργειακής ευαισθητοποίησης (Afenyo & Caesar, 2023).

Η προσαρμογή των πολιτικών ασφάλειας δεν είναι απλώς μια αντίδραση στις κυβερνοαπειλές, αλλά και μια στρατηγική επένδυση για τη βιώσιμη ανάπτυξη της ναυτιλίας. Με την εφαρμογή αυτών των βελτιωμένων πολιτικών, οι ναυτιλιακές εταιρείες μπορούν να εξασφαλίσουν όχι μόνο την ασφάλεια των συστημάτων τους αλλά και τη μακροχρόνια ενεργειακή τους αποδοτικότητα.

7.6.3 Ενεργειακά αποδοτική άμυνα έναντι κυβερνοεπιθέσεων: Σύγχρονες τάσεις

Η ενεργειακή αποδοτικότητα αποτελεί έναν κρίσιμο παράγοντα στην άμυνα κατά των κυβερνοεπιθέσεων, καθώς οι σύγχρονες τάσεις απαιτούν την ανάπτυξη ολοκληρωμένων στρατηγικών που συνδυάζουν την ασφάλεια και την ενεργειακή διαχείριση. Οι κυβερνοεπιθέσεις έχουν αυξηθεί σε συχνότητα και πολυπλοκότητα, γεγονός που καθιστά απαραίτητο τον κατάλληλο σχεδιασμό των συστημάτων για την ελαχιστοποίηση των επιπτώσεών τους. Οι οργανισμοί πλέον στρέφονται προς έξυπνα συστήματα παρακολούθησης και ανάλυσης δεδομένων, τα οποία χρησιμοποιούν τεχνητή νοημοσύνη για τη βελτιστοποίηση της κατανάλωσης ενέργειας και την ανίχνευση ανωμαλιών που μπορεί να υποδεικνύουν κυβερνοαπειλές (Loganathan et al, 2018).

Μια τάση που αναδεικνύεται είναι η ολοκλήρωση των συστημάτων κυβερνοασφάλειας με τα ενεργειακά συστήματα, επιτρέποντας τη λήψη αποφάσεων σε πραγματικό χρόνο που μειώνουν την ενεργειακή κατανάλωση κατά την εφαρμογή αμυντικών στρατηγικών. Οι ευέλικτες αρχιτεκτονικές των δικτύων επιτρέπουν την ταχεία αναδιάρθρωση των πόρων, ώστε να διατηρηθεί η ενεργειακή αποδοτικότητα, ακόμη και σε συνθήκες έκτακτης ανάγκης (Loganathan et al, 2018).

Η εκπαίδευση του προσωπικού και η καλλιέργεια κουλτούρας κυβερνοασφάλειας είναι επίσης κρίσιμες. Οι οργανισμοί που επενδύουν στη συνεχή εκπαίδευση του προσωπικού τους σχετικά με τις τελευταίες απειλές και τις στρατηγικές άμυνας έχουν καλύτερες πιθανότητες να διατηρήσουν την ενεργειακή τους αποδοτικότητα κατά τη διάρκεια κυβερνοεπιθέσεων (Shixing et al, 2023).

8 Συμπεράσματα

Ο σχεδιασμός και η εφαρμογή μίας ολιστικής πολιτικής ασφάλειας αποτελεί τη βάση της ασφάλειας ενός συστήματος. Πάνω στη βάση αυτή θα στηριχθούν τα υπόλοιπα στοιχεία της υλοποίησης, συμπεριλαμβάνοντας τα τεχνικά μέσα και οι διαδικαστικές προβλέψεις. Ειδικότερα, οι ενέργειες της ανάλυσης επικινδυνότητας/ρίσκου, της αποτίμησης κινδύνων, της επιλογής τεχνικών μέσων και του ορισμού συγκεκριμένων διαδικασιών που άπτονται της ασφάλειας, καθοδηγούνται αποτελεσματικά από τις προβλέψεις της πολιτικής ασφάλειας. Συνολικά, η πολιτική ασφάλειας περιλαμβάνει προβλέψεις για ενδεχόμενες περιστάσεις που απειλούν την ασφάλεια των συστημάτων καθώς και κατευθύνσεις για τα μέτρα που θα πρέπει να υιοθετηθούν για την αντιμετώπιση τους. Τονίζεται ιδιαίτερα ότι αν και η εφαρμογή τεχνικών μέτρων ή μηχανισμών μπορούν αφ' εαυτών να φέρουν ορισμένα αποτελέσματα, αυτά θα είναι αποσπασματικά και δεν θα παρέχουν επαρκείς εγγυήσεις για την ασφάλεια του συστήματος. Για να παρέχονται αυξημένα εχέγγυα, θα πρέπει να υιοθετηθεί κάποιο μοντέλο ασφάλειας που θα εκφράζεται μέσω συγκεκριμένης πολιτικής. Από την άλλη πλευρά, είναι σαφές ότι μία πολιτική είναι αδύνατον να προβλέπει το σύνολο των δυνατών ενδεχομένων για επιθέσεις ή περιστατικά ασφαλείας. Με αυτό το δεδομένο, ο ανθρώπινος παράγων, η εκπαίδευση, η εμπειρία και η διαίσθηση εξακολουθούν να διαδραματίζουν σημαντικό ρόλο.

Ειδικότερα για το θέμα των πλοίων, η παρούσα εργασία τονίζει την σημασία της κυβερνοασφάλειας, λαμβάνοντας υπ' όψιν τις ιδιαίτερες απαιτήσεις και συνθήκες, και διερευνά σχεδιαστικές αρχές και μέτρα που θα πρέπει να εξετάζονται στη διαμόρφωση της πολιτικής αλλά και στην υλοποίησή της.

Πηγές – Βιβλιογραφία

Afenyo, M. & Caesar, L. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management. 10.1016/j.ocecoaman.2023.106493.

Al-Mamary, Y. H., Shamsuddin, A. & Aziati, N. (2014, August). *"The Role of Different Types of Information Systems In Business Organizations : A Review"*. International Journal of Research.

Alzate, P., Isaza, G.A., Toro, E.M. Jaramillo-Garzón, J.A., Hernandez, S., Jurado, I. & Hernandez, D. (2024). Operational efficiency and sustainability in smart ports: a comprehensive review. Mar Syst Ocean Technol (2024). https://doi.org/10.1007/s40868-024-00142-z

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X. (2022). *Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends*. Information. 2022; 13(1):22. https://doi.org/10.3390/info13010022

Bidgoli, H. (2006). *'Handbook of Information Security'*. John Wiley & Sons.

Bourgeois, D. T. (2014, February). *"Information Systems for Business and Beyond."* pp 14, 30, 85. Through the Open Text Book Challenge by the Saylor Academy.

Boyce, J. (2002). 'Information Assurance: Managing Organizational It Security Risks'. Butterworth-Heinemann.

Clouds net, (n.d.). ecdis-info.com. Retrieved from http://www.ecdis-info.com/about_ecdis.html

Deloitte. (2022). *Five in 5: Cybersecurity in the energy sector. Energy cybersecurity risks and mitigation strategies.*

Dimakopoulou, A., Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. Journal of Marine Science and Engineering. 2024; 12(6):919. https://doi.org/10.3390/jmse12060919

DNV. (2023). *Cyber priority 2023*. DNV. Retrieved from https://www.dnv.com

Erbas, M. & Khalil, S. & Tsiopoulos, L. (2024). *Systematic literature review of threat modeling and risk assessment in ship cybersecurity*. Ocean Engineering. 306. 118059. 10.1016/j.oceaneng.2024.118059.

Grcsolutions.io (2022). 'Specialist services and solutions for IT governance, risk management, compliance and information security'. (2012). Retrieved from: http://www.itgovernance.co.uk/

Harwood, S. (2015, September). "Cyber Risk". Joint Hull

Hebergementwebs. (2023). Use OSINT for maritime intelligence. Ανακτήθηκε 28 Μαρτίου 2026, από https://www.hebergementwebs.com/news/use-osint-for-maritime-intelligence

Heidarkhani, A., khomami, A.A, Jahanbazi, Q., & Alipoor, H. (2013). *"The Role of Management Information Systems (MIS) in Decision-Making and Problems of its Implementation"*. Universal Journal of Management and Social Sciences. Vol. 3.

Hicks (1993) quoted by Checkland and Holwell [1998] in Boland. (1985). Data , Infromation and Meaning: "Information Systems are data becoming information in consciousness; organizations are socially constructed through language, and our reasoning about both these processes takes place in dialogue." Chapter 3. Retrieved from: https://repository.up.ac.za/dspace/bitstream/handle/2263/27367/03chapter3.pdf

Homeland Security (2016, March) "Consequences to Seaport Operations from Malicious Cyber Activity", National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA), Critical Infrastructure Security and Resilience Note https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf

IBM. (2022). *Cost of a Data Breach Report.*

Identity Finder, LLC. (2009). Data at rest vs. data in motion. https://docs.media.bitpipe.com/io_12x/io_125438/item_1205707/Data-at-Rest%20v%20Data-in-Motion.pdf

IMSO.org (2024). International Mobile Satelite Organization, https://imso.org/

Information Security Policies and Standards. (2012). Retrieved from: http://www.information-security-policies-and-standards.com/

Inventory of Risk Management /Risk Assessment methods and tools. (2012). Retrieved from: http://rm-inv.enisa.europa.eu

iRami (2012). *The Economic Role of The Shipping Industry*. iRami. Retrieved from : https://ramiwaheed.wordpress.com/2012/09/15/the-economic-role-of-the-shipping-industry/

ISO. (2022). *ISO/IEC 27001:2022 - Information security management systems.*

ISO/IEC. (2000). *17799 Code of Practice for Information Security Management*. Geneva, Switzerland. INTERNATIONAL STANDARD .

ISO/IEC/JTC1. (1996). TR 13335 Information Technology - Security Techniques - Guidelines for the management of IT Security (GMITS). Geneva, Switzerland.

Jaramillo Jimenez, V. & Kim, H. & Munim, Z. (2022). *A review of ship energy efficiency research and directions towards emission reduction in the maritime industry*. Journal of Cleaner Production. 366. 132888. 10.1016/j.jclepro.2022.132888.

Laudon, K.C. & Jane, P. (2012). “Laudon, Management Information Systems – Managing the digital firm”. Pearson Education. pp 423.

Li, J., Guo, C., Si, W., & Huang, X. (2019). The Approaches of Prevention, Detection, and Response for Cybersecurity of I&C Systems in NPPs. In Lecture Notes in Electrical Engineering (pp. 283–290). Springer Singapore. https://doi.org/10.1007/978-981-13-3113-8_33

Liu, X., Huang, H., Xiao, F. & Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. IEEE Internet Things J. 7, 4101–4112 (2019).

Loganathan, N., Mayurappriyan, P. & Lakshmi, Kvn. (2018). *Smart energy management systems: a literature review.* MATEC Web of Conferences. 225. 01016. 10.1051/matecconf/201822501016.

NIST. (2023). *Cybersecurity Framework.* National Institute of Standards and Technology.

Pangalos, G. (1992). *'Security in Medical Database Systems'*. EEC, SEISMED Project Report.

Pfleeger, (1997). *'Security in Computing'*. Prentice-Hall Inc.

Pfleeger, C., Pfleeger, S. L., & Coles-Kemp, L. (2023). *Security in computing* (6th edn). Boston, MA: Addison Wesley.

Potamos, G., Stavrou, E., Stavrou, S. (2024). *Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis.* Sensors. 2024; 24(11):3458. https://doi.org/10.3390/s24113458

Poulsen, R. T., Viktorelius, M., Varvne, H., Rasmussen, H B., von Knorring, H. (2022) Energy efficiency in ship operations: Exploring voyage decisions and decision-makers Transportation Research Part D: Transport and Environment. 102: 103120 https://doi.org/10.1016/j.trd.2021.103120

Powell, S. & Shim, J.P. (2009). "Wireless Technology Application, Management and Security". Springer.

Qyusi Consulting. (2017, May 15). Risiko dan peluang ISO 9001. https://www.qyusiconsulting.com/risiko-dan-peluang-iso-9001/

Rash, M., Orebaugh, A. D., Clark, G., Pinkard, B. & Babbin, J. (2005). *Intrusion Prevention and Active Response: Deployment Network and Host IPS*. Syngress.

Risk World. (2012). Retrieved from: http://www.riskworld.net/

Safety4Sea. (2018, October 5). UNCTAD: Seaborne trade volume reached 10.7 billion tons in 2017. https://safety4sea.com/unctad-seaborne-trade-volume-reached-10-7-billion-tons-in-2017/

Scasfone, K. & Mell, P. (2007). *"Guide to Intrusion Detection and Prevention Systems (IDPS)"*. National Institute of Standards and Technology.

Season Ship Management & Maritime Services. (n.d.). Gallery. Ανακτήθηκε 28 Μαρτίου 2026, από https://www.seasonship.co.in/gallery.php

Shine micro (2021). Receive Better. https://www.shinemicro.com/ais-overview/

Ship Technology, 2021. https://www.ship-technology.com/projects/triple-e-class-container-ship/

Shixing, D., Yijun, X., Mert, K. & Yang, C. (2023). *Review of cybersecurity for integrated energy systems with integration of cyber-physical systems*. Energy Conversion and Economics. 4. n/a-n/a. 10.1049/enc2.12097.

Siponen, M., (2000). 'Policies for Construction of Information Systems Security Guidelines'. Kluwer Academic Publishers.

Stair, R. & Reynolds, G. (2010). *"Principles of Information Systems – A Managerial Approach."* 9th, . Course Technology, 28 ch10, p3

Stair, R., & Reynolds, G. (2010). *"Principles of Information Systems – A Managerial Approach."* 9th, , Course Technology. pp460, ch11, p3

Stallings, W. (2003). "Network Security Essentials: Applications and Standards". 2nd edition, Prentice Hall.

Tam, K., Jones, K. & Papadaki, M. (2016). *Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference*. 1. 10.1049/etr.2015.0123.

Tanenbaum, A. S. (2003). *'Computer Networks'*, 4th Edition, Pearson Education Inc.

Thales Group. (n.d.). Cybersecurity. Ανακτήθηκε 28 Μαρτίου 2026, από https://www.thalesgroup.com/en/cybersecurity

Times Newsroom, (2024, February). Αστεροσκοπείο του Γκρίνουιτς: λειτουργεί από το 1998 ως μουσείο. Ιδρύθηκε το 1675 από τον βασιλιά της Αγγλίας Κάρολο Β΄, λίγα χιλιόμετρα έξω

από το κέντρο του Λονδίνου. Retrieved from: https://www.timesnews.gr/asteroskopeio-toy-gkrinoyits/

Tutorials Point. (n.d.). *Basics of Computer Networking.* Retrieved from : https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

UNCTAD (2018). *"Review of Maritime Transport 2018,"* pp. 15, 2018, United Nations, New York and Geneva, 2018.

Vantorre, M., Delefortrie, G., Eloot, K. & Laforce, Erik. (2003). *Experimental investigation of ship-bank interaction forces.* Marsim'03.

Vantorre, M., Verzhbitskaya, E. & Laforce, E. (2002). Model test based formulations of ship-ship interaction forces. Ship Technology Research. 49. 124-141.

Wikipedia, 2025. Guglielmo Marconi. https://en.wikipedia.org/wiki/Guglielmo_Marconi#Developing_radio_telegraphy

Wikipedia, 2025. Triple E-class container ship . https://en.wikipedia.org/wiki/Maersk_Triple_E-class_container_ship

Wikipidia, (n.d.). Cavity magnetron. Retrieved from: https://en.wikipedia.org/wiki/Cavity_magnetron

Wikipidia, (n.d.). ENIAC. Retrieved from: https://en.wikipedia.org/wiki/ENIAC

Wikipidia, (n.d.). *Guglielmo Marconi*. Retrieved from:

Wikipidia, (n.d.). Hyperbolic navigation. Retrieved from: https://en.wikipedia.org/wiki/Hyperbolic_navigation

Wikipidia, (n.d.). Transistor. Retrieved from: https://en.wikipedia.org/wiki/Transistor

Wikipidia, (n.d.). *Triple E-class container ship.* Retrieved from: https://en.wikipedia.org/wiki/Automatic_identification_system

Yang, C., Lu, Z., Wang, W., Li, Y., Chen, Y. & Xu, B. (2023*). Energy management of hybrid electric propulsion system: Recent progress and a flying car perspective under three-dimensional transportation networks.* Green Energy and Intelligent Transportation. Volume 2, Issue 1, 2023, 100061, ISSN 2773-1537, https://doi.org/10.1016/j.geits.2022.100061 https://www.sciencedirect.com/science/article/pii/S2773153722000615

Αλβέρτης Χρήστος, Αφορδάκος Ευάγγελος & Ράπτης Στυλιανός 'Ασφάλεια Δικτύων – Το ηλεκτρονικό Ταχυδρομείο', Πάτρα 2016.

Γεωργιάδης Αντώνιος (2018). 'Η Ασφάλεια Πληροφοριών στις Σύγχρονες Επιχειρήσεις & Μελέτη Περίπτωσης σε μια Εταιρεία' Πανεπιστήμιο Πειραιώς :Τμήμα Οργάνωσης και Διοίκησης Επιχειρήσεων. Πειραιάς 2018.

Γεωργίου, Σ. (2012). Ανάλυση και διαχείριση επικινδυνότητας στα πληροφοριακά συστήματα: Υλοποίηση μεθοδολογίας σε επιχειρησιακό περιβάλλον (Μεταπτυχιακή διπλωματική εργασία, Πανεπιστήμιο Πειραιώς). https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4745/Georgiou.pdf

Γκριτζάλης, Δ. Α. & Κάτσικας Σ. Κ. (2003). 'Ασφάλεια δικτύων υπολογιστών: τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης'. Παπασωτηρίου.

Δουφεξή Αναστασία (2018). 'Ανάπτυξη Βασεων Δεδομένων Επιχειρησιακού ενδιαφέροντος σε σύστημα MySQL', Παγανία Σπυριδούλα και Σουνδιά Γεωργία (Πάτρα 2018)

Ευελπίδου, Ν., & Αντωνίου, Β., (2015). "Γεωγραφικά συστήματα πληροφοριών." [ηλεκτρ. βιβλ.] Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/1044

Καρατζάς, Πέτρος (2013). Πολυκριτήρια αξιολόγηση μέτρων ασφαλείας σε πληροφορικά συστήματα εμπορικών λιμένων. National Technical University of Athens, http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/16760/1/DT2013-0247.pdf

Καρύδα, Μ. (2005). ‘Διοίκηση ασφάλειας πληροφοριακών συστημάτων: Οργανωσιακά Ζητήματα Ανάπτυξης, Εφαρμογής και ενσωμάτωσης Πολιτικών Ασφάλειας.’ Οικονομικό Πανεπιστήμιο Αθηνών: Τμήμα Πληροφορικής.

Κάτσικας, Σ. (2001). *"Ασφάλεια Δικτύων"*. ΕΑΠ.

Κιουντούζης, Ε., (2002). ‘Μεθοδολογίες ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων’. Β’ Εκδόσεις Μπένου.

Κλαδάκης, Ν. & Λεκάτης Γ. (2001). ‘Ασφάλεια δικτύων και συστημάτων’. Παπασωτηρίου.

Κομνηνός, Θ., Σπυράκης, Π. & Παύλος, Γ. (2002). ‘Ασφάλεια δικτύων & υπολογιστικών συστημάτων : αναχαιτίστε τους εισβολείς’. Ελληνικά Γράμματα.

Λέρα Μαρία (2012). ‘ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ’ Κοζάνη. Διπλωματική εργασία. ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ

Μάττας, Α. (2007). *‘Ασφάλεια Πληροφοριακών Συστημάτων σε συνεργατικά περιβάλλοντα εφαρμογών με βάση το διαδίκτυο’*. Θεσσαλονίκη. Διδακτορική Διατριβή. ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ – ΓΕΝΙΚΟ ΤΜΗΜΑ ΤΟΜΕΑΣ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΜΕΘΟΔΩΝ και ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ Η/Υ.

Μαυρίδης, Ι. (2015). Βασικές έννοιες και ζητήματα ασφάλειας, https://repository.kallipos.gr/handle/11419/1025

Μπεσαράτ, Τζέριες (2022). *Ασφάλεια συστημάτων (Μάθημα 2, 18.3.2022,* , Πανεπιστήμιο Ιωαννίνων*)*. Ανακτήθηκε από https://www.dit.uoi.gr/e-class/modules/document/file.php/304/Lesson2-ASFALEIA%20%2818.3.22%29.pdf

Μπιλάλης Κων/νος, Γούναρης Άγγελος και Πεπελάσης Σπυρίδων (2016) ‘Τεχνικές Ανακάλυψης Ενδιαφέρουσας Πληροφορίας σε Βάσεις Δεδομένων’, Αθήνα 2016

Μπόζιος, Ε., (2007). ‘Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστημάτων’. Θεσσαλονίκη.

Νικολακόπουλος, Κ. (2015). “Χρήση Γεωγραφικών Συστημάτων Πληροφοριών και Τηλεπισκόπησης στην Εφαρμοσμένη Γεωλογία”. 1.0. Πάτρα.

Νόμος 2472/97. (1997). Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, 10-4-97/ΦΕΚ 50/Τεύχος Α’.

Νόμος 2474/1999, (1999). Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Νόμος 3418/2005, (2005). Κώδικας Ιατρικής Δεοντολογίας.

Πάγκαλος, Γ. & Μαυρίδης Ι. (2002). *‘Ασφάλεια πληροφοριακών συστημάτων και δικτύων’*. Ανικούλα.

Παλληκάρης, Α. Η. & Κατσούλης, Γ. Θ. (1008). “Ιστορική εξέλιξη και προοπτικές της ηλεκτρονικής ναυτιλίας”.

Πανέτσος, Σ. (2007). ‘Επικοινωνίες & Δίκτυα Υπολογιστών’. Εκδόσεις Τζιόλα.

Ρόδιος Εμμανουήλ, ‘Κύριοι Άξονες Πολιτικής της Ε.Ε. για την Ασφάλεια στη Θάλασσα και η Σημασία τους για την Ανταγωνιστικότητα της Ευρωπαΐκης Ναυτιλίας. Πανεπιστ’ημιο Πειραιώς, Τμήμα Ναυτιλιακών Σπουδών, Πειραιάς 2017.

Σαλτσίδης, Χ. (2018). Έλεγχος πληροφοριακών συστημάτων: Σύγχρονα θέματα και τάσεις στην Ελλάδα (Διπλωματική εργασία, Πανεπιστήμιο Μακεδονίας). https://dspace.lib.uom.gr/bitstream/2159/21660/4/SaltsidisCharalamposMsc2018.pdf