Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Διπλωματική Εργασία

Μελέτη Αδυναμιών σε Κρίσιμες Υποδομές με έμφαση στη Ναυτιλία

Φοιτητής: **Παπαδάκης Εμμανουήλ**

ΑΜΦ: **ΜΤΕ 1729**

Email: **papadakis_manolis@ssl-unipi.gr**

Επιβλέπων: **Λαμπρινουδάκης Κωνσταντίνος, clam@unipi.gr**

Πειραιάς 2018-19

Περίληψη

Οι θαλάσσιες μεταφορές είναι κρίσιμες για την παγκόσμια οικονομία. Σε ένα ανταγωνιστικό περιβάλλον, ο κλάδος αναζητά συνεχώς οικονομίες κλίμακας και αποτελεσματικότητας. Αυτό οδήγησε στην εισαγωγή πλοίων μεγαλύτερης χωρητικότητας και την αυξανόμενη χρήση της τεχνολογίας των πληροφοριών για την επίτευξη μεγαλύτερης αυτοματοποίησης, τόσο στην ξηρά όσο και στη θάλασσα. Η αυξημένη ψηφιοποίηση μπορεί να αποδειχθεί ωφέλιμη για τη βιομηχανία όσον αφορά την παραγωγικότητα, την αποδοτικότητα και τη βελτιστοποίηση της απόδοσης, αλλά και να δημιουργήσει σοβαρές απειλές με τη σύνδεση ενός πλοίου με τον κυβερνοχώρο. Σε έναν όλο και περισσότερο συνδεδεμένο και τεχνολογικά εξαρτώμενο κόσμο, εμφανίζονται νέες ευπάθειες. Αυτό οφείλεται στον συνεχώς αυξανόμενο αριθμό τρίτων που χρησιμοποιούν κλεμμένα δεδομένα από τα διάφορα συστημάτων των ναυτιλιακών οργανισμών. Οι χρησιμοποιούμενες τεχνολογίες είναι ευάλωτες στις ίδιες απειλές που επηρεάζουν τα εμπορικά, παραγωγικά και κυβερνητικά συστήματα. Η παρούσα διπλωματική εργασία εξετάζει τις απειλές στη ναυτιλιακή βιομηχανία και διερευνά τις πιθανές επιθέσεις σε συστήματα σχετικά με την πλοήγηση, την πρόωση και διαχείριση του φορτίου στα πλοία.

Abstract

Maritime transport is critical to the global economy. In a competitive environment, the industry is constantly seeking economies of scale and efficiencies. This has led to the introduction of larger vessels and an increasing use of information technology to achieve greater automation, both on shore and at sea. The increased digitalization may prove to be beneficial to the industry in terms of productivity, efficiency and performance optimization but also, impose serious threats from the consistent connection of a ship with the cyber world. In an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. This is due to the ever growing number of illegitimate parties that stand to gain from manipulation stolen data of the industry's on-board and onshore systems. The technologies employed are vulnerable to the same cyber-security threats as those in other sectors affecting commercial, production and government systems. This thesis reviews the threats in the maritime environment and explores the possible cyber-attacks on maritime-related systems for navigation, propulsion, and cargo-related functions.

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή κύριο Λαμπρινουδάκη Κώστα για την ευκαιρία που μου έδωσε την ευκαιρία να ασχοληθώ με ένα εξαιρετικά ενδιαφέρον και σύγχρονο θέμα. Θα ήθελα επίσης να τον ευχαριστήσω για τη στήριξη και την καθοδήγηση που μου προσέφερε για την ολοκλήρωση της παρούσας διπλωματικής εργασίας.

Ακρωνύμια

ICS - Industrial Control Systems

IT – Information Technology

OT - Operational Technology

IMO – International Maritime Organization

TMSA – Tanker Management Self-Assessment

ABS – American Bureau of Shipping

DNV – Det Norsk Veritas

BIMCO – Baltic and International Maritime Council

ISPS – International Ship and Port Security

ISM - International Security Management

ICT – Information and Communication Technology

SIRE – Ship Inspection Reporting Program

SMS – Safety Management System

PDCA – Plan, Do, Check, Act

ISMS – Information Security Management System

VISHING – Voice Phishing

DMAIC – Define, Measure, Analyze, Increase, Control

IoT – Internet of Things

AIS – Automatic Identification System

GMDSS – Global Maritime Distress and Safety System

ECDIS – Electronic Chart Display and Information System

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

OCIMF – Oil Companies International Marine Forum

DoS – Denial of Service

CIA – Confidentiality, Integrity, Availability

NIST – National Institute of Standards and Technology

Πίνακας Περιεχομένων

Περιεχόμενα Εικόνων

Περιεχόμενα Πινάκων

Κεφάλαιο 1

Κεφάλαιο 1.1: Εισαγωγή

Η ασφάλεια των θαλάσσιων μεταφορών αποτελεί έναν από τους κύριους στόχους του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) τα τελευταία χρόνια. Ο Διεθνής Κώδικας Διαχείρισης Ασφάλειας (ISM) και ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ISPS) δημιουργήθηκαν για να εξασφαλίσουν την ασφάλεια στις πλωτές και λιμενικές επιχειρήσεις, καθώς και στα εμπορικά και επιβατηγά πλοία. Οι παραπάνω Κώδικες αφορούν τον εντοπισμό των κινδύνων στα πλοία, την πρόληψη ατυχημάτων και την αντιμετώπιση επικίνδυνων καταστάσεων με σημαντικές συνέπειες, όπως η απώλεια ζωής και η περιβαλλοντική καταστροφή. Σήμερα, οι ανησυχίες για την ασφάλεια δεν περιορίζονται μόνο σε φυσικές καταστροφές. Ιστορικά, όταν ένα πλοίο έφευγε από το λιμάνι, ήταν απομονωμένο και οι δυνητικοί κίνδυνοι ήταν μόνο θέμα ανθρώπινου σφάλματος ή μηχανικής αποτυχίας. Ωστόσο, με την ανάπτυξη της τεχνολογίας και των ανοιχτών επικοινωνιών με τις εγκαταστάσεις της ξηράς, τα πλοία εισήλθαν σε ένα νέο και πολλά υποσχόμενο κόσμο: Την ψηφιακή εποχή.

Η ψηφιοποίηση έχει μετασχηματίσει τη ναυτιλιακή βιομηχανία. Η διαδικασία λήψης αποφάσεων πραγματοποιείται σε πολύ μεγάλο βαθμό μέσω ψηφιακών πληροφοριών που συλλέγονται κατά τη διάρκεια ενός ταξιδιού και μεταδίδονται στα κεντρικά γραφεία των οργανισμών. Ωστόσο, αυτή η αναδυόμενη ευκαιρία για τη ναυτιλία ενέχει σοβαρούς κινδύνους. Η αυξημένη δια- λειτουργικότητα δημιουργεί νέες προκλήσεις στο ναυτιλιακό κόσμο, όπως για παράδειγμα ο κυβερνό- πόλεμος, ο οποίος αποτελείται από υψηλό επίπεδο αβεβαιότητας και από έλλειψη κατανόησης των κινδύνων. Η αυξανόμενη πολυπλοκότητα, η ψηφιοποίηση, η ολοκλήρωση και η αυτοματοποίηση των συστημάτων στην οποία βασίζεται η ναυτιλιακή βιομηχανία απαιτεί ολιστική διαχείριση του ζητήματος. Συχνότερα, διαφορετικά συστήματα συνδέονται όχι μόνο στο τοπικό δίκτυο του πλοίου αλλά και στο Διαδίκτυο, γεγονός που αυξάνει τον κίνδυνο [1]. Η ασφάλεια των ψηφιακών συστημάτων είναι πλέον υποχρεωτική όχι μόνο για την προστασία των δεδομένων αλλά και για την εξασφάλιση ασφαλών και αξιόπιστων εργασιών [2]. Στη χειρότερη περίπτωση, ένα περιστατικό που αφορά την ασφάλεια στον κυβερνοχώρο μπορεί να οδηγήσει σε: διάπραξη εγκληματικών πράξεων - όπως αρπαγή του πλοίου ή κλοπή του φορτίου, σε απώλεια ελέγχου του πλοίου ή απώλεια δεδομένων ή ακόμα και σε απώλεια ανθρώπινης ζωής [3].

Η χρήση νέων τεχνολογιών μπορεί να συμβάλει στην αποτελεσματικότητα και την ασφάλεια του πλοίου, ωστόσο αυξάνει την πιθανότητα να συμβεί περιστατικό κυβερνό- ασφάλειας. Προκειμένου να επιτευχθούν πλήρως τα οφέλη, η ασφάλεια πληροφοριών πρέπει να εξεταστεί σε όλα τα επίπεδα του οργανισμού. Οι οργανισμοί πρέπει να καθιερώσουν και να ακολουθήσουν μια σταθερή στρατηγική στον κυβερνοχώρο. Ένα μεγάλο μέρος των παραβιάσεων της ασφάλειας συστημάτων οφείλεται στους ανθρώπους και τις ελλιπείς διαδικασίες που έχουν εφαρμοσθεί από τους οργανισμούς. Επομένως, κατά τη διαδικασία αξιολόγησης του κινδύνου πρέπει να λαμβάνονται υπόψη τόσο το προσωπικό του οργανισμού όσο και οι λειτουργίες που επιτελούν τα συστήματα [2]. Εφαρμόζοντας τις βέλτιστες πρακτικές για την κυβερνό- ασφάλεια, ο οργανισμός μπορεί να ενισχύσει την ασφάλεια και να τη χρησιμοποιήσει ως ανταγωνιστικό πλεονέκτημα αυξάνοντας το μερίδιο του στην αγορά.

Κεφάλαιο 1.2: Στόχος

Οι κύριοι στόχοι της εργασίας είναι:

• Να ερευνηθεί η σημασία της ασφάλειας πληροφοριών σε ολόκληρο τον κύκλο ζωής ενός πλοίου

• Να εξετασθούν τα συστήματα ενός πλοίου και οι πιθανές επιπτώσεις των κυβερνό-επιθέσεων στα συστήματα αυτά

• Να διερευνηθούν οι διάφοροι παράγοντες απειλής, να εντοπιστούν τα κίνητρά και να αναγνωριστεί η προέλευση των επιθέσεων

• Να χαρτογραφηθούν οι πιθανοί τρόποι επίθεσης και να προσδιοριστούν τα συστήματα που δημιουργούν τρωτά σημεία στην ασφάλεια του πλοίου

• Να προσδιοριστούν οι κύριες πτυχές που συμβάλλουν στην άμβλυνση των κινδύνων και να προταθεί ένα πλαίσιο αντιμετώπισης τους

Κεφάλαιο 1.3: Ορισμός της Ασφάλειας στον Κυβερνοχώρο

Το κεφάλαιο αυτό καθώς και τα υποκεφάλαια του εξηγούν τις βασικές έννοιες της ασφάλειας στον κυβερνοχώρο. Η κατηγοριοποίηση, τα εργαλεία και τα στοιχεία που παρουσιάζονται σε αυτό το κεφάλαιο διευκολύνουν την πλήρη αντίληψη της διαχείρισης του κινδύνου, η οποία είναι κοινή για διάφορες προσεγγίσεις όπως αναλύονται σε επόμενα κεφάλαια αυτής της διατριβής. Δεν υπάρχει ενιαίος ορισμός για την ασφάλεια στον κυβερνοχώρο. Αντίθετα, μπορεί να θεωρηθεί ως η επιχείρηση που διεξάγει ένας οργανισμός για να προστατευτεί από τις επιθέσεις και τις συνέπειές τους, καθώς και τα απαραίτητα αντίμετρα που πρέπει να υιοθετήσει [3]. Σύμφωνα με τους [4], ο κίνδυνος και η ανάλυση της απειλής αποτελούν θεμέλιο λίθο της ασφάλειας στον κυβερνοχώρο. Η ενίσχυση της κυβερνό- ασφάλειας μπορεί να επιτευχθεί με τη μείωση της έκθεσης στον κίνδυνο, δίνοντας έμφαση στα συστήματα που σχετίζονται κυρίως με την ασφάλεια, όπως οι κρίσιμες υποδομές. Μια προσέγγιση βασισμένη στον κίνδυνο και στην ολιστική διαχείριση του κινδύνου είναι το κλειδί για την επίτευξη αυτού του στόχου από έναν οργανισμό. Η διαχείριση του κινδύνου μπορεί να οριστεί ως «η διαδικασία προσδιορισμού, ανάλυσης, αξιολόγησης και κοινοποίησης ενός κινδύνου που συνδέεται με την ασφάλεια πληροφοριών και την αποδοχή, αποφυγή, μεταφορά ή άμβλυνση του κινδύνου σε αποδεκτό επίπεδο, λαμβάνοντας υπόψη το κόστος και τα οφέλη των δράσεων που λαμβάνονται» [5]. Η εφαρμογή της κυβερνό- ασφάλειας ξεκινά από το επίπεδο της Διοίκησης και απαιτεί δέσμευση από όλα τα επίπεδα του οργανισμού, δεδομένου ότι ο αντίκτυπος του ανθρώπινου παράγοντα είναι από τους πιο σημαντικούς. Για τη βελτίωση της ασφάλειας απαιτείται η ανάπτυξη ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS) και συνεχείς διαδικασίες βελτίωσης του, όπως είναι η εφαρμογή του PDCA ή ο καθορισμός, η μέτρηση, η ανάλυση, η βελτίωση και έλεγχος (DMAIC) της μεθόδου έξι σίγμα, όπως προβλέπει το πρότυπο ασφάλειας πληροφοριών ISO/IEC 27001:2015

Κεφάλαιο 1.3.1: Ιδιαίτερα χαρακτηριστικά της Ναυτιλίας και απειλές

Η ανάπτυξη των διασυνδεδεμένων συστημάτων ελέγχου αποτελεί σημαντικό παράγοντα για τους οργανισμούς της ναυτιλιακής βιομηχανίας. Τα συστήματα πληροφοριών και επιχειρησιακών λειτουργιών (Operational Technology - OT) των πλοίων είναι όλο και περισσότερο δικτυωμένα όχι μόνο μεταξύ τους, αλλά και στο Διαδίκτυο. Τα διάφορα συστήματα πλοίων ή πλατφορμών όπως: τα συστήματα πρόωσης, τα συστήματα ελέγχου έρματος και διαχείρισης φορτίου, σε συνδυασμό με τη δυνατότητα απομακρυσμένης πρόσβασης ευνόησε την εμφάνιση νέων απειλών: όπως τον κίνδυνο εκτέλεσης κακόβουλου λογισμικού και το vishing, δηλαδή το voice phishing (phishing) [6]. Στον ναυτιλιακό τομέα, η πρόσβαση τρίτων στα συστήματα και γενικότερα τα σημαντικά περιουσιακά στοιχεία του οργανισμού αποτελούν κοινή πρακτική, προσθέτοντας επιπλέον απαιτήσεις στην κυβερνό- ασφάλεια του οργανισμού. Κατά την αξιολόγηση κινδύνου προτεραιότητα πρέπει να έχουν τα κρίσιμα συστήματα των πλοίων. Η διαδικασία της αξιολόγησης αρχίζει με τον εντοπισμό των πιθανών απειλών, οι οποίες μπορεί να είναι είτε εξωτερικές είτε εσωτερικές. Οι παράγοντες που επιχειρούν να εκμεταλλευτούν πιθανές ευπάθειες μπορεί να είναι οργανισμοί ή άτομα με διαφορετικά κίνητρα:

1. Ακτιβιστές οι οποίοι προσπαθούν να πλήξουν τη φήμη του οργανισμού
2. Εγκληματίες που έχουν ως σκοπό το οικονομικό όφελος
3. Καιροσκόποι που επιθυμούν την πρόκληση
4. Κρατικά υποστηριζόμενοι τρομοκράτες που επιδιώκουν πολιτικό όφελος μέσω της διατάραξης της εύρυθμης λειτουργίας των οικονομιών και των κρίσιμων υποδομών [7]
5. Το προσωπικό του οργανισμού που μπορεί σκόπιμα ή ακούσια να υπονομεύσει τα συστήματα και τα δεδομένα [7]

Ο οργανισμός πρέπει να εξετάσει τη πιθανότητα ανθρώπινων σφαλμάτων κατά τη λειτουργία και τη διαχείριση των συστημάτων του πλοίου, την αποτυχία της τήρησης των τεχνικών και διαδικαστικών μέτρων προστασίας, καθώς και των εργαζόμενων που επιχειρούν σκοπίμως να βλάψουν τον οργανισμό. Οι κυβερνό- επιθέσεις μπορούν να χωριστούν σε δύο κατηγορίες :

A. Τις στοχευμένες και
B. Μη στοχευμένες επιθέσεις

Στις στοχευμένες επιθέσεις ο οργανισμός ή τα συστήματα και τα δεδομένα του πλοίου είναι ο στόχος, ενώ στις μη στοχευμένες επιθέσεις, είναι ένας από τους πολλούς στόχους. Στον πίνακα 1 παρουσιάζονται ορισμένα από τα τυπικά εργαλεία και τεχνικές που χρησιμοποιούνται σε αυτές τις περιπτώσεις.

Μη στοχευμένες επιθέσεις	**Στοχευμένες επιθέσεις**
Malware: Κακόβουλο λογισμικό για να αποκτήσει ο επιτιθέμενος πρόσβαση ή να βλάψει έναν υπολογιστή χωρίς τη γνώση του ιδιοκτήτη	**Brute Force:** Αναζήτηση όλων των πιθανών κωδικών πρόσβασης μέχρι να εντοπιστεί ο σωστός
Social Engineering: Τεχνική που χρησιμοποιείται για να χειραγωγήσει το προσωπικό ενός οργανισμού και να παραβιάσει τις διαδικασίες κυβερνό- ασφάλειας, για παράδειγμα μέσω της αλληλεπίδρασης στα μέσα κοινωνικής δικτύωσης	**Denial of Service (DoS) and Distributed Denial of Service (DDoS):** Υπερχείλιση του δικτύου με δεδομένα προκειμένου να εμποδιστούν οι νόμιμοι χρήστες να αποκτήσουν πρόσβαση σε πληροφορίες (σε DDoS πολλοί

	διακομιστές/υπολογιστές λαμβάνονται υπό έλεγχο)
Phishing: Μηνύματα ηλεκτρονικού ταχυδρομείου που στοχεύουν σε μεγάλο αριθμό ατόμων ζητώντας ευαίσθητες ή εμπιστευτικές πληροφορίες ή μια επίσκεψη σε έναν κακόβουλο ιστότοπο	**Spear Phishing:** Μηνύματα ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα συγκεκριμένο άτομο (που συχνά περιέχει κακόβουλο λογισμικό ή συνδέσμους)
Scanning: Τυχαία επίθεση με στόχο ένα μεγάλο τμήμα του Διαδικτύου	

Πίνακας 1: Τυπικά εργαλεία και τεχνικές επιθέσεων στον κυβερνοχώρο

Σύμφωνα με τις προτάσεις του DNV GL υπάρχουν τέσσερις πιθανοί τρόποι αντιμετώπισης του κινδύνου:

- Η αποφυγή: Καταστρατήγηση του κινδύνου
- Η μείωση: Εφαρμογή «διορθωτικών μέτρων για τη μείωση της πιθανότητας και/ή της σοβαρότητας του κινδύνου»
- Η αποδοχή: Αποδοχή του κινδύνου και αναγνώριση της πιθανότητας να υπάρξουν αρνητικές επιπτώσεις στον οργανισμό
- Η μεταφορά του κινδύνου: Εξωτερική ανάθεση της αντιμετώπισης των επιπτώσεων του κινδύνου, μέσω της ανταλλαγής του με τρίτα μέρη (Ασφαλιστικές Εταιρείες).

Κεφάλαιο 1.3.2: IT/ OT Συστήματα

Κατά την εξέταση της κυβερνό- ασφάλειας ενός πλοίου, είναι απαραίτητο να γίνει η διάκριση μεταξύ των IT συστημάτων και των συστημάτων (OT – Operational Technology) που συμμετέχουν σε επιχειρησιακές λειτουργίες του πλοίου (Μονάδα διαχείρισης θαλασσίου έρματος, σύστημα διαχείρισης φορτίου, ελέγχου ευστάθειας πλοίου κλπ). Σύμφωνα με τις κατευθυντήριες οδηγίες του Διεθνή Ναυτιλιακού Οργανισμού (IMO) για τη διαχείριση του κινδύνου της κυβερνό- ασφάλειας, τα IT συστήματα επικεντρώνονται στη χρήση δεδομένων ως πληροφορία, ενώ τα συστήματα επιχειρησιακών λειτουργιών (OT) επικεντρώνονται στη χρήση δεδομένων για τον έλεγχο ή την παρακολούθηση των φυσικών διεργασιών του πλοίου. Η προστασία της πληροφορίας και της ανταλλαγής δεδομένων μεταξύ των συστημάτων αποτελεί επίσης σημαντικό παράγοντα που πρέπει να εξεταστεί. Η συνεχής ανάπτυξη νέων τεχνολογιών έχει ως αποτέλεσμα την ολοένα και μεγαλύτερη διασύνδεση των συστημάτων πληροφορικής και τηλεπικοινωνιών των πλοίων τόσο μεταξύ τους και όσο και με το Διαδίκτυο. Το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο (BIMCO) επισημαίνει ότι η διασύνδεση μαζί με την ψηφιοποίηση, την ενσωμάτωση και την αυτοματοποίηση των συστημάτων αυξάνει τους κινδύνους στον κυβερνοχώρο - για παράδειγμα με τη μορφή μη εξουσιοδοτημένης πρόσβασης ή κακόβουλων επιθέσεων στα συστήματα και τα δίκτυα του πλοίου [7]. Αντίστοιχα, ο νηογνώμονας Lloyd’s Register (LR) στις σχετικές οδηγίες [9], [10] αναφέρει ότι τα δια- συνδεδεμένα συστήματα του πλοίου, μετατρέπουν το πλοίο σε ένα σύνολο διασυνδεδεμένων συστημάτων – «Ένα σύστημα από συστήματα». Τέτοια πλοία μπορούν να περιγραφούν με έναν νέο όρο, "cyber-enabled". Σύμφωνα με τον Lloyd’s Register (LR), τα συστήματα αυτά δεν υποκαθιστούν ακριβώς τα παραδοσιακά ηλεκτρομηχανικά συστήματα και τους χειριστές αλλά επιτρέπουν το συνδυασμό παραδοσιακών

στοιχείων με πιο περίπλοκες συμπεριφορές. Σύμφωνα με τον LR, οι κίνδυνοι αυτοί πρέπει να αναγνωριστούν, να μελετηθούν και να περιορισθούν για να διασφαλιστεί η ασφαλής ενσωμάτωση των τεχνολογιών στο σχεδιασμό και τη λειτουργία των πλοίων.

Σύμφωνα με τους BIMCO και LR, τα επιχειρησιακά συστήματα των πλοίων περιλαμβάνουν, χωρίς να περιορίζονται σε:

Συστήματα Πλοήγησης: Τα συστήματα πλοήγησης γίνονται όλο και περισσότερο ψηφιακά και δικτυωμένα με συστήματα στη στεριά. Η χρήση αφαιρούμενων μέσων (USB removable media) για την ενημέρωση των συστημάτων αυτών μπορεί να κάνει τα συστήματα γέφυρας, ακόμη και όσα δεν είναι συνδεδεμένα με το διαδίκτυο εξίσου ευάλωτα στις κυβερνό- επιθέσεις. Συστήματα σε αυτήν την κατηγορία είναι για παράδειγμα: το ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών (ECDIS), το παγκόσμιο σύστημα εντοπισμού θέσης (GPS), το δυναμικό σύστημα εντοπισμού θέσης (DPS), το παγκόσμιο δορυφορικό σύστημα πλοήγησης (GNSS), το σύστημα αυτόματης αναγνώρισης (AIS), το σύστημα καταγραφής ταξιδιού (VDR) και το ραντάρ / αυτόματο βοήθημα σχεδιασμού ραντάρ (ARPA).

Συστήματα Διαχείρισης Φορτίου: Τα συστήματα διαχείρισης και ελέγχου φορτίου μπορεί να είναι διασυνδεδεμένα με πολλαπλά συστήματα στην ξηρά. Για παράδειγμα, τα εργαλεία παρακολούθησης αποστολής που είναι διαθέσιμα μέσω σύνδεσης στο διαδίκτυο εκθέτουν κρίσιμα δεδομένα σε κίνδυνο.

Συστήματα Επικοινωνιών: Η σύνδεση στο Διαδίκτυο μέσω δορυφόρου ή άλλων ασύρματων επικοινωνιών, συμπεριλαμβανομένων των ραδιοεπικοινωνιών (ευρυζωνική σύνδεση, Voice Over IP (VOIP)), αυξάνει πιθανώς τις ευπάθειες στο πλοίο.

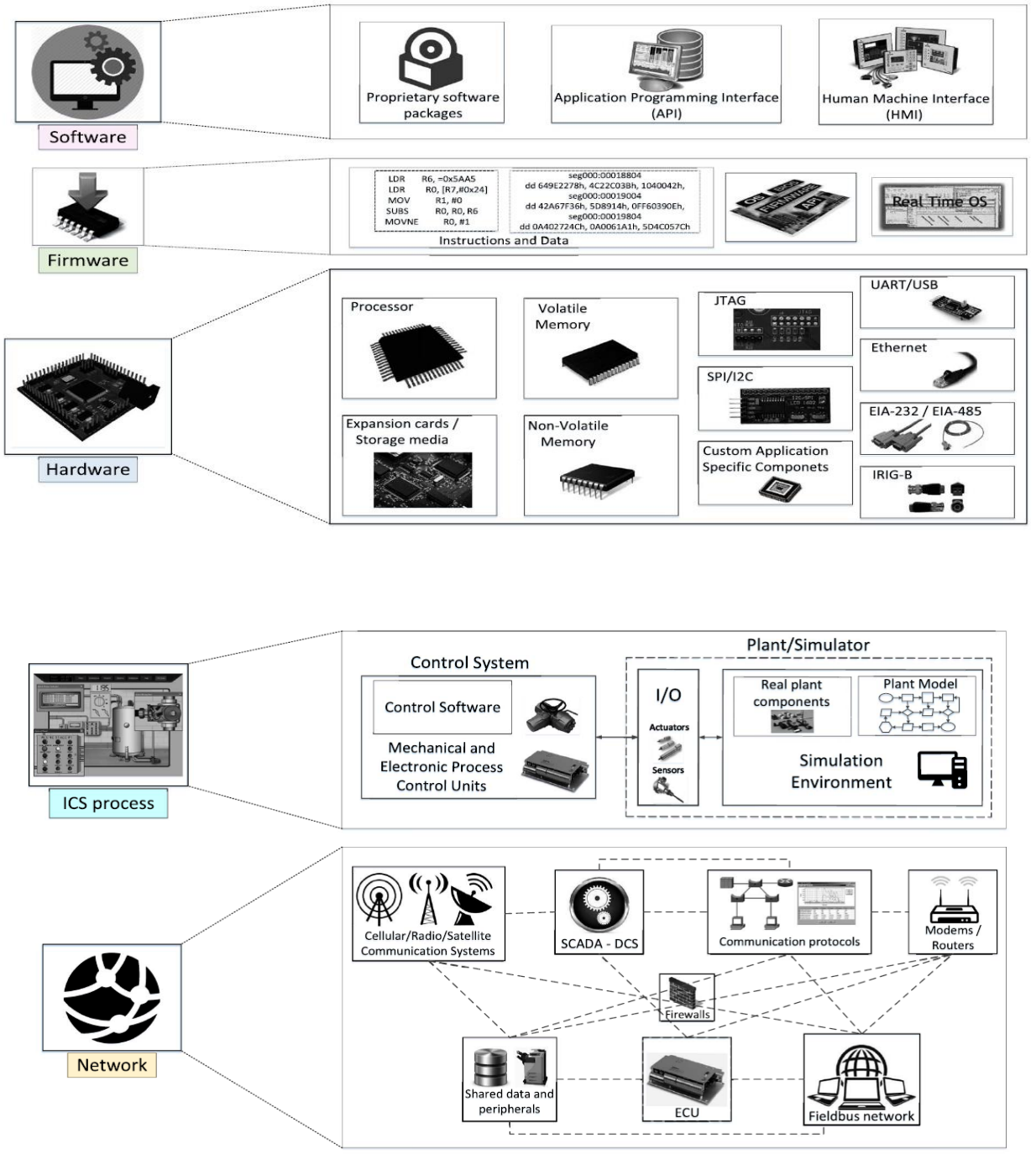
Συστήματα ελέγχου: Τα ψηφιακά συστήματα ελέγχου και παρακολούθησης για ηλεκτρομηχανικά συστήματα, συμπεριλαμβανομένων των κύριων μηχανών, γεννητριών, δεξαμενών έρματος, αντλιών καυσίμου και λαδιού, υδατοστεγών θυρών, συναγερμών πυρκαγιάς και χειριστηρίων, ανεμιστήρων φορτίου, περιβαλλοντικών ελέγχων, είναι ευάλωτα στις επιθέσεις στον κυβερνοχώρο.

Συστήματα ελέγχου πρόσβασης: Τα συστήματα αυτά χρησιμοποιούνται για τη διασφάλιση της φυσικής ασφάλειας του πλοίου και του φορτίου - συμπεριλαμβανομένης της επιτήρησης, του συναγερμού ασφαλείας του πλοίου και των ηλεκτρονικών συστημάτων «επί του πλοίου».

Εξοπλισμός Ναυλωτή: Οι ναυλωτές μπορούν να χρησιμοποιήσουν εξοπλισμό, για παράδειγμα συστήματα σόναρ και σεισμικών ερευνών, ασύρματα σημεία πρόσβασης, θύρες IP και ασύρματα τηλέφωνα, τα οποία αυξάνουν τις ευπάθειες στον κυβερνοχώρο.

Συστήματα εξυπηρέτησης και διαχείρισης επιβατών: Αξιόλογα δεδομένα που αφορούν τους επιβάτες μπορούν να υπόκεινται σε επεξεργασία από ψηφιακά συστήματα που χρησιμοποιούνται για την επιβίβαση και τον έλεγχο πρόσβασης στα πλοία. Οι ευφυείς συσκευές, όπως τα έξυπνα τηλέφωνα και οι φορητοί σαρωτές, μπορούν να δράσουν ως φορείς επίθεσης όταν τα δεδομένα που συλλέγονται μεταδίδονται σε άλλα συστήματα. Τα σταθερά και ασύρματα δίκτυα με σύνδεση στο διαδίκτυο, για παράδειγμα, για χρήση ψυχαγωγίας του επισκέπτη, θα πρέπει να θεωρούνται μη ελεγχόμενα και να

διαχωρίζονται από τα συστήματα κρίσιμης σημασίας για το πλοίο. Τα δίκτυα πλοίων που χρησιμοποιούνται για τη διοίκηση του πλοίου ή την καλή διαβίωση του πληρώματος, καθώς και λογισμικό που παρέχεται από εταιρείες διαχείρισης πλοίων ή τους ιδιοκτήτες, ανήκουν στην ίδια κατηγορία [7], [8].



Εικόνα 1: OT Συστήματα

Κεφάλαιο 1.3.3: Safety and Security

Εκτός από τη διάκριση μεταξύ των IT και OT συστημάτων, η ασφάλεια μπορεί να εξετασθεί από δύο διαφορετικές απόψεις - safety και security. Τόσο το cyber safety όσο και το cyber security επηρεάζουν την ασφάλεια του πλοίου, όχι μόνο στο ίδιο το πλοίο αλλά και στο προσωπικό του πλοίου ή το φορτίο. Σύμφωνα με τις κατευθυντήριες οδηγίες της BIMCO [7], ο όρος cyber- safety επικεντρώνεται στην προστασία των IT και OT συστημάτων των πλοίων και των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και επεξεργασία, ενώ ο όρος cyber- security διαχειρίζεται τον κίνδυνο από την απώλεια διαθεσιμότητας και την ακεραιότητα των κρίσιμων για την ασφάλεια δεδομένων και συστημάτων. Η BIMCO στο [7] εισάγει πολλά παραδείγματα συμβάντων σχετικά με την ασφάλεια στον κυβερνοχώρο, από τα οποία είναι πιθανόν να προκύψουν ατυχήματα. Για παράδειγμα, η κακόβουλη επεξεργασία των δεδομένων ενός συστήματος ECDIS αποτελεί ένα περιστατικό ασφάλειας στον κυβερνοχώρο, το οποίο επηρεάζει τη διαθεσιμότητα και την ακεραιότητα του συστήματος, με αποτέλεσμα να τίθεται σε κίνδυνο η ασφάλεια του πλοίου. Επιπλέον παραδείγματα που παρουσιάστηκαν από τη BIMCO είναι οι αποτυχίες κατά τη διάρκεια της συντήρησης λογισμικού και της απώλειας ή κακόβουλης επεξεργασίας των δεδομένων αισθητήρων που είναι κρίσιμοι για τη λειτουργία του πλοίου (π.χ. inner gas generator). Αυτά τα παραδείγματα δείχνουν, ότι οι αιτίες των cyber safety και cyber security ενδέχεται να διαφέρουν, ωστόσο η αποτελεσματική διαχείριση του κινδύνου με χρήση σεμιναρίων και ευαισθητοποίησης του προσωπικού σχετικά με των διαδικασίες και τις πολιτικές της εταιρείας είναι απαραίτητη και στις δύο περιπτώσεις. Οι διάφορες ομάδες εργασίας της Ευρωπαϊκής Επιτροπής Προτυποποίησης (CSCG, CEN, CENELEC) εμβαθύνουν τον ορισμό της κυβερνό- ασφάλειας στο [16] διαιρώντας την ασφάλεια σε πέντε τομείς:

1. Λειτουργίες,
2. Πληροφόρηση,
3. Επικοινωνίες,
4. Φυσική Ασφάλεια και
5. Εθνική Ασφάλεια

Με την Ασφάλεια Επικοινωνιών, η CEN - CENELEC ορίζει την “προστασία από την απειλή στην τεχνική υποδομή ενός συστήματος" το οποίο μπορεί να καταστήσει το σύστημα ανίκανο να εκτελέσει τις αρχικές προβλεπόμενες δραστηριότητές του. Η Φυσική Ασφάλεια επικεντρώνεται στην πρόληψη φυσικών απειλών, όπως η φυσική πρόσβαση σε ένα διακομιστή ή την εισαγωγή κακόβουλων αφαιρούμενων μέσων σε ένα δίκτυο, τα οποία επηρεάζουν την ομαλή λειτουργία του συστήματος. Η Εθνική Ασφάλεια εξετάζει την πιθανότητα ένας κακόβουλος χρήστης να εκκινήσει επίθεση για πολιτικούς, στρατιωτικούς ή στρατηγικούς λόγους.

Κεφάλαιο 1.3.4: Μοντέλο Εμπιστευτικότητας, Ακεραιότητας, Διαθεσιμότητας (C,I,A)

Το Εθνικό Ινστιτούτο Τεχνολογίας και Προτύπων (NIST) παρουσιάζει μια κατηγοριοποίηση για τα δεδομένα και την ασφάλεια του συστήματος πληροφοριών σύμφωνα με τα ομοσπονδιακά πρότυπα επεξεργασίας πληροφοριών (FIPS). Αυτό το μοντέλο ασφαλείας αναφέρεται συχνά ως εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Confidentiality, Integrity, Availability). Ο νόμος για τη διαχείριση της ασφάλειας πληροφοριών (FISMA) του 2002 ορίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ως τους τρεις στόχους ασφαλείας για πληροφορίες και πληροφοριακά συστήματα.

Η εμπιστευτικότητα ορίζεται ως η διατήρηση περιορισμών στην πρόσβαση σε πληροφορίες. Είναι το δικαίωμα που έχει ο κάθε άνθρωπος σύμφωνα με το οποίο η ιδιωτικότητα και οι προσωπικές πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες. Αυτός ο στόχος του μοντέλου CIA τονίζει την ανάγκη για προστασία των πληροφοριών. Η αξία της εμπιστευτικότητας είναι πολύ σημαντική για την περιορισμένη πρόσβαση σε πληροφορίες. Για παράδειγμα, στην περίπτωση των πληροφοριών ενός οργανισμού ή των προσωπικών δραστηριοτήτων των ατόμων, το απόρρητο θα πρέπει να προστατεύεται. Ωστόσο, για να επιτευχθεί αυτός ο στόχος, τα κανάλια επικοινωνίας πρέπει να παρακολουθούνται και να ελέγχονται σωστά, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.

Η ακεραιότητα των δεδομένων είναι η ιδιότητα που καθορίζει αν τα δεδομένα είναι σωστά, αληθή και αμετάβλητα. Στην ασφάλεια των πληροφοριών, η διασφάλιση της ακεραιότητας των δεδομένων σημαίνει διατήρηση της ακρίβειας και της πληρότητας τους σε όλα τα στάδια της παραγωγής, της επικοινωνίας, της αποθήκευσης και της ανάκτησης των δεδομένων. Πιθανή απώλεια ακεραιότητας σημαίνει μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών. Στην περίπτωση αυτή, θα πρέπει να ληφθούν υπόψη τα παραπάνω χαρακτηριστικά που περιλαμβάνονται σε όλα τα στάδια της παραγωγής, της επικοινωνίας, της αποθήκευσης και της ανάκτησης δεδομένων. Ως ελάχιστο, υπάρχει ανάγκη για:

- Διαχείριση της αρχικής συλλογής δεδομένων
- Προστασία των δεδομένων από μη εξουσιοδοτημένη ή ακούσια αλλαγή
- Εντοπισμός των μετατροπών και κατάλληλη αντιμετώπιση του περιστατικού

Η διαθεσιμότητα είναι ο βαθμός στον οποίο τα δεδομένα είναι προσβάσιμα όταν απαιτείται. Συνήθως αυτό αποτελεί ανησυχία όταν μια εφαρμογή ή ένα σύστημα κάνει χρήση επικοινωνιών ή δεδομένων που παρέχονται ως υπηρεσία εκτός του άμεσου ελέγχου του συστήματος. Ωστόσο, η διαθεσιμότητα είναι επίσης ένα ζήτημα για πιο συμβατικές και μικρότερες αρχιτεκτονικές συστημάτων όπου η υποδομή επικοινωνίας μπορεί να μην έχει τη δυνατότητα να διαχειρίζεται μεγάλο φορτίο δεδομένων ή είναι επιρρεπής σε διακοπές. Απώλεια διαθεσιμότητας σημαίνει ότι το σύστημα δεν είναι ικανό να παρέχει πρόσβαση στους πόρους του.

Από την πλευρά των IT συστημάτων, όταν μελετώνται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (CIA), η εμπιστευτικότητα είναι ο πρωταρχικός στόχος. Πληροφορίες προσωπικών δεδομένων, καθώς και οποιεσδήποτε άλλες ευαίσθητες πληροφορίες του οργανισμού, πρέπει να διατηρούνται εμπιστευτικές. Η ακεραιότητα και η διαθεσιμότητα είναι επίσης παράγοντες με μεγάλη

σημασία, αλλά η εμπιστευτικότητα είναι ύψιστης προτεραιότητας. Από την άλλη πλευρά, από την οπτική γωνία των OT συστημάτων, οι ειδικοί συνήθως θεωρούν τη διαθεσιμότητα ως την πιο κρίσιμη πτυχή για τον οργανισμό. Τα συστήματα πρέπει πάντα να διατηρούνται και να χειρίζονται με ασφάλεια, καθώς μια δυνητική απώλεια μπορεί να οδηγήσει σε επικίνδυνες καταστάσεις. Η ακεραιότητα και η εμπιστευτικότητα των δεδομένων διαδραματίζουν επίσης ζωτικό ρόλο στην προστασία των συστημάτων του πλοίου, αλλά το μοντέλο εδώ γίνεται AIC (Availability, Integrity, Confidentiality) – και διαφοροποιείται ελαφρώς από την παραπάνω προσέγγιση. Στη ναυτιλιακή βιομηχανία, για παράδειγμα, η απώλεια της εμπιστευτικότητας των δεδομένων που παράγουν οι αισθητήρες των OT συστημάτων έχει χαμηλή επίδραση στις επιχειρησιακές λειτουργίες του πλοίου, δεδομένου ότι οι αισθητήρες αυτοί είναι διαθέσιμοι σε όλους πάνω στο πλοίο. Ωστόσο, από την πλευρά της ασφάλειας του πλοίου είναι σημαντικό οι πληροφορίες που μεταδίδονται από τους αισθητήρες να είναι αξιόπιστες, γεγονός που αυξάνει τη σημαντικότητα της ακεραιότητας. Πρόκειται επίσης για σοβαρό ζήτημα ασφάλειας εάν δεν είναι δυνατή η πρόσβαση στις πληροφορίες των αισθητήρων, γεγονός που οδηγεί σε δυνητικά σε υψηλό αντίκτυπο λόγω απώλειας διαθεσιμότητας. Οι λύσεις που έχουν σχεδιαστεί για την ασφάλεια των IT συστημάτων, στοχεύουν στην αντιμετώπιση κυρίως ζητημάτων ιδιωτικότητας. Είναι συνήθης πρακτική μετά από μια κακόβουλη επίθεση στα IT συστήματα, να αντιμετωπίζονται όλες οι ύποπτες δραστηριότητες κλείνοντας τα συστήματα. Ωστόσο, η υιοθέτηση της ίδιας προσέγγισης όσον αφορά τα OT συστήματα μπορεί να έχει επικίνδυνες συνέπειες για τη λειτουργία των πλοίων. Κατά την αντιμετώπιση της ασφάλειας των OT, τα μέτρα που εφαρμόζονται στα IT συστήματα δεν εγγυώνται πλήρως την ασφάλεια και την επιχειρησιακή συνέχεια των συστημάτων. Η απόφαση ενός συστήματος ανίχνευσης (IDS system) – είτε θετική είτε αρνητική - είναι ικανή να ενισχύσει την αντιμετώπιση μιας επίθεσης σε IT συστήματα, αλλά είναι πιθανότερο να προκαλέσει σημαντικά προβλήματα κλείνοντας ένα OT σύστημα.

Σύμφωνα με την BIMCO [13], κατά την αξιολόγηση του κινδύνου με βάση το μοντέλο CIA ορίζονται οι παρακάτω καταστάσεις:

- Απώλεια Εμπιστευτικότητας: Αποκάλυψη πληροφοριών ή δεδομένων σχετικά με πλοία, πληρώματα, φορτίο ή επιβάτες σε μη εξουσιοδοτημένες οντότητες
- Απώλεια Ακεραιότητας: Τροποποίηση ευαίσθητων για το σκάφος δεδομένων τα οποία είναι δυνατόν να θέσουν σε κίνδυνο την ασφαλή και αποτελεσματική λειτουργία του πλοίου
- Απώλεια Διαθεσιμότητας: Προκαλείται από την καταστροφή των πληροφοριών ή των δεδομένων ή διακοπή των συστημάτων του πλοίου

Πρόσθετες ιδιότητες, όπως η αξιοπιστία, η μη αποκήρυξη και η λογοδοσία, μπορούν επίσης να προστεθούν στο μοντέλο, αλλά η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι οι βασικότερες απαιτήσεις. Ο Πίνακας 2 παρουσιάζει τα πιθανά επίπεδα επιπτώσεων του μοντέλου της CIA και περιγράφει τη φύση των συνεπειών μίας παραβίασης ασφάλειας σε κάθε επίπεδο:

Επίπεδο	**Ορισμός**	**Συνέπειες**
Χαμηλή	Απώλεια στα στοιχεία του μοντέλου CIA (A): περιορισμένης έκτασης επίδραση στα	Μια παραβίαση ασφαλείας μπορεί: i) να προκαλέσει πρόβλημα στη λειτουργία του

	περιουσιακά στοιχεία του οργανισμού (πλοία ή άτομα)	πλοίου ή τη διάρκεια στην οποία μπορούν να χρησιμοποιηθούν οι κύριες λειτουργίες εξακολουθούν να εκτελούνται αλλά η αποτελεσματικότητά τους μειώνεται αισθητά · ii) προκαλεί μικρές ζημιές στα περιουσιακά στοιχεία · iii) να έχουν ως αποτέλεσμα οικονομικά μειονεκτήματα απώλεια; ή iv) έχουν ως αποτέλεσμα μικρότερη βλάβη σε άτομα.
Μεσαία	Απώλεια στα στοιχεία του μοντέλου CIA (A): σημαντική επίδραση στα περιουσιακά στοιχεία του οργανισμού (πλοία ή άτομα)	Μια παραβίαση ασφαλείας μπορεί: i) Να προκαλέσει σημαντική- υποβάθμιση της λειτουργίας του πλοίου συνολικά ή για μία χρονική διάρκεια στην οποία οι κύριες λειτουργίες είναι δυνατόν να πραγματοποιούνται, ωστόσο η λειτουργικότητα τους να μειώνεται σημαντικά · ii) να προκαλέσει σημαντική ζημιά στα περιουσιακά στοιχεία του οργανισμού · ή iii) να προκαλέσει σημαντική βλάβη στους εργαζόμενους, εξαιρουμένης της απώλειας ζωής.
Υψηλή	Απώλεια στα στοιχεία του μοντέλου (A): σοβαρές ή καταστροφικές επιπτώσεις για τον οργανισμό	Μια παραβίαση ασφαλείας μπορεί: i) να προκαλέσει σοβαρή υποβάθμιση ή απώλεια της λειτουργίας του πλοίου σε στην οποία μία ή περισσότερες πρωτογενείς λειτουργίες δεν μπορούν να εκτελεστούν. ii) προκαλούν σημαντική ζημιά στα περιουσιακά στοιχεία του οργανισμού ·iii) έχουν ως αποτέλεσμα σημαντικές οικονομικές ζημίες · ή iv) προκαλούν σοβαρή ή καταστροφική βλάβη στους εργαζόμενους, συμπεριλαμβανομένης της απώλειας ζωής.

Πίνακας 2:Μοντέλο CIA [13]

Κεφάλαιο 1.3.5: Ο Ανθρώπινος Παράγοντας

Η επίδραση του ανθρώπινου παράγοντα στην ασφάλεια δεν μπορεί να υποτιμηθεί. Το ανθρώπινο στοιχείο διαδραματίζει σημαντικό ρόλο στην πλειοψηφία των περιστατικών στον κυβερνοχώρο [3]. Λόγω του υψηλού βαθμού δια- συνδεσιμότητας των συστημάτων, ακόμη και μικρά ανθρώπινα σφάλματα, μπορούν να προκαλέσουν σοβαρά προβλήματα στη λειτουργία τους. Η εκπαίδευση του προσωπικού σε θέματα ασφαλείας κρίνεται απαραίτητη για την αποφυγή περιστατικών που μπορεί να προκληθούν για παράδειγμα με χρήση κοινωνικής μηχανικής, ή από εξωτερικούς συνεργάτες που χρησιμοποιούν απομακρυσμένη πρόσβαση. Όταν εξετάζεται η ασφάλεια, είναι υποχρεωτική μια ολιστική προσέγγιση. Το μοντέλο κρεμμυδιού είναι ένας αποτελεσματικός τρόπος για να περιγραφεί η σημασία του ανθρώπινου παράγοντα για την ασφάλεια στον κυβερνοχώρο. Για παράδειγμα, η απενεργοποίηση των περιττών θυρών αφαιρούμενων μέσων (USB) ενός φορητού υπολογιστή μπορεί να είναι μια τεχνική μέθοδος ελέγχου για την ασφάλεια- μειώνοντας την πιθανότητα εισαγωγής κακόβουλων εξωτερικών συσκευών στο φορητό υπολογιστή. Ο φορητός υπολογιστής μπορεί να θεωρηθεί ότι βρίσκεται στο κέντρο ενός ανοιχτού κρεμμυδιού. Ο υπολογιστής βρίσκεται σε ένα ντουλάπι, το οποίο αντιπροσωπεύει το επόμενο στρώμα του κρεμμυδιού. Το ντουλάπι βρίσκεται σε ένα δωμάτιο, το οποίο είναι μέσα σε ένα πλοίο, το οποίο αντιπροσωπεύουν τα επόμενα στρώματα του κρεμμυδιού. Η πρόσβαση από το ένα στρώμα στο άλλο είναι ασφαλισμένη - για παράδειγμα, μόνο τα εξουσιοδοτημένα άτομα επιτρέπονται στο σκάφος και περαιτέρω, μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στο δωμάτιο. Τέλος, μόνο περιορισμένος αριθμός ατόμων μπορεί να έχει κλειδί στο ντουλάπι. Για να έχει πρόσβαση στις θύρες USB του φορητού υπολογιστή, ο επιτιθέμενος πρέπει να είναι ικανός να ξεπεράσει όλους αυτούς τους ελέγχους, οι οποίοι συχνά σχετίζονται με τον ανθρώπινο παράγοντα. Ο επιτιθέμενος μπορεί για παράδειγμα να εισχωρήσει μέσα στο πλοίο με χρήση κοινωνικής μηχανικής, η οποία ενεργοποιείται από ανθρώπινο σφάλμα. Από την άλλη πλευρά, σε περίπτωση που όλα τα εξωτερικά στρώματα πετύχουν τα μέτρα προστασίας, ο επιτιθέμενος δεν θα αποκτήσει ποτέ πρόσβαση στο φορητό υπολογιστή. Σε αυτήν την περίπτωση, η απενεργοποίηση των περιττών θυρών USB έχει μικρή σημασία. Το σενάριο αυτό αντικατοπτρίζει τη σημασία του σχεδιασμού της ασφάλειας του κυβερνοχώρου ως ένα σύνολο πολιτικών, ξεκινώντας από τα υψηλότερα επίπεδο.

Κεφάλαιο 1.4: Στόχος της Εργασίας

Βασικοί στόχοι της διατριβής είναι:

- Να μελετηθεί η σημασία της κυβερνό- ασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής ενός πλοίου
- Να εξετασθεί ο δυνητικός αντίκτυπος των κυβερνό-επιθέσεων σε ένα πλοίο, καθώς και η αντανάκλαση στα συστήματα της εταιρείας
- Να διερευνηθούν τα συστήματα ενός πλοίου και οι επιπτώσεις που μπορούν να έχουν στο θαλάσσιο περιβάλλον από περιστατικό ασφαλείας
- Να μελετηθούν οι διάφοροι παράγοντες απειλής και να προσδιορισθούν τα κίνητρά τους
- Να χαρτογραφηθεί το τοπίο της επίθεσης και να αναγνωρισθεί η προέλευση των επιθέσεων

- Να αναγνωριστούν τα ευάλωτα στοιχεία του συστήματος και αποτελούν απειλή για την ασφάλεια του οργανισμού
- Να προσδιοριστούν οι κύριες πτυχές που συμβάλλουν στην αντιμετώπιση του κινδύνου και να προταθεί ένα πλαίσιο για την αντιμετώπιση των αδυναμιών

Κεφάλαιο 2: Ψηφιακός Μετασχηματισμός της Ναυτιλιακής Βιομηχανίας

Κεφάλαιο 2.1: Εισαγωγή

Σήμερα η ναυτιλία αποτελεί αναπόσπαστο μέρος της παγκόσμιας οικονομίας και διακινεί σχεδόν το 80% του παγκόσμιου εμπορίου. Κάθε χώρα είναι πλέον αλληλεξαρτώμενη των συναλλαγών που πραγματοποιούνται κυρίως από τη θάλασσα. Σχεδόν 50.000 πλοία και ένα εκατομμύριο ναυτικοί συμμετέχουν ενεργά σε αυτό το παγκόσμιο εμπόριο [14]. Σε αυτό εμπορικό πλαίσιο, το ψηφιακό πεδίο αυξάνεται συνεχώς τα τελευταία 25 χρόνια για τους ναυτιλιακούς οργανισμούς. Η τεχνολογία ρυθμίζει τις επικοινωνίες καθώς και τον έλεγχο και διαχείριση του φορτίου του πλοίου. Αυτός ο τεχνολογικός μετασχηματισμός του εμπορικού πλοίου έχει αλλάξει βαθιά τον τρόπο με τον οποίο γίνεται η διαχείριση του. Σήμερα πραγματοποιούνται ανταλλαγές καθημερινά μεταξύ του πλοίου, της εταιρείας, των λιμενικών εγκαταστάσεων και των ναυτιλιακών πρακτόρων. Η ψηφιοποίηση αναφέρεται στη "χρήση ψηφιακών τεχνολογιών για την αλλαγή του επιχειρησιακού μοντέλου ενός οργανισμού και να προσφέρει νέες ευκαιρίες" [15]. Είναι ευρέως κατανοητό ότι η ανάγκη αλλαγής και βελτιστοποίησης διαφορετικών επιχειρηματικών μοντέλων σήμερα είναι άμεσα συνδεδεμένη με την εφαρμογή των νέων ψηφιακών τεχνολογιών που παρέχουν αυτοματοποίηση των διαδικασιών και λειτουργιών στα πλοία. Αυτός ο αυτοματισμός μπορεί να αποδειχθεί ότι βελτιώνει την ασφάλεια, τη λειτουργία των συστημάτων και την αποδοτικότητα του πλοίου και, παράλληλα, έχει ως αποτέλεσμα την αύξηση των πιθανών κινδύνων. Όσον αφορά την προοπτική του ψηφιακού μετασχηματισμού των ναυτιλιακών οργανισμών, οι εταιρείες εφαρμόζουν όλες τις διαφορετικές τεχνολογίες και προσπαθούν να τις συνδυάσουν με το υφιστάμενο επιχειρησιακό μοντέλο καθώς και με νέες υπηρεσίες και προϊόντα. Ωστόσο, αυτός ο συνδυασμός τελικά οδηγεί σε μια τελείως διαφορετική κατάσταση λειτουργίας. Ο οργανισμός δεν λειτουργεί πλέον με τον υφιστάμενο τρόπο και αυτό το αποτέλεσμα είναι στην πραγματικότητα αυτό που πρεσβεύει ο ψηφιακός μετασχηματισμός.

Κεφάλαιο 2.2: Το πλοίο σαν Data Center

Ο ναυτιλιακός τομέας αποτελεί ζωτικό τμήμα της παγκόσμιας οικονομίας, είτε φέρει φορτίο, είτε επιβάτες είτε οχήματα. Τα πλοία καθίστανται όλο και περισσότερο πολύπλοκα και εξαρτώνται από την εκτεταμένη χρήση ψηφιακών τεχνολογιών καθ' 'όλη τη διάρκεια λειτουργίας τους. Αν και η δια-συνδεσιμότητα των συστημάτων και το Διαδίκτυο ωφελεί τις επιχειρήσεις για πολύ μεγάλο χρονικό διάστημα στις άλλες βιομηχανίες, αρχίζουν σταδιακά να γίνονται ολοένα και πιο δημοφιλή στο ναυτιλιακό περιβάλλον.

Οι λόγοι για αυτή την αυξημένη δημοτικότητα σε σχέση με το κόστος και τη λειτουργικότητα είναι οι ακόλουθοι:

Υπολογιστική ισχύς: Τα συστήματα μπορούν πλέον να λειτουργούν και να εκτελούν εντολές ταχύτερα. Μεγάλο πλήθος εντολών, μαθηματικών υπολογισμών και αλγορίθμων μπορούν να εκτελούνται εντός δευτερολέπτων παρέχοντας συνεχή ροή πληροφοριών και άμεσες απαντήσεις στη βιομηχανία.

Αποθήκευση δεδομένων: Η εξέλιξη στις δυνατότητες αποθήκευσης δεδομένων, του υλικού και του υπολογισμού στο νέφος (cloud) έχουν συμβάλει στην ανάπτυξη οικονομικά προσιτών και ισχυρών λύσεων αποθήκευσης δεδομένων που ωφελούν τις εταιρείες στη διαχείριση της εκθετικά αναπτυσσόμενων όγκων δεδομένων.

Συνδεσιμότητα: Είναι μια νέα και αναπτυσσόμενη πτυχή για τη ναυτιλιακή βιομηχανία. Η βελτίωση της δια- συνδεσιμότητας ωφελεί τη βιομηχανία παρέχοντας σε πραγματικό χρόνο πληροφορίες σχετικά με τις επιδόσεις του πλοίου (και όχι μόνο) εκατοντάδες μίλια μακριά από την ακτή.

Αισθητήρες: Συλλέγουν δεδομένα σε πραγματικό χρόνο σχετικά με τα συστήματα του πλοίου, όπως οι εκπομπές αερίων και η θερμοκρασία του φορτίου, αυξάνουν την αποδοτικότητα της συντήρησης και της ασφάλειας και ταυτόχρονα μειώνουν τις λειτουργικές δαπάνες και τον κίνδυνο αποτυχίας λόγω αμέλειας.

Η ικανότητα και η κάλυψη των συστημάτων των πλοίων εξελίχθηκαν σταδιακά κατά τη διάρκεια του 20ό αιώνα. Η Παγκόσμια Ασφάλεια Ναυτιλιακών Κινδύνων (GMDSS) έφερε την εισαγωγή δορυφορικών επικοινωνιών με την απλή, αλλά αποτελεσματική, ψηφιακή αποστολή μηνυμάτων για την υποστήριξη των πλοίων σε περιπτώσεις κινδύνου. Τα Δορυφορικά συστήματα, σήμερα, χρησιμοποιούνται όλο και περισσότερο για μια ποικιλία λειτουργικών και εμπορικών σκοπών, καθώς και για αναψυχή και ψυχαγωγία [16]. Παρόλο που η "συνδεσιμότητα" έχει πρωτίστως να κάνει με την επικοινωνία, ο όρος είναι ανούσιος αν δεν περιλαμβάνει και τα δεδομένα που επικοινωνούν. Σήμερα υπάρχουν τεράστιοι όγκοι δεδομένων στα πλοία και αυτά παράγονται από πολλές διαφορετικές πηγές. Πολλά από τα ενσωματωμένα συστήματα είναι σχεδιασμένα για τη συλλογή και την παρουσίαση δεδομένων στην εταιρεία, το πλήρωμα, σε διαφορετικούς προμηθευτές και κατασκευαστές ως ζωτικής σημασίας βοηθητικά μέσα στη διαδικασία λήψης αποφάσεων κατά την καθημερινή λειτουργία του πλοίου. Ως αποτέλεσμα της εξέλιξης των αισθητήρων, της επικοινωνίας και ανάλυσης δεδομένων, προκύπτουν νέες αρχιτεκτονικές πλοίων που επιτρέπουν την υλοποίηση νέων εφαρμογών με βάση τα δεδομένα που είναι διαθέσιμα στο πλοίο. Για παράδειγμα, τα ναυπηγεία Hyundai Heavy Industries (HHI), τον Ιούλιο του 2017, ανακοίνωσαν την ανάπτυξη της ολοκληρωμένης λύσης έξυπνης πλοήγησης (ISSS), μιας συλλογής συστημάτων τεχνολογίας πληροφοριών που στοχεύουν στη βελτιστοποίηση των διαδικασιών πλοήγησης, συλλέγοντας και αναλύοντας πληροφορίες σε πραγματικό χρόνο σχετικά με την πλοήγηση των πλοίων. Για το σκοπό αυτό η νέα αρχιτεκτονική χρησιμοποιεί αισθητήρες που επεξεργάζονται μια ποικιλία δεδομένων, όπως δεδομένα σχετικά με την τοποθεσία του πλοίου, τον καιρό και τον ωκεανό, καθώς και πληροφορίες σχετικά με την προπέλα και την κατάσταση του φορτίου του πλοίου. Τα δεδομένα που συλλέγονται θα επιτρέψουν στους οργανισμούς να μελετήσουν όχι μόνο την πληροφορία σε πραγματικό χρόνο αλλά να επεξεργαστούν ιστορικά δεδομένα του στόλου, την ανάλυση των πληροφοριών, την παρακολούθηση της κατάστασης των πλοίων και την αξιολόγηση χρήσιμων δεδομένων για κρίσιμες αποφάσεις, σε πραγματικό χρόνο. Η HHI (Hyundai Heavy Industries) ισχυρίζεται ότι η συγκεκριμένη λύση είναι σε θέση να μειώσει το ετήσιο λειτουργικό κόστος κατά 6%

και το έχει ήδη υλοποιήσει σε 300 πλοία και σύμφωνα με την Clarkson Research αναμένεται να εγκατασταθεί σε περίπου 6.500 πλοία παγκοσμίως τα επόμενα πέντε χρόνια [17]. Η δια-συνδεσιμότητα των συστημάτων του πλοίου θα επιτρέψει μέσω των αναλύσεων δεδομένων να προσφέρει σημαντικά πλεονεκτήματα στους ναυτιλιακούς οργανισμούς, όπως καλύτερη απόδοση και βελτιωμένη αξιοπιστία και ασφάλεια στα πλοία. Η ναυτιλιακή βιομηχανία κινείται πλέον στον κόσμο της ψηφιοποίησης. Η Ανάλυση Μεγάλων δεδομένων, το Διαδίκτυο των πραγμάτων, η υπολογιστική στο νέφος (cloud computing), το machine learning και η τεχνητή νοημοσύνη είναι μόνο μερικές από τις πτυχές που θα μεταμορφώσουν τον τρόπο με τον οποίο λειτουργούν τα πλοία. Τα μη επανδρωμένα αυτόνομα πλοία δημιουργούν ήδη αυξανόμενο ενδιαφέρον για τη βιομηχανία, αλλά τα συστήματα απομακρυσμένης παρακολούθησης και ελέγχου των πλοίων είναι ήδη πραγματικότητα για πολλές εταιρείες σε όλο τον κόσμο.

Κεφάλαιο 2.3: Σύγχρονες Προκλήσεις

Η ταχεία εξέλιξη στη χρήση και την εξάρτηση από τις ψηφιακές τεχνολογίες, καθώς και η πρόοδος της αυτοματοποίησης αυξάνουν τη σημασία της αντιμετώπισης όλων των πιθανών προκλήσεων. Ο παραδοσιακός τρόπος επικοινωνίας μέσω της φωνή και του χαρτιού έχει αντικατασταθεί από τις ψηφιακές και αυτοματοποιημένες ανταλλαγές πληροφοριών. Αυτή η νέα τάση δημιουργεί νέες απαιτήσεις για την εξακρίβωση της ταυτότητας του παραγόμενου εγγράφου, την ακεραιότητα των μηνυμάτων καθώς και την εμπιστευτικότητα όταν αυτό απαιτείται. Μερικές από τις προκλήσεις που θα κληθεί η βιομηχανία να αντιμετωπίσει πριν την υιοθέτηση αυτών των πολλά υποσχόμενων καινοτομιών αφορούν την ποιότητα δεδομένων, την προσαρμογή των οργανισμών στους κανονισμούς σχετικά με την ασφάλεια και την ανθρώπινη συμβολή όσον αφορά την αυτονομία. Η εμπιστοσύνη αποτελεί επίσης σημαντικό παράγοντα για την επιτυχή υιοθέτηση της τέταρτης βιομηχανικής επανάστασης στον ναυτιλιακό κόσμο. Η εμπιστοσύνη στην ποιότητα των δεδομένων που παράγουν οι αισθητήρες, η εμπιστοσύνη στους ανθρώπους που χειρίζονται τα δεδομένα καθώς και η εμπιστοσύνη στους αλγόριθμους που εξάγουν το συμπέρασμα από τα παραγόμενα δεδομένα είναι απαραίτητες προϋποθέσεις για τη διατήρηση και την αύξηση της λογοδοσίας μεταξύ των διαφόρων μερών [18]. Η αντιμετώπιση των προκλήσεων ασφάλειας που προκύπτουν από τις ψηφιακές τεχνολογίες είναι μια σοβαρή πτυχή την οποία τόσο οι κυβερνήσεις όσο και οι οργανισμοί θα πρέπει να λάβουν υπόψη.

Εν κατακλείδι, η αυξανόμενη χρήση μεγάλων δεδομένων, τα έξυπνα πλοία και το Διαδίκτυο των πραγμάτων θα αυξήσουν τον όγκο των πληροφοριών που θα είναι διαθέσιμες στους επιτιθέμενους και την πιθανή επιφάνεια επίθεσης σε επίδοξους εγκληματίες του κυβερνοχώρου. Αυτό καθιστά την ανάγκη για ισχυρές προσεγγίσεις στην ασφάλεια του κυβερνοχώρου, σημαντικές τόσο τώρα όσο και στο μέλλον.

Κεφάλαιο 2.4: Προκλήσεις που Αφορούν την Ασφάλεια

Ως ένας τεράστιος και σε μεγάλο βαθμό μη ελέγξιμος χώρος, ο τομέας της ναυτιλίας είναι επιρρεπής στη διάδοση των εγκληματικών φορέων που επωφελούνται από τα ανοιχτά θαλάσσια σύνορα. Η Πειρατεία και η τρομοκρατία στη θάλασσα, το λαθρεμπόριο όπλων και ανθρώπων, η παράνομη μετανάστευση, η ρύπανση του θαλάσσιου περιβάλλοντος είναι μόνο λίγες από τις παράνομες

δραστηριότητες που πραγματοποιούνται στην θάλασσα. Ωστόσο, ένας από τους πιο σοβαρούς κινδύνους που η ψηφιοποίηση και η αύξηση της δια- σύνδεσης των συστημάτων πρόκειται να αντιμετωπίσουν προέρχεται από την ασφάλεια στον κυβερνοχώρο. Σήμερα, ανταλλαγές δεδομένων λαμβάνουν χώρα καθημερινά μεταξύ των πλοίων, της εταιρείας, των λιμένων και των ναυτιλιακών πρακτόρων. Το πλοίο δεν επωφελείται πλέον από ένα ψηφιακό επίπεδο ασφαλείας απομονώνοντας το από όλα τα άλλα ψηφιακά δίκτυα. Το πλοίο πλέον είναι ένα πολύπλοκο σύνολο βιομηχανικών συστημάτων. Η λειτουργία των συστημάτων δυστυχώς δεν εξαιρείται από πιθανά ψηφιακά σφάλματα. Επομένως, τα συστήματα αυτά μπορούν να αποτελέσουν το σημείο εισόδου για μια κακόβουλη πράξη.

Οι δραστηριότητες στον κυβερνοχώρο έχουν αρχίσει να αποτελούν υψηλή προτεραιότητα για τη ναυτιλιακή βιομηχανία, καθώς ήδη από το 2010 η επιτροπή στρατηγικής άμυνας και ασφάλειας κατέταξε την ασφάλεια στον κυβερνοχώρο ως απειλή για την εθνική ασφάλεια [19]. Ωστόσο, η τρέχουσα εξάρτηση από την ψηφιακή επικοινωνία, την αυτοματοποίηση και τη διασύνδεση της παγκόσμιας οικονομίας καθιστά την ασφάλεια του κυβερνοχώρου όχι μόνο θέμα εθνικής ασφάλειας αλλά παγκόσμιας σημασίας. Αναδυόμενες απειλές στον κυβερνοχώρο, συμπεριλαμβανομένων του κακόβουλου λογισμικού, των εγκλημάτων και των διαρροών δεδομένων έχουν επιπτώσεις στις κυβερνήσεις αλλά και τη βιομηχανία. Παρόλο που οι κακόβουλες ενέργειες εναντίον ενός πλοίου παραμένουν εμπιστευτικές και περιορισμένες στο ευρύ κοινό, είναι θέμα τεράστιας σημασίας να προστατευθεί. Μια δυνητική επίθεση στα συστήματα ενός πλοίου μπορεί να οδηγήσει σε τραυματισμό ή απώλεια ζωής, καταστροφή στο περιβάλλον, τη ναυτιλία και στις λιμενικές υποδομές. Επιπλέον, μια παραβίαση της κυβερνό- ασφάλειας είναι πιθανό να προκαλέσει διαταραχές στις επιχειρησιακές διαδικασίες, με αποτέλεσμα να υπάρξουν οικονομικές απώλειες για τον οργανισμό και αρνητικές επιπτώσεις στη φήμη του. Λαμβάνοντας υπόψη όλους αυτούς τους κινδύνους, η εταιρεία είναι πιθανό να αντιμετωπίσει οικονομική ζημία ή νομικά ζητήματα καθώς και την πρόκληση να ανακάμψει γρήγορα από το περιστατικό και να επανέλθει στην κανονικότητα. Η προστασία ενός πλοίου σημαίνει διατήρηση των λειτουργικών και οργανωτικών λειτουργιών. Ο τελικός στόχος αποσκοπεί στην εξασφάλιση ότι η κακόβουλη πράξη δεν μπορεί να θέσει σε κίνδυνο τη λειτουργία του πλοίου. Τα πλοία είναι ένα μέσο μεταφοράς μεταξύ πολλών άλλων. Ωστόσο, η βιομηχανία θα πρέπει να γνωρίζει ότι είναι δεν είναι άνοσα απέναντι στο “τρίγωνο του κινήτρου” της απειλής του κυβερνοχώρου: κλοπή χρημάτων, κλοπή ευαίσθητων δεδομένων, δραστηριότητες ακτιβισμού / τρομοκρατίας [20]. Η ασφάλεια δεν περιορίζεται στην αποτροπή της πρόσβασης κακόβουλων χρηστών σε συστήματα και πληροφορίες, με ενδεχόμενη απώλεια εμπιστευτικότητας και έλεγχο τους. Αφορά επίσης τη διατήρηση της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των συστημάτων, εξασφαλίζοντας τη συνέχεια της επιχείρησης και τη συνεχή χρήση των ψηφιακών στοιχείων και συστημάτων. Για να επιτευχθεί αυτό πρέπει να δοθεί σημασία όχι μόνο στην προστασία των συστημάτων των πλοίων από φυσική επίθεση αλλά και να διασφαλιστεί ο σχεδιασμός των συστημάτων και η υποστήριξη των διαδικασιών, ώστε να είναι ανθεκτικές από πιθανές επιθέσεις. Να υπάρχουν κατάλληλοι τρόποι επαναφοράς σε περίπτωση παραβίασης των συστημάτων αυτών. Η απειλή εκ των έσω, από υπαλλήλους στα γραφεία των οργανισμών ή ακόμα και από ναυτικούς που αποφασίζουν να ενεργήσουν με κακόβουλο ή μη τρόπο δεν μπορούν να αγνοηθούν. Οι Ιδιοκτήτες πλοίων πρέπει να κατανοήσουν την ασφάλεια στον κυβερνοχώρο και να προωθήσουν την ευαισθητοποίηση σχετικά με το θέμα αυτό στα ενδιαφερόμενα μέρη, συμπεριλαμβανομένου του προσωπικού του πλοίου. Η

ασφάλεια μπορεί να οριστεί ως “συλλογή εργαλείων, πολιτικών ασφάλειας, κατευθυντήριων οδηγιών, προσεγγίσεων διαχείρισης κινδύνου, δράσεων, καταρτίσεων, βέλτιστων πρακτικών και τεχνολογιών που μπορούν να χρησιμοποιηθούν για την προστασία των συστημάτων και γενικά των περιουσιακών στοιχείων του χρήστη”[21]. Στο πλαίσιο του ορισμού αυτού, ως «κυβερνοχώρος» ορίζεται το σύνολο των διασυνδεδεμένων δικτύων τόσο των IT συστημάτων όσο και των φυσικών συστημάτων που χρησιμοποιούν ηλεκτρονικά, υπολογιστικά και ασύρματα συστήματα, συμπεριλαμβανομένων των πληροφοριών, των υπηρεσιών, των κοινωνικών και επιχειρησιακών λειτουργιών των πλοίων. Σε ένα πλοίο, τα συστήματα που βασίζονται σε υπολογιστές θα περιλαμβάνουν μια σειρά στοιχείων (για παράδειγμα προσωπικοί υπολογιστές (PC), φορητοί υπολογιστές, tablets, διακομιστές και συσκευές δικτύωσης όπως δρομολογητές και διακόπτες, συστήματα ελέγχου, αισθητήρες, ενεργοποιητές, ραντάρ κ.λπ.). Ο «οργανισμός και τα περιουσιακά στοιχεία του χρήστη» περιλαμβάνουν συνδεδεμένες υπολογιστικές συσκευές, προσωπικό, υποδομή, εφαρμογές, υπηρεσίες, συστήματα τηλεπικοινωνιών και το σύνολο των μεταδιδόμενων, επεξεργασμένων και / ή αποθηκευμένων δεδομένων και πληροφοριών στο κυβερνοχώρο. Η ποικίλη φύση των απειλών στον κυβερνοχώρο σημαίνει ότι δεν υπάρχει ενιαία προσέγγιση ικανή να αντιμετωπίσει όλους τους κινδύνους που προκύπτουν. Ο ρυθμός μεταβολής στην τεχνολογία και η σταθερή ροή σοβαρών τρωτών σημείων στα λειτουργικά συστήματα, τις βιβλιοθήκες λογισμικού και τις εφαρμογές, σημαίνει ότι οποιαδήποτε στρατηγική πρέπει να παρακολουθείται τακτικά. Η αλλαγή των επιχειρήσεων έχει επίσης σημαντικό αντίκτυπο στην ασφάλεια στον κυβερνοχώρο, για παράδειγμα η υιοθέτηση της πολιτικής “Bring your Own Device” και στην τάση να θεωρεί ορισμένα στοιχεία ενεργητικού ως υπηρεσίες, για παράδειγμα, η εξ αποστάσεως διαχείριση ορισμένων στοιχείων ενεργητικού από ένα τρίτο οργανισμό, όπως η διάταξη των σταθμών παραγωγής ηλεκτρικής ενέργειας / στροβίλων για την ισχύ ή την πρόωση. Είναι ευρέως κατανοητό ότι ένα μεγάλο ποσοστό παραβιάσεων ασφάλειας προκαλείται από τους ανθρώπους και τις ελλιπείς διαδικασίες. Είναι σημαντικό να αξιολογείται το προσωπικό, οι διαδικασίες και οι φυσικές πτυχές που σχετίζονται με τα θαλάσσια συστήματα και να λαμβάνονται τα κατάλληλα μέτρα.

Κεφάλαιο 2.5: Κανονιστικό Πλαίσιο

Η ταχεία υιοθέτηση νέων τεχνολογιών και η αυξημένη εξάρτηση από δικτυακές δομές, ανοίγει τη δυνατότητα επιθέσεων στον κυβερνοχώρο που θα μπορούσαν να απειλήσουν την οικονομία, την ασφάλεια του πληρώματος, το περιβάλλον ή την εθνική ασφάλεια. Το κυρίαρχο ενδιαφέρον για την ασφάλεια στον κυβερνοχώρο έθεσε την ανάγκη δημιουργίας ενός ρυθμιστικού πλαισίου, ικανού να αντιμετωπίσει τις συνεχώς αυξημένες προκλήσεις στο ναυτιλιακό τομέα. Ο IMO, η Ευρωπαϊκή Ένωση (ΕΕ) και οι πετρελαϊκές εταιρείες έχουν αναγνωρίσει την απειλή και πρότειναν ένα νομοθετικό πλαίσιο για την αντιμετώπιση των περιστατικών ασφάλειας.

2.5.1: IMO (International Maritime Organization)

Ο κυρίαρχος οργανισμός προτυποποίησης για τις ναυτιλιακές επιχειρήσεις είναι ο IMO. Στις 5 Ιουλίου 2017, ο IMO εξέδωσε την οδηγία MCS-FAL.1/Circ.3 “Guidelines on Maritime cyber risk management”, παρέχοντας προτάσεις για την ενίσχυση της ασφάλειας της Ναυτιλιακής Βιομηχανίας απέναντι στις κυβερνό- επιθέσεις [1]. Οι κατευθυντήριες γραμμές αποσκοπούν στην παροχή συστάσεων υψηλού

επιπέδου και λειτουργικών στοιχείων που μπορούν να ενσωματωθούν στις υφιστάμενες διαδικασίες διαχείρισης κινδύνων για την αποτελεσματική διαχείριση της ασφάλειας στη Ναυτιλιακή Βιομηχανία. Σύμφωνα με τον IMO, η διαχείριση του κινδύνου είναι θεμελιώδης προκειμένου να προστατευθεί η ναυτιλία από τις τρέχουσες και αναδυόμενες απειλές και τα τρωτά σημεία που προκαλούνται από τη "Ψηφιοποίηση, ολοκλήρωση και αυτοματοποίηση διαδικασιών και συστημάτων στη ναυτιλία". Οι κατευθυντήριες γραμμές υπενθυμίζουν ότι, ενώ οι νέες τεχνολογίες και τα ICT συστήματα παρέχουν αποτελεσματικότητα, συγχρόνως προσθέτουν και κινδύνους σε κρίσιμα συστήματα και διαδικασίες. Οι οδηγίες ορίζουν ως απειλή τόσο τις κακόβουλες ενέργειες που έχουν στόχο να πλήξουν τον οργανισμό, όσο και τις ακούσιες ενέργειες (πχ. συντήρηση λογισμικού) που υπάρχει πιθανότητα να επηρεάσουν τη λειτουργία του οργανισμού. Αυτές οι ενέργειες μπορούν να εκθέσουν ή να εκμεταλλευτούν μια ευπάθεια στα IT / OT συστήματα, η οποία μπορεί να οφείλεται π.χ. σε ατελή σχεδιασμό ή ενσωμάτωση συστημάτων. Προκειμένου ο οργανισμός να καταστεί ικανός να επιτύχει αυτόν τον στόχο, οι Οδηγίες παρουσιάζουν πέντε ενότητες, επισημαίνοντας ότι οι ενότητες αυτές δεν είναι διαδοχικές αλλά συνεχείς και ταυτόχρονες, υποστηρίζοντας την αποτελεσματική διαχείριση του κυβερνοχώρου:

- Αναγνώριση: Ο προσδιορισμός των ρόλων και των ευθυνών του προσωπικού, ή ακόμα και ο προσδιορισμός ενδεχόμενων κινδύνων σε πλοία, περιουσιακά στοιχεία και δεδομένα
- Προστασία: Εφαρμογή διαδικασιών και μέτρων ελέγχου κινδύνων. Σχεδιασμός σχεδίων κατά των επιθέσεων στον κυβερνοχώρο
- Ανίχνευση: Ανάπτυξη και υλοποίηση δραστηριοτήτων και σχεδίων για την ανθεκτικότητα και την αποκατάσταση των συστημάτων που διαταράσσονται από κυβερνό- επιθέσεις
- Επαναφορά: Προσδιορισμός των μέτρων υποστήριξης και αποκατάστασης των συστημάτων που πλήττονται από κυβερνό- επιθέσεις

Με τη διαχείριση του κινδύνου, ο οργανισμός ορίζει τη διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης και επικοινωνίας ενός κινδύνου που συνδέεται με την ασφάλεια και την αποδοχή, αποφυγή, μεταβίβαση του σε αποδεκτό επίπεδο λαμβάνοντας υπόψη το κόστος και τα οφέλη των ενεργειών που αναλαμβάνονται. Ο IMO τροποποίησε δύο από τους γενικούς κώδικες διαχείρισης ασφαλείας προκειμένου να συμπεριλάβει ρητά την ασφάλεια στον κυβερνοχώρο. Οι ISPS και ISM περιγράφουν τον τρόπο με τον οποίο οι λιμενικοί και οι διαχειριστές των πλοίων θα πρέπει να αναπτύσσουν διαδικασίες διαχείρισης κινδύνων. Θεωρώντας τον κίνδυνο ως μέρος των υφισταμένων συστημάτων διαχείρισης της ασφάλειας, η επιτροπή αύξησε την ευαισθητοποίηση μεταξύ της ναυτιλιακής κοινότητας και ανάγκασε τη Βιομηχανία να ασχοληθεί με τους κινδύνους αυτούς. Σύμφωνα με τον κανονισμό, οι Κυβερνήσεις ενθαρρύνονται να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται κατάλληλα στα υπάρχοντα συστήματα διαχείρισης της ασφάλειας, όχι αργότερα από τον ετήσιο έλεγχο συμμόρφωσης την 1η Ιανουαρίου 2021. Μία πιθανή παραβίαση των συστημάτων μπορεί να προκαλέσει λειτουργικές αστοχίες ή αστοχίες ασφαλείας με επικίνδυνες συνέπειες. Στο τέλος των κατευθυντήριων γραμμών, αναφέρονται διάφορες βέλτιστες πρακτικές για την εφαρμογή της διαχείρισης του κινδύνου. Σύμφωνα με τον IMO αυτές είναι οι:

- "The Guidelines on Cyber Security Onboard Ships" (2017) της BIMCO
- ISO/ IEC 27001:2013 (2013)

- NIST Framework (2017)

2.5.2: TMSA

Την 1η Ιανουαρίου 2018, η ένωση των δεξαμενόπλοιων του διεθνούς πετρελαϊκού ναυτιλιακού οργανισμού (OCIMF) έθεσε σε ισχύ την τρίτη έκδοση του κανονισμού TMSA (Tanker Management and Self Assessment) [22]. Το TMSA παρέχει στις εταιρείες ένα μέσο βελτίωσης και μέτρησης των δικών συστημάτων διαχείρισης της ασφάλειας. Μια από τις σημαντικές αλλαγές της τρίτης έκδοσης του TMSA είναι η προσθήκη του 13ου στοιχείου απόδοσης το οποίο επικεντρώνεται στη θαλάσσια ασφάλεια. Αυτό το νέο στοιχείο θα απαιτήσει, από τα μέλη του OCIMF που έχουν εγγραφεί στο πρόγραμμα επιθεώρησης εκθέσεων πλοίων (Ship Inspection Reporting Programe - SIRE), την ενσωμάτωση των πολιτικών ασφάλειας στον κυβερνοχώρο και των διαδικασιών των επιχειρησιακών λειτουργιών μεταξύ της εταιρείας και του πλοίου. Για να είμαστε πιο συγκεκριμένοι, οι διαχειριστές των πλοίων θα υποχρεούνται να διαθέτουν:

- Διαδικασίες διαχείρισης λογισμικού
- Καθοδήγηση σχετικά με τον τρόπο εντοπισμού και αποφυγής των απειλών στον κυβερνοχώρο
- Διαθεσιμότητα των τελευταίων οδηγιών για την ασφάλεια στον κυβερνοχώρο από τη βιομηχανία όσο και τους νηογνώμονες
- Διαδικασίες Διαχείρισης κωδικών πρόσβασης
- Σχέδιο για την ασφάλεια πληροφοριών, το οποίο έχει γνωστοποιηθεί όχι μόνο στους υπαλλήλους στο γραφείο αλλά και στα πλοία

Ενώ ο Διεθνής Ναυτιλιακός Οργανισμός (IMO), μέσω της 98^{ης} συνεδρίασης της Επιτροπής για την Ασφάλεια στη Θάλασσα τον Ιούνιο του 2017, ενέκρινε το ψήφισμα MSC.428 (98) το οποίο επιτρέπει στους ιδιοκτήτες και τους διαχειριστές πλοίων έως την 1η Ιανουαρίου 2021 την ενσωμάτωση του συστήματος διαχείρισης κινδύνου για τον κυβερνοχώρο σύμφωνα με τον Διεθνή Κώδικα Διαχείρισης Ασφάλειας (ISM), ο OCIMF κατέληξε στο συμπέρασμα ότι απαιτείται πιο άμεση δράση μέσω της συμμόρφωσης με τις απαιτήσεις του TMSA 3 για την κυβερνό- ασφάλεια.

2.5.3: Νηογνώμονες

Σε αυτό το κεφάλαιο εισάγονται οι προσεγγίσεις ασφάλειας των επιλεγμένων νηογνωμόνων: Lloyd's Register, DNV GL και ABS (American Bureau of Shipping)

2.5.3.1: Lloyd’s Register (LR)

Η προσέγγιση του Lloyd’s “Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping” (2016) [10] για τη διασφάλιση της ασφάλειας του σύγχρονου δικτυοκεντρικού πλοίου αρχίζει με τον ορισμό του κυβερνοχώρου. Η δημοσίευση, που αναφέρεται ως "Οδηγός", απαριθμεί έξι βασικούς τομείς κινδύνου που πρέπει να ληφθούν υπόψη και να αντιμετωπιστούν κατά την εξασφάλιση της ασφάλειας της αξιοπιστίας ενός πλοίου:

- Σύστημα

- Άνθρωπος – Σύστημα
- Λογισμικό
- Δίκτυα και Επικοινωνίες
- Διασφάλιση Δεδομένων
- Ασφάλεια

Ο LR προτείνει μια διαδικασία ανάλυσης κινδύνου κάνοντας αναφορές στα πρότυπα ISO / IEC. Επίσης εισάγει τους δικούς του κανόνες για τη διακυβέρνηση και την ασφάλεια των ICT συστημάτων. Σύμφωνα με τις οδηγίες του LR, μία από τις σημαντικότερες διαδικασίες είναι ο εντοπισμός των συστημάτων που είναι κρίσιμα για την ασφάλεια και την αξιοπλοΐα των πλοίων. Για να γίνει αυτό μπορεί να χρησιμοποιηθεί μία προσέγγιση ανάλυσης κινδύνου όπως είναι η πρόταση του LR: "Assessment of Risk Based Design" (ARBD), είτε η πρόταση του NIST. Οι οδηγίες του LR υπενθυμίζουν ότι η απομακρυσμένη σύνδεση με τα συστήματα στην ξηρά δημιουργεί ένα επιπλέον επίπεδο πολυπλοκότητας, κινδύνου και επιπλέον ερωτήσεις (όπως: Είναι τα συστήματα στη στεριά ενημερωμένα και προστατευμένα σε ένα αποδεκτό επίπεδο), οι οποίες πρέπει να απαντηθούν κατά τη διάρκεια ανάλυσης του κινδύνου. Οι οδηγίες του LR αναφέρουν ότι η βοήθεια ή η αντικατάσταση των καθηκόντων που εκτελούν τα πληρώματα στο πλοίο, τα οποία οι ΤΠΕ καθιστούν δυνατό, μπορεί να προσφέρει οφέλη. Ωστόσο για να επιτευχθεί αυτό, πρέπει να αντιμετωπιστούν διάφορα ζητήματα επικοινωνίας ανθρώπου - συστήματος που προκύπτουν από τη χρήση των ΤΠΕ. Ο επιτυχημένος σχεδιασμός λαμβάνει υπόψη τις μεταβαλλόμενες προσδοκίες που απευθύνονται στους χρήστες για τη λειτουργία και την αποτυχία διάγνωσης των συστημάτων, τον επανασχεδιασμό των καθηκόντων των ναυτικών και του προσωπικού στη στεριά, τον αντίκτυπο των αλλαγών στην ασφαλή και αποτελεσματική απόδοση του προσωπικού και την ανάγκη παρακολούθησης των εργασιών του πλοίου. Ο LR προτείνει μία δομημένη, ανθρωποκεντρική προσέγγιση χρησιμοποιώντας ως αναφορά τις προτάσεις του ISO 9241-210 "Human- Centred Design (HCD) for Interactive Systems standard" (2010). Όσον αφορά τα δίκτυα και τις επικοινωνίες ο LR σημειώνει ότι οι προμηθευτές θα πρέπει να παρέχουν ασφαλή συστήματα στους διαχειριστές. Ωστόσο τα συστήματα αυτά συχνά δε δοκιμάζονται ολοκληρωμένα στο περιβάλλον για το οποίο έχουν κατασκευασθεί να λειτουργούν. Για το λόγο αυτό πρέπει να διασφαλιστεί ότι τα στοιχεία του δικτύου πληρούν τα κατάλληλα πρότυπα και υπάρχουν διαθέσιμα ανταλλακτικά στα πλοία για όλα τα κρίσιμης σημασίας συστήματα (ECDIS, GMDSS, LOADICATOR, AMS). Επίσης, ο LR τονίζει την αυξανόμενη σημασία της συντήρησης λογισμικού (Software Maintenance - SW) των συστημάτων. Κατά τον LR, η δημιουργία και η συντήρηση του λογισμικού θα πρέπει να ικανοποιούν τις απαιτήσεις ενός διεθνώς αναγνωρισμένου προτύπου (π.χ. IEC 61508:2010 (2010),"Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"). Σύμφωνα με τον LR, στόχος είναι η διαχείριση όχι μόνο του κινδύνου που προκαλείται από τα χαρακτηριστικά του λογισμικού αλλά και συνολικά του συστήματος το οποίο λειτουργεί με το συγκεκριμένο λογισμικό [23]. Σύμφωνα με τις οδηγίες είναι ευθύνη του παρόχου να πιστοποιήσει ότι το παραδοτέο προϊόν ικανοποιεί τις βέλτιστες πρακτικές. Επιπροσθέτως, το προϊόν πρέπει να παραδοθεί σύμφωνα με τις κατευθύνσεις του προτύπου ISO 9001:2015 (2015) για τη διαχείριση ποιότητας. Σύμφωνα με τον LR, ένας πολύ σημαντικός παράγοντας που επηρεάζει την ασφάλεια σε μεγάλο βαθμό είναι η δυνατότητα παραμετροποίησης του λογισμικού. Λόγω του υψηλού βαθμού ενσωμάτωσης διαφορετικών συστημάτων, οποιαδήποτε τροποποίηση συμβεί σε ένα μεμονωμένο υπό-

σύστημα, επηρεάζει τη λειτουργία άλλων υπό- συστημάτων και υπάρχει η πιθανότητα να προκαλέσει απώλεια λειτουργίας του συνολικού συστήματος. Τον κίνδυνο αυτό επιχειρούν να ελαχιστοποιήσουν τα πρότυπα ISO 9001 και ISO 10007:2017 (2017), προσπαθώντας να προτείνουν υλοποιήσεις κατάλληλων διαδικασιών παραμετροποίησης. Ο νηογνώμονας επισημαίνει ότι , αν και τα δεδομένα είναι εξαιρετικά ζωτικής σημασίας για κάθε οργανισμό, πολλές επιχειρήσεις δεν είναι σε θέση να χειριστούν τα δεδομένα τους αποτελεσματικά – Ενδεχομένως να μη γνωρίζουν τι δεδομένα κατέχουν, τι χρειάζονται ή ακόμα και την ποιότητα των δεδομένων αυτών. Οι οργανισμοί πρέπει να τηρούν ορισμένα κριτήρια για τη διασφάλιση δεδομένων κατά το σχεδιασμό του συστήματος:

- Ακεραιότητα,
- Διαθεσιμότητα,
- Εμπιστευτικότητα,
- Αυθεντικοποίηση,
- Εξουσιοδότηση και
- Μη αποκήρυξη

Σύμφωνα με τις κατευθυντήριες οδηγίες, υπογραμμίζεται η ανάγκη διασφάλισης των κρίσιμων ναυτιλιακών συστημάτων από τις αυξημένες απειλές στον κυβερνοχώρο, ιδίως επειδή η παγκόσμια οικονομία εξαρτάται όλο και περισσότερο από το ναυτιλιακό εμπόριο. Για το λόγο αυτό, ο ρόλος της εκπαίδευσης και της δημιουργίας εταιρικής κουλτούρας είναι κρίσιμοι για την ανάπτυξη ενός σχεδίου ασφαλείας. Τέλος, ο LR τονίζει ότι η συνδεσιμότητα είναι το στοιχείο που καθιστά το θαλάσσιο περιβάλλον μοναδικό για περιστατικά ασφαλείας.

2.5.3.2: DNV (Det Norsk Veritas)

Αρχικά, ο DNV στις οδηγίες του [2] παρουσιάζει τις κατηγορίες των πιθανών απειλών, οι οποίες θα παρουσιαστούν αναλυτικά στα επόμενα κεφάλαια της εργασίας. Ακολούθως, ο νηογνώμονας παραθέτει τους παράγοντες οι οποίοι, κατά τον DNV, είναι απαραίτητοι για τη βελτίωση του σχεδίου κυβερνό- ασφάλειας του οργανισμού:

- Αξιολόγηση
- Βελτίωση
- Επαλήθευση και Επικύρωση

του σχεδίου [3]. Σύμφωνα με το νηογνώμονα υπάρχουν ομοιότητες μεταξύ της ασφάλειας και των συστημάτων διαχείρισης ποιότητας. Ο κύκλος Plan – Do – Check – Act (PDCA) και η έννοια της συνεχούς βελτίωσης των διαδικασιών και της συμμόρφωσης με τους κώδικες ISM και ISPS είναι κοινοί, κάνοντας αναφορά στα πρότυπα ISO/IEC 27001:2013 (2013) και IEC 62443-3-3:2013 (2013). Ο νηογνώμονας προτείνει 3 διαφορετικές προσεγγίσεις για την αξιολόγηση του κινδύνου:

- Υψηλού Επιπέδου (απευθύνεται στο επίπεδο της Διοίκησης)
- Εστιασμένη και Περιεκτική (αφορά συγκεκριμένα συστήματα και σύνολα δεδομένων)
- Σε βάθος ανάλυση (είναι η συνολική εικόνα ασφάλειας του Οργανισμού)

Τα τέσσερα βήματα της ανάλυσης Υψηλού Επιπέδου είναι:

- Ο καθορισμός των κρίσιμων συστημάτων του οργανισμού
- Εξέταση των συνεπειών μιας επίθεσης (χρησιμοποιώντας το μοντέλο CIA)
- Αξιολόγηση της πιθανότητας μιας επίθεσης
- Απεικόνιση των αποτελεσμάτων των προηγούμενων βημάτων σε ένα πίνακα

Μετά την αξιολόγηση υψηλού επιπέδου, ο οργανισμός έχει μια γενική εικόνα των ευπαθειών και με τη βοήθεια αυτών των αποτελεσμάτων μπορεί να αρχίσει να επικεντρώνεται στους τομείς που απαιτείται αξιολόγηση σε μεγαλύτερη λεπτομέρεια. Η εστιασμένη αξιολόγηση συνίσταται για συστήματα και σύνολα δεδομένων τα οποία τοποθετούνται στο σημείο του πίνακα κινδύνου, στο οποίο δεν γίνεται αποδοχή του κινδύνου.

Τα τέσσερα στάδια της Εστιασμένης μεθόδου είναι:

- Ο εντοπισμός των απειλών στα συστήματα, τα οποία υποστηρίζουν συγκεκριμένες λειτουργίες των πλοίων και επιχειρηματικές διαδικασίες
- Ο εντοπισμός των μέτρων πρόληψης περιστατικών που σχετίζονται με αυτές τις απειλές
- Ο εντοπισμός των μέτρων μείωσης των συνεπειών, σε περίπτωση εμφάνισης αυτών των συμβάντων
- Η αξιολόγηση αυτών των μέτρων πρόληψης και μείωσης των συνεπειών

Το εμπόδιο στην ασφάλεια μπορεί να είναι μια “ενέργεια, συσκευή, διαδικασία ή τεχνική που μειώνει την απειλή, την ευπάθεια ή την επίθεση - εξαλείφοντάς την ή ελαχιστοποιώντας τη βλάβη που μπορεί να προκαλέσει ή εντοπίζοντας την και προειδοποιώντας τον οργανισμό έτσι ώστε να ληφθούν οι απαραίτητες διορθωτικές ενέργειες”. Ο DNV GL προτείνει να χρησιμοποιηθεί η μέθοδος Bow-Tie στην εστιασμένη αξιολόγηση. Η μέθοδος Bow-Tie βοηθάει στην γρήγορη απεικόνιση της ανάγκης για εφαρμογή περισσότερων μέτρων για την ασφάλεια του κυβερνοχώρου, καθώς δεν επικεντρώνεται στην πιθανότητα ή τη συχνότητα της επίθεσης - αντιθέτως αξιολογεί τους κινδύνους, τους ελέγχους και τα αντίμετρα κατά ορισμένων επιθέσεων. Τα διαγράμματα Bow-Tie είναι επίσης ένας αποτελεσματικός τρόπος για να προσδιοριστεί η προσπάθεια που πρέπει να επενδυθεί στον τομέα της ασφάλειας. Τα κύρια μέρη της μεθόδου Bow-Tie είναι:

- Ο κίνδυνος,
- Το κορυφαίο συμβάν,
- Οι απειλές,
- Οι συνέπειες και
- Τα εμπόδια

Η προτεινόμενη μέθοδος παρέχει διάφορες λίστες ερωτήσεων, ενεργειών και κατηγοριών προκειμένου να βοηθήσει στην ταυτοποίηση των απαραίτητων στοιχείων για την ολοκλήρωση της εστιασμένης αξιολόγησης. Η εστιασμένη και σε βάθος αξιολόγηση είναι πιο τεχνικές και ενδέχεται να απαιτήσουν τη βοήθεια εξωτερικών συνεργατών. Χρησιμοποιείται όταν απαιτείται πιο λεπτομερής αξιολόγηση και σχετίζεται με κυρίως με τα κρίσιμα συστήματα και επιχειρηματικές διαδικασίες του οργανισμού.

Τα πέντε βήματα της εμπεριστατωμένης και εις βάθος αξιολόγησης είναι:

- Ο καθορισμός των κρίσιμων IT/ OT συστημάτων του οργανισμού
- Ο προσδιορισμός των συνεπειών επίθεσης σε κάθε ένα από τα παραπάνω συστήματα
- Ο καθορισμός της πρόσβασης σε κάθε ένα από αυτά τα συστήματα
- Η αξιολόγηση των συστημάτων σχετικά με τον κίνδυνο
- Η σύγκριση των υφιστάμενων μέτρων σε σχέση με το σύστημα - στόχο

Ο DNV παρέχει διάφορους καταλόγους ερωτήσεων, ενεργειών και κατηγοριοποιήσεων για να βοηθήσει στην ταυτοποίηση των απαραίτητων στοιχείων για την ολοκλήρωση της συνολικής, σε βάθος αξιολόγησης. Για τα IT συστήματα, ο DNV-GL παρέχει πρακτικές οδηγίες για τον τρόπο με τον οποίο ένας οργανισμός μπορεί να δημιουργήσει λίστες ελέγχου σύμφωνα με το πρότυπο IEC/ISO 27001 (2013) και για τα OT συστήματα σύμφωνα με το IEC 6443-3-3 (2013).

Οι αξιολογήσεις που παρουσιάστηκαν στις προηγούμενες ενότητες βοηθούν τον οργανισμό να βρει τους τομείς βελτίωσής του. Η προτεινόμενη μέθοδος δηλώνει ότι η ανάλυση κόστους- οφέλους είναι υποχρεωτική όταν ορίζουμε την περισσότερο αποτελεσματική στρατηγική απομείωσης των κινδύνων. Αυτό απαιτεί τον προσδιορισμό της συνολικής εικόνας του κινδύνου του οργανισμού και μπορεί να χρησιμοποιηθεί για τη δημιουργία οικονομικών μοντέλων για τη στήριξη της λήψης αποφάσεων για επενδύσεις σε βελτιωτικές ενέργειες. Η μέθοδος Bow- Tie καθώς και ο πίνακας απεικόνισης κινδύνων, που παρουσιάστηκαν παραπάνω, μπορούν να χρησιμοποιηθούν σαν εργαλεία. Όταν είναι επιθυμητή η μείωση του κινδύνου, προτείνονται αντίστοιχοι κατάλογοι ελέγχου και σχέδιο εργασίας που βασίζεται σε αυτά τα εργαλεία. Επειδή η εικόνα κινδύνου αλλάζει διαρκώς, απαιτείται να χρησιμοποιηθούν κύκλοι συνεχούς βελτίωσης, όπως το PDCA, για να διασφαλιστεί ότι οι κατάλογοι ελέγχου και οι διαδικασίες παραμένουν ενημερωμένοι. Μέσω της συνεχούς βελτίωσης, η ωριμότητα και το επίπεδο ανθεκτικότητας του οργανισμού μπορεί να βελτιωθεί. Κατά τον DNV GL οι βελτιώσεις μπορεί να αφορούν τη γενική ευαισθητοποίηση και την κατάρτιση, να έχουν πιο τεχνικό χαρακτήρα ή να σχετίζονται με τη δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών - ΣΔΑΠ (Information Security Management System - ISMS). Η πρόταση του νηογνώμονα υπογραμμίζει τη σημασία του ανθρώπινου παράγοντα στην ασφάλεια του κυβερνοχώρου - για παράδειγμα, η κοινωνική μηχανική και το ηλεκτρονικό ψάρεμα έχουν κοινά χαρακτηριστικά, ωστόσο πρέπει να ληφθεί υπόψη και η εσωτερική απειλή.

Είναι πολύ σημαντικό να καλλιεργηθεί η ευαισθητοποίηση και η ικανότητα του προσωπικού, καθώς οι εργαζόμενοι πολλών οργανισμών δεν είναι σε θέση να αντιδράσουν σωστά σε περίπτωση συμβάντος. Κατά τον DNV-GL θα μπορούσε να αποδειχθεί πολύτιμο εργαλείο, για έναν οργανισμό, η δημιουργία ενός ΣΔΑΠ σύμφωνα με το πρότυπο IEC/ISO 27001 (2013), το οποίο μπορεί να ενσωματωθεί στο κεντρικό σύστημα του οργανισμού. Ενώ η προτεινόμενη οδηγία επικεντρώνεται στις λειτουργικές πτυχές της διαχείρισης της ασφάλειας, το πρότυπο IEC/ISO 27001 προσεγγίζει περισσότερο οργανωτικά το όλο θέμα. Η πρακτική παρέχει μια λίστα των οδηγιών του IEC/ISO 27001 για την πλήρη συμμόρφωση με το πρότυπο και τη δημιουργία ενός αποτελεσματικού ΣΔΑΠ. Το τελικό τμήμα των οδηγιών του DNV GL παρουσιάζει διάφορες προσεγγίσεις για την επικύρωση και επαλήθευση μετά την ολοκλήρωση των

ενεργειών αξιολόγησης και βελτίωσης, εισάγοντας την παρακολούθηση και τον έλεγχο των τεχνικών μέτρων.

2.5.3.3: American Bureau of Shipping (ABS)

Ο ABS ήταν ο πρώτος νηογνώμονας ο οποίος δημοσίευσε ένα πρόγραμμα διαχείρισης κινδύνου. Η σειρά "CyberSafety" του ABS, παρουσιάζει τις βέλτιστες πρακτικές για την ασφάλεια σε τέσσερις βασικές περιοχές θαλάσσιων και υπεράκτιων οργανισμών [24]. Το πρόγραμμα αποτελείται από μια οικογένεια πέντε εγγράφων:

- “Volume 1: Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations”
- “Volume 2: Guide for Cybersecurity Implementation for the Marine and Offshore Industries”
- “Volume 3: Guidance Notes on Data Integrity for Marine and Offshore Operations”
- “Volume 4: Guide for Software Systems Verification”
- “Volume 5: Guidance Notes on Software Provider Conformity Program”

Η διατριβή αυτή επικεντρώνεται στους πρώτους δύο τόμους της σειράς, ώστε να δοθεί στον αναγνώστη μια καλή επισκόπηση του προγράμματος, καθώς τα τρία τελευταία έγγραφα της σειράς επικεντρώνονται στην παροχή λεπτομερούς τεχνικής κατεύθυνσης για την εφαρμογή εμπεριστατωμένης ασφάλειας στον κυβερνοχώρο.

Ο τόμος 1 της σειράς ABS CyberSafety περιγράφει τον τρόπο με τον οποίο η αυξανόμενη εξάρτηση από το λογισμικό, την αυτοματοποίηση και την ενοποίηση των συστημάτων της ναυτιλιακής βιομηχανίας καθιστά την εύρυθμη διαχείριση της ασφάλειας και της ακεραιότητας του λογισμικού ολοένα και πιο σημαντική. Το πρόγραμμα κυβερνό- ασφάλειας απαντά σε αυτές τις ανάγκες παρουσιάζοντας ένα μοντέλο δυνατοτήτων που βοηθά τον οργανισμό να βελτιώσει το επίπεδο ασφαλείας όχι μόνο στα OT συστήματα αλλά και στα συνδεδεμένα επιχειρηματικά συστήματα. Η ιδέα του προγράμματος είναι η σταδιακή βελτίωση των παραπάνω δυνατοτήτων “με βάση τις ανάγκες ασφάλειας, τις ικανότητες του προσωπικού, τους διαθέσιμους πόρους και την οργανωτική ωριμότητα στην κυβερνό- ασφάλεια του οργανισμού” [25]. Το μοντέλο του ABS CyberSafety στον 1^{ο} τόμο παρουσιάζει τρία σύνολα δυνατοτήτων:

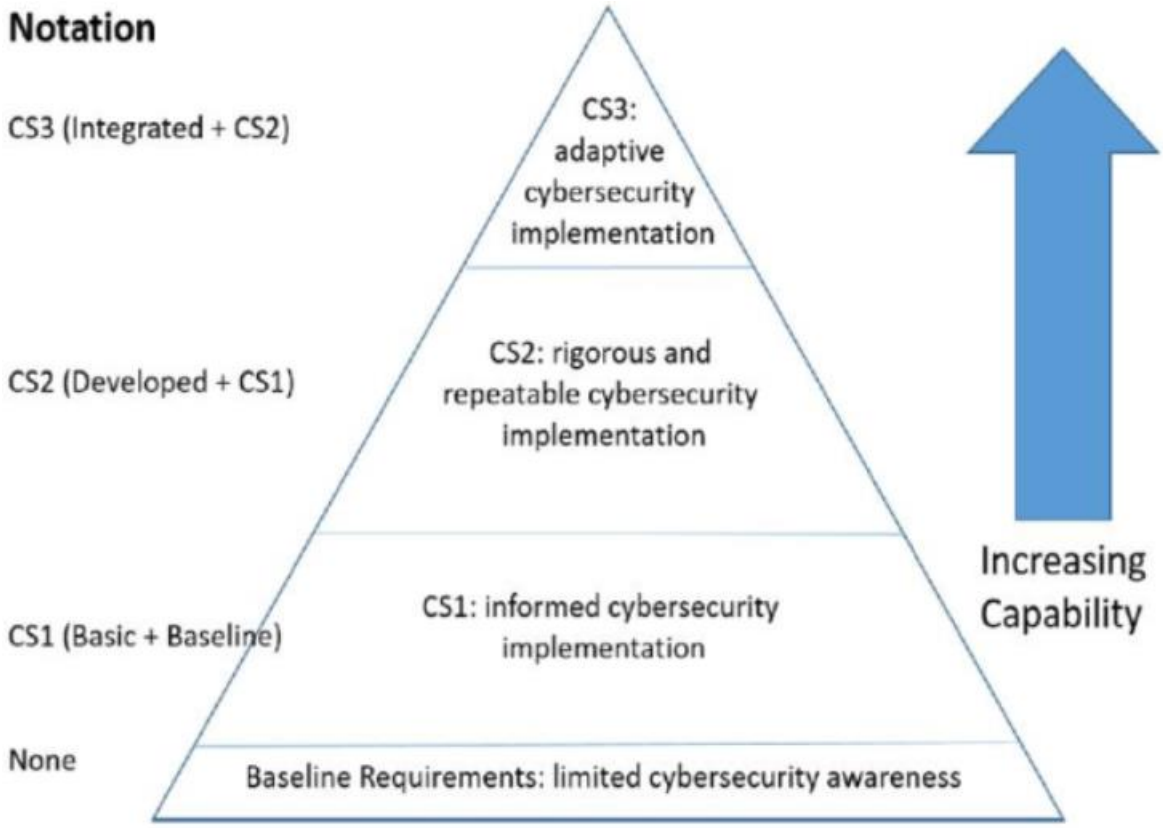
- Βασικές δυνατότητες,
- Ανεπτυγμένες δυνατότητες και
- Ολοκληρωμένες δυνατότητες

Παρουσιάζονται συνολικά 37 δυνατότητες, οι οποίες χρησιμεύουν ως κύρια στοιχεία της κυβερνό-ασφάλειας του οργανισμού και η εφαρμογή τους μπορεί να προτεραιοποιηθεί με μετρήσιμο τρόπο. Το παράρτημα Α παρουσιάζει το μοντέλο πλήρους ικανότητας, στο οποίο οι πρώτες εννέα δυνατότητες αποτελούν το βασικό σύνολο δυνατοτήτων, οι δυνατότητες από 10 έως 23 παρουσιάζουν το σύνολο αναπτυγμένων δυνατοτήτων και τις τελικές δυνατότητες από 24 σε 37 το ολοκληρωμένο σύνολο δυνατοτήτων. Στις επόμενες παραγράφου του 1^{ου} τόμου του εγγράφου, εισάγονται οι βέλτιστες

πρακτικές για καθεμία από τις δυνατότητες. Οι προτεινόμενες βέλτιστες πρακτικές αποτελούν γνώση η οποία έχει αποκτηθεί από διαφορετικές πηγές, συμπεριλαμβανομένων των διαφόρων βιομηχανιών, κυβερνητικών εκθέσεων και προτάσεων ακαδημαϊκών οργανισμών. Για κάθε βέλτιστη πρακτική, παρέχεται κατάλογος αναφορών για την περαιτέρω κατανόηση. Ο δεύτερος τόμος του ABS CyberSafety ακολουθεί τον τόμο 1 παρέχοντας προδιαγραφές για την εφαρμογή των παραπάνω δυνατοτήτων. Στόχος είναι η δημιουργία ενός κύκλου αξιολόγησης ικανοτήτων-εργασίας και η ανάπτυξη ενός συστήματος διαχείρισης κινδύνου για τα περιουσιακά στοιχεία του οργανισμού. Ο τόμος 2 παρέχει κριτήρια για την αξιολόγηση των εταιρικών συστημάτων και των περιουσιακών στοιχείων καθώς και την ετοιμότητα του οργανισμού για την αποτροπή συμβάντων στον κυβερνοχώρο, για την ασφάλεια των δεδομένων, των συστημάτων και των περιουσιακών στοιχείων. Στον τόμο 2, υπάρχει μια προαιρετική σημειογραφία "CS – Class Series Notation" (CS1, CS2 και CS3), η οποία έχει ως στόχο να βοηθήσει τον οργανισμό να υποδείξει την ετοιμότητά του σε θέματα κυβερνό- ασφάλειας. Η κατηγοριοποίηση βασίζεται στις απαιτήσεις που παρουσιάζονται στο έγγραφο και είναι κατάλληλη για όλα τα σκάφη που συμμορφώνονται με τον ISM. Ένας οργανισμός που συμμορφώνεται με τις διαδικασίες και τα κριτήρια που ορίζονται στον τόμο 2 μπορεί να λάβει ένα πιστοποιητικό συστήματος διαχείρισης ασφάλειας (CyberSafety Management System Certificate - CMSC) και πιστοποίηση C1, C2 ή C3 (Σε περίπτωση που το πλοίο είναι εγγεγραμμένο στον ABS) ή σε διαφορετική περίπτωση ένα Πιστοποιητικό Συμμόρφωσης (Certificate of Cyber Compliance - CCC) [26].

Το παρακάτω σχήμα παρουσιάζει τα επίπεδα ασφάλειας σύμφωνα με την προσέγγιση του ABS. Τα επίπεδα βασίζονται στις υλοποιημένες δυνατότητες. Αυτό σημαίνει, ότι μόνο βελτιώνοντας τις ικανότητες θα έχει τη δυνατότητα ο οργανισμός να μετακινηθεί προς το υψηλότερο επίπεδο της ιεραρχίας. Το επίπεδο στο οποίο κατατάσσεται ο οργανισμός περιγράφει επίσης και το επίπεδο ωριμότητας του σε σχέση με την ασφάλεια. Τα διάφορα επίπεδα συνδέονται με τα αντίστοιχα σύνολα δυνατοτήτων που παρουσιάζονται στον τόμο 1 του προγράμματος. Κατά την εφαρμογή του βασικού συνόλου δυνατοτήτων, ο οργανισμός μπορεί να φθάσει στο επίπεδο CS1. Από το σύνολο αναπτυγμένων δυνατοτήτων μπορεί να επιτευχθεί το επίπεδο CS2 και από το ολοκληρωμένο σύνολο δυνατοτήτων, το υψηλότερο επίπεδο C3 [27].

Ακολουθώντας την ανάλυση της ιεραρχίας, ο δεύτερος τόμος παρέχει μια πιο αναλυτική περιγραφή των απαιτήσεων κάθε επιπέδου, καθώς και μια επισκόπηση των ικανοτήτων. Η προτεινόμενη προσέγγιση εστιάζει κυρίως στον πίνακα δυνατοτήτων, ο οποίος καθορίζει τις βέλτιστες πρακτικές, ορίζει και παρέχει "Τα χαρακτηριστικά των εταιρικών διαδικασιών για κάθε ικανότητα σε συνδυασμό με τα χαρακτηριστικά των IT και OT συστημάτων" [28].



Εικόνα 2: ABS Cyber Safety Notation

Το παράρτημα β παρουσιάζει ένα παράδειγμα του τρόπου με τον οποίο η πρώτη δυνατότητα που αφορά τις βέλτιστες πρακτικές του βασικού συνόλου δυνατοτήτων εμφανίζεται στον πίνακα δυνατοτήτων, τις προδιαγραφές και τις απαιτήσεις που σχετίζονται με αυτήν τη δυνατότητα. Στο τέλος του δεύτερου εγγράφου, δηλώνεται ότι αν ένας οργανισμός επιθυμεί να αποκτήσει το πιστοποιητικό Κυβερνό- ασφάλειας που εκδίδει ο ABS, πρέπει να καθιερώσει ένα σύστημα διαχείρισης ασφάλειας στον κυβερνοχώρο (Cyber Security Management System- CMS), με σκοπό την εφαρμογή και παρακολούθηση της στρατηγικής και του σχεδίου ασφάλειας του οργανισμού. Κατά τον ABS, το CMS είναι το πλαίσιο για τη διαχείριση ικανοτήτων και παρακολούθησης, καθώς και το κλειδί για την ανάπτυξη των δυνατοτήτων του οργανισμού στα επιθυμητά επίπεδα ώστε να υποστηριχθεί η επιχειρησιακή κατανόηση των μέτρων ασφαλείας, η συμμόρφωση με τις απαιτήσεις και η θέσπιση της συνεχούς παρακολούθησης της ασφάλειας του οργανισμού. Ο δεύτερος τόμος παρουσιάζει μια λίστα με τις απαιτήσεις που έχουν οριστεί για το CMS, ώστε να είναι σε θέση ο οργανισμός να σχεδιάσει, να εφαρμόσει και λειτουργήσει ένα τέτοιο σύστημα.

2.5.4: Baltic and International Maritime Council (BIMCO)

Η BIMCO έχει εκδώσει την οδηγία “The Guidelines on Cyber Security Onboard Ships” (2017), ενσωματώνοντας τις οδηγίες του IMO σχετικά με την Διαχείριση της Ασφάλειας. Σύμφωνα με την

BIMCO κατά την ανάπτυξη των οδηγιών, χρησιμοποιήθηκε το πλαίσιο του NIST. Κατά την άποψη του Συμβουλίου παρόλο που η προσέγγιση της ασφάλειας είναι διαφορετική για το γραφείο και το πλοίο, θα πρέπει να ακολουθούνται τα "κατάλληλα πρότυπα και απαιτήσεις των εθνικών κανονισμών" [30]. Μια άλλη πτυχή την οποία υπογραμμίζει η BIMCO στις κατευθυντήριες οδηγίες της είναι ότι τα σχέδια και οι διαδικασίες διαχείρισης της ασφάλειας του οργανισμού πρέπει να είναι συμπληρωματικά προς τα υφιστάμενα φυσικής ασφάλειας που παρουσιάζονται σε άλλα συστήματα και κώδικες που ακολουθούνται, όπως είναι:

- Ο Διεθνής Κώδικας Διαχείρισης για την Ασφαλή Λειτουργία των Πλοίων και την πρόληψη της ρύπανσης (ISM),
- Ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (International Ship and Port Facility Security - ISPS)
- Το Σύστημα Διαχείρισης Ασφάλειας (Safety Management System - SMS)

Το παρακάτω σχήμα παρουσιάζει την προσέγγιση της BIMCO σχετικά με την ασφάλεια. Οι έξι βασικές έννοιες της αποτελεσματικής διαχείρισης του κινδύνου στον κυβερνοχώρο είναι:

1. Η αναγνώριση των απειλών
2. Η αναγνώριση των ευπαθειών
3. Η αξιολόγηση του κινδύνου
4. Η ανάπτυξη μέτρων ανίχνευσης και προστασίας
5. Η κατάρτιση σχεδίων έκτακτης ανάγκης
6. Η ανταπόκριση και ανάκαμψη από περιστατικά στον κυβερνοχώρο

Εικόνα 3: BIMCO

Θέματα σχετικά με τον εντοπισμό απειλών και τρωτών σημείων παρουσιάστηκαν στο κεφάλαιο 1.3.1 της εργασίας. Για το θέμα της εκτίμησης της έκθεσης σε κινδύνους, οι Κατευθυντήριες Γραμμές της BIMCO υποδεικνύουν ότι η λογοδοσία και η κυριότητα για την αξιολόγηση ξεκινά από το ανώτερο επίπεδο διοίκησης του οργανισμού:

- Δεδομένου ότι η βελτίωση της ασφάλειας του κυβερνοχώρου μπορεί να αποδώσει επιχειρηματικές διαδικασίες περισσότερο χρονοβόρες ή δαπανηρές , το ανώτερο επίπεδο διοίκησης πρέπει να αξιολογεί και να αποφασίζει συγκρίνοντας τον κίνδυνο με τα παραπάνω μειονεκτήματα

- Η βελτίωση της ασφάλειας μπορεί να σχετίζεται περισσότερο με τις επιχειρησιακές διαδικασίες και την κατάρτιση του προσωπικού παρά με τα συστήματα πληροφορικής και για το λόγο αυτό πρέπει να αντιμετωπίζεται σε επίπεδο οργανισμού
- Το ανώτερο επίπεδο διοίκησης πρέπει να αποφασίσει εάν και πώς θα τροποποιηθούν οι σχέσεις του οργανισμού με τους πελάτες, τους προμηθευτές και τις αρχές, σε περίπτωση που η βελτίωση της ασφάλειας στον κυβερνοχώρο απαιτεί νέο είδος συνεργασίας μεταξύ των μερών
- Όταν οι τρεις προηγούμενες πτυχές γίνουν κατανοητές, θα είναι δυνατόν να οριστούν οι απαιτήσεις πληροφορικής σχετικά με την ασφάλεια, οι οποίες μπορούν να γίνουν από το τμήμα πληροφορικής
- Οι γενικές στρατηγικές αποφάσεις και ο κίνδυνος έναντι των trade-off καθοδηγούν την εκπόνηση σχεδίων έκτακτης ανάγκης για ενδεχόμενα περιστατικά στον κυβερνοχώρο

Οι κατευθυντήριες γραμμές υπενθυμίζουν ότι πρέπει να λαμβάνονται υπ' όψιν τα χαρακτηριστικά της ναυτιλιακής βιομηχανίας (αναφέρθηκαν σε προηγούμενο κεφάλαιο της εργασίας) κατά την εκτίμηση του κινδύνου. Η BIMCO προτείνει δύο προσεγγίσεις για την αξιολόγηση του κινδύνου

1. Τις αξιολογήσεις του οργανισμού και
2. Τις αξιολογήσεις τρίτων εταιριών

Η διαδικασία εκτίμησης κινδύνου που διενεργείται από τον οργανισμό πρέπει να ξεκινήσει με την αξιολόγηση των συστημάτων στο πλοίο, με στόχο την όσο το δυνατό περισσότερο αποδοτική διαχείριση των απειλών. Κατά την BIMCO πρέπει να προσδιοριστούν:

- Οι υφιστάμενοι τεχνικοί και διαδικαστικοί έλεγχοι που προστατεύουν τα IT και OT συστήματα,
- Τα συστήματα (IT και OT) που είναι ευάλωτα καθώς και τις ευπάθειες,
- Οι ευπαθείς λειτουργίες του πλοίου ,
- Πιθανά περιστατικά στον κυβερνοχώρο και ο αντίκτυπός τους στις βασικές λειτουργίες του πλοίου,
- Η πιθανότητα εμφάνισης των παραπάνω περιστατικών

Ο οργανισμός μπορεί να συνεργαστεί με τους κατασκευαστές του εξοπλισμού και των συστημάτων προκειμένου να ενημερωθεί για τους τεχνικούς ελέγχους και τις διαδικασίες που έχουν εφαρμοστεί και σχετίζονται με την ασφάλεια.

Οι αξιολογήσεις κινδύνου από τρίτες εταιρίες, συμπληρώνουν τις εσωτερικές αξιολογήσεις και βοηθούν στον εντοπισμό των κενών και των κινδύνων που δεν εντοπίστηκαν κατά τη διαδικασία του εσωτερικού ελέγχου. Προκειμένου να διαπιστωθεί εάν το επίπεδο άμυνας του οργανισμού συμφωνεί με αυτό που ορίζεται στη στρατηγική του οργανισμού, μπορούν να πραγματοποιηθούν δοκιμαστικές επιθέσεις στα IT και OT συστήματα του οργανισμού. Οι επιθέσεις αυτές, όπως η κοινωνική μηχανική ή η φυσική διείσδυση στην περίμετρο ασφαλείας της εγκατάστασης, μπορούν να είναι κατάλληλες για τα IT συστήματα πληροφορικής, ωστόσο τα OT συστήματα μπορεί να είναι αρκετά σημαντικά για την λειτουργίες του οργανισμού ώστε να μην μπορούν να ληφθούν οι σχετικοί κίνδυνοι. Σε αυτές τις περιπτώσεις, θα μπορούσαν να χρησιμοποιηθούν παθητικοί έλεγχοι, όπως τα δεδομένα σάρωσης που

μεταδίδονται από τα συστήματα. Η BIMCO εισάγει μια διαδικασία εκτίμησης κινδύνου τεσσάρων φάσεων, η οποία έχει ως τελικό αποτέλεσμα:

1. Μία έκθεση (περιλαμβανομένης της σύνοψης),
2. Τα τεχνικά ευρήματα,
3. κατάλογο δράσεων και
4. Συμπληρωματικά δεδομένα και παραρτήματα

Μόλις αντιμετωπιστούν τα ευρήματα, μπορεί να χρειαστεί να σταλεί ένα υποσύνολο των ευρημάτων στους κατασκευαστές των επηρεαζόμενων συστημάτων και να πραγματοποιηθεί ανάλυση από εξωτερικούς εμπειρογνώμονες. Το πέμπτο μέρος, αναφέρεται στην ανάπτυξη μέτρων προστασίας και ανίχνευσης. Κατά την BIMCO, ο στόχος και το αποτέλεσμα της στρατηγικής στον κυβερνοχώρο πρέπει να είναι η μείωση του κινδύνου. Περιπτώσεις, όπου δεν έχει ελεγχθεί ποιος έχει πρόσβαση στα συστήματα του πλοίου, όπως στο δεξαμενισμό, χρειάζονται ιδιαίτερη προσοχή. Τα αντίμετρα προστασίας μπορεί να είναι τεχνικά ή και διαδικαστικά, ωστόσο πρέπει να είναι συμβατά με το CIA μοντέλο. Θα πρέπει να εφαρμόζονται οι οικονομικά αποδοτικοί τεχνικοί έλεγχοι και να δίνεται προτεραιότητα σε εκείνους με το μεγαλύτερο όφελος για τον οργανισμό. Οι οδηγίες αναφέρονται στον κατάλογο των Κρίσιμων Ελέγχων Ασφαλείας (Critical Security Controls- CSC) του Κέντρου για την Ασφάλεια στο Διαδίκτυο (Centre for Internet Security- CIS) και συγκέντρωσαν τα πιο συναφή με τα συστήματα που υπάρχουν στα πλοία:

- Limitation to and control of network ports, protocols and services
- Configuration of network devices such as firewalls, routers and switches
- Physical security
- Detection, blocking and alerts
- Satellite and radio communication
- Wireless access control
- Malware detection
- Secure configuration for hardware and software
- Email and web browser protection
- Data recovery capability
- Application software security (patch management)
- Training and awareness
- Access for visitors
- Upgrades and software maintenance
- Anti-virus and anti-malware tool updates
- Remote access
- Use of administrator privileges
- Physical and removable media controls
- Equipment disposal, including data destruction
- Obtaining support from ashore and contingency plans" (The Guidelines on Cyber Security Onboard Ships 2017, p. 25-34).

Στο τελευταίο μέρος του εγγράφου η κατάρτιση σχεδίων έκτακτης ανάγκης, η ανταπόκριση και η ανάκτηση από περιστατικά στον κυβερνοχώρο, επισημαίνεται ότι είναι σημαντικό να κατανοηθεί η σημασία κάθε περιστατικού στον κυβερνοχώρο ειδικά για IT και τα OT. Οι οδηγίες υπενθυμίζουν ότι τα σχέδια έκτακτης ανάγκης για τα περιστατικά πρέπει να δημιουργηθούν σύμφωνα με τις κατάλληλες διαδικασίες λειτουργίας και έκτακτης ανάγκης που περιλαμβάνονται στο SMS. Συνήθως περιλαμβάνει διαδικασίες για την αναφορά ατυχημάτων ή επικίνδυνων καταστάσεων, καθώς και τα διάφορα επίπεδα επικοινωνίας και λήψης αποφάσεων μέσα στον οργανισμό. Αυτές οι διαδικασίες μπορούν να τροποποιηθούν για να ταιριάζουν στις καταστάσεις που δημιουργούνται από τα περιστατικά ασφαλείας.

Τα σχέδια έκτακτης ανάγκης πρέπει να είναι διαθέσιμα σε μη ηλεκτρονικό μέσο, για παράδειγμα, στην περίπτωση που υπάρξει συμβάν με καταστροφή δεδομένων. Σε ιδιαίτερα περίπλοκα ή σοβαρά περιστατικά , είναι πιθανό να απαιτηθεί βοήθεια εμπειρογνωμόνων. Στο τέλος των οδηγιών, η BIMCO προτείνει να χρησιμοποιηθούν πληροφορίες από τα περιστατικά που έχουν αντιμετωπιστεί για τη βελτίωση του σχεδίου ανταπόκρισης. Για να επιτευχθεί μια αποτελεσματική αντιμετώπιση σε ένα περιστατικό, θα πρέπει να έχει δημιουργηθεί μια ομάδα από το προσωπικό και / ή εξωτερικών συνεργατών που θα εξυπηρετούν τόσο τις εγκαταστάσεις στην ξηρά όσο και τα πλοία για την αποκατάσταση των συστημάτων πληροφορικής και τηλεπικοινωνιών που θα επιτρέπουν την κανονική λειτουργία του σκάφους

Κεφάλαιο 3: Αναγνώριση Απειλών

Για να αναγνωριστούν οι απειλές για την ασφάλεια του οργανισμού, είναι απαραίτητο να γίνουν κατανοητά τα κίνητρα του επιτιθέμενου. Δεδομένου ότι το μεγαλύτερο κίνητρο για το έγκλημα είναι το κέρδος, μια κορυφαία βιομηχανία όπως η ναυτιλία, δεν θα μπορούσε να παραμείνει αλώβητη. Οι περισσότερες από τις επιθέσεις στη ναυτιλιακή βιομηχανία έχουν ως κίνητρο οικονομικά οφέλη ή τη βιομηχανική κατασκοπεία, όπως η υπονόμευση και η διατάραξη των δραστηριοτήτων του πλοίου [2]. Η βιομηχανία αντιμετωπίζει μια συνεχή εμφάνιση νέων απειλών. Το τελευταίο έτος πολλοί οργανισμοί υπήρξαν θύματα από ιούς τύπου Ransomware. Το Ransomware είναι μια μορφή κακόβουλου λογισμικού που κρυπτογραφεί αρχεία και προκαλεί άρνηση πρόσβασης στα δεδομένα του οργανισμού. Οι ενορχηστρωμένες επιθέσεις σε βιομηχανικά συστήματα ελέγχου έχουν επίσης αυξηθεί σε μεγάλο βαθμό.

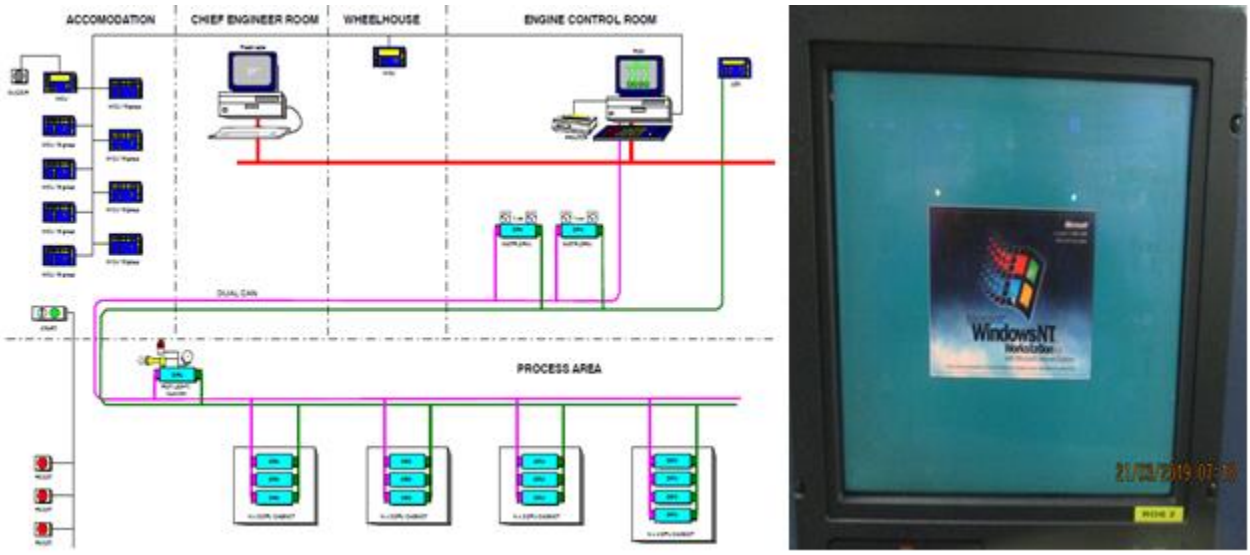
Κεφάλαιο 3.1: Υποδομή στην ξηρά

Μετά το περιστατικό της Maersk το 2017 [30] όταν η επίθεση NotPetya μόλυνε τα IT συστήματα της εταιρείας, επιβάλλοντας το κλείσιμο όλων των συσκευών και το χειροκίνητο χειρισμό όλων των λειτουργιών, οι οργανισμοί συνειδητοποίησαν ότι η ναυτιλιακή βιομηχανία δεν έχει ανοσία απέναντι στο κυβερνό- έγκλημα. Μια επίθεση σε ένα απροστάτευτο δίκτυο θα μπορούσε να προκαλέσει σύγχυση και πολλές ημέρες καθυστέρησης λόγω υπολειτουργικότητας των συστημάτων. Οι δυσαρεστημένοι ναυλωτές, οι καθυστερήσεις στην παράδοση φορτίου, η απώλεια χρημάτων και η δυσφήμηση είναι μόνο μερικά από τα αποτελέσματα που μπορεί να προκαλέσει ένα περιστατικό ασφαλείας. Σήμερα, οι ναυτιλιακές εταιρείες πραγματοποιούν μεγάλο αριθμό συναλλαγών

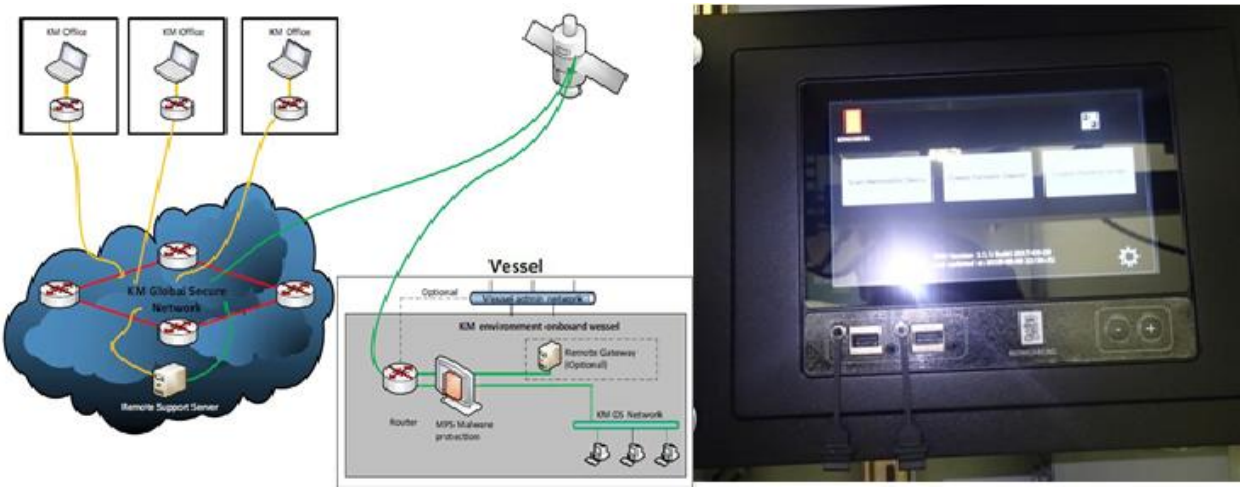
προσελκύοντας πιθανούς εγκληματίες για οικονομικό όφελος. Η αξιοποίηση των συναλλαγών του γραφείου θα μπορούσε να μετατραπεί σε έναν αρκετά εύκολο στόχο για πιθανές επιθέσεις. Με χρήση απλών τεχνικών όπως το ηλεκτρονικό ταχυδρομείο, για παράδειγμα, είναι πιθανή η πρόκληση κλοπής ηλεκτρονικών συναλλαγών.

Κεφάλαιο 3.2: Υποδομή στο πλοίο

Σήμερα, οι κορυφαίοι κατασκευαστές αλλά και οι διαχειριστές πλοίων τείνουν να ενσωματώνουν καινοτομίες χρησιμοποιώντας τα τελευταία συστήματα ΤΠΕ. Στόχος είναι η δημιουργία αποδοτικών πλοίων με βελτιωμένες δυνατότητες παρακολούθησης και επικοινωνίας, που μπορούν να προσεγγιστούν και να ελεγχθούν απομακρυσμένα. Τα συστήματα ΤΠΕ, για παράδειγμα, έχουν τη δυνατότητα να βελτιώσουν την ασφάλεια, την αξιοπιστία και την απόδοση του οργανισμού. Ωστόσο, είναι πολυάριθμοι οι κίνδυνοι που πρέπει να εντοπιστούν, να κατανοηθούν και αντιμετωπιστούν για να διασφαλιστεί ότι οι τεχνολογίες ενσωματώνονται με ασφάλεια στο σχεδιασμό και τις λειτουργίες του πλοίου. Η ναυτιλιακή βιομηχανία αντιμετωπίζει σύνθετες και σοβαρές προκλήσεις όταν επιχειρεί να αξιοποιήσει πλήρως τα οφέλη της χρήσης των ΤΠΕ και η ασφάλεια στον κυβερνοχώρο είναι μία από τις σημαντικότερες.



Εικόνα 4: (LAN (between W/S) - Windows NT- Obsolete W/S PC - No antivirus - Must be protected by internal "attacks")



Εικόνα 5: LAN+ Internet, Windows XP, Malware Protection Server (network traffic scanning, USB scanner) - Exposed to the internet risks

Κεφάλαιο 3.2.1: Διαχωρισμός των Συστημάτων

Η ευρεία υιοθέτηση των ΤΠΕ σε όλα τα σύγχρονα πλοία οδήγησε τους ερευνητές να επικεντρωθούν περισσότερο σε θέματα ασφάλειας. Ένα ερώτημα είναι πώς μία ενδεχόμενη παραβίαση της ασφάλειας στις τεχνολογίες του πλοίου θα επηρεάσει τη λειτουργία του πλοίου και τα μέλη του πληρώματος. Στο πλαίσιο των τεχνολογιών που χρησιμοποιούνται για την επεξεργασία και τον έλεγχο των εργασιών ενός πλοίου, οι ερευνητές αναγνώρισαν τη διάκριση μεταξύ των συστημάτων τεχνολογιών πληροφορικής - ΤΠΕ (Information and Communication Technology - ICT) και των επιχειρησιακών τεχνολογιών (Operational Technology - OT). Ενώ τα IT συστήματα είναι υπεύθυνα για τη συλλογή, μεταφορά και επεξεργασία δεδομένων που παρέχουν πληροφορίες στην επιχείρηση, τα OT συστήματα περιλαμβάνουν το χειρισμό, την παρακολούθηση και αυτοματοποίηση των ICT συστημάτων. Σύμφωνα με το λεξιλόγιο πληροφορικής του Gartner, το OT είναι “Το υλικό και το λογισμικό που ανιχνεύει ή προκαλεί αλλαγή μέσω της άμεσης παρακολούθησης ή / και ελέγχου των φυσικών συσκευών, διαδικασιών και συμβάντων στην επιχείρηση”, ενώ IT σημαίνει “ο κοινός όρος για ολόκληρο το φάσμα των τεχνολογιών- για την επεξεργασία πληροφοριών, συμπεριλαμβανομένου του λογισμικού, του υλικού, των τεχνολογιών επικοινωνιών και των συναφών υπηρεσιών, ενώ δεν περιλαμβάνει ενσωματωμένες τεχνολογίες που δεν δημιουργούν δεδομένα για επιχειρησιακή χρήση” [31]. Τα IT συστήματα έχουν διαφορετικό σκοπό σε σχέση με τα OT συστήματα μέσα στον οργανισμό: τα OT συσχετίζονται περισσότερο με τον φυσικό κόσμο, ενώ τα IT αναφέρονται στην επεξεργασία πληροφοριών. Ειδικότερα στον τομέα της ναυτιλίας:

IT Συστήματα	**OT Συστήματα**
IT Δίκτυα	PLC’s
E-mail	SCADA
Εφαρμογές Γραφείου (Λίστα Πληρωμάτων)	Τηλεμετρία
Εφαρμογές Προγραμματισμένης Συντήρησης	ECDIS
Εφαρμογές Ζήτησης Ανταλλακτικών	GPS
Εγχειρίδια σε ηλεκτρονική μορφή	Απομακρυσμένη Υποστήριξη συστημάτων

	Μηχανής
Ηλεκτρονικά Πιστοποιητικά	Συστήματα Ελέγχου Μηχανής και Φορτιίου
Charter Party, Bill of Lading	Dynamic Positionic

Πίνακας 3: Διαχωρισμός Συστημάτων στο Δίκτυο ενός Πλοίου

Παρόλο που οι απειλές για τις κρίσιμες υποδομές έχουν αναλυθεί, τα ΟΤ συστήματα παραδοσιακά δεν θεωρήθηκαν ως δυνητική απειλή για διάφορους λόγους. Αρχικά, λόγω της ανάγκης για παρακολούθηση σε πραγματικό χρόνο, τα ΟΤ συστήματα δεν μπορούσαν να εξαρτώνται από πρωτόκολλα όπως το Ethernet και ήταν απλά, απομονωμένα δίκτυα σημείου προς σημείο. Ωστόσο, με την πάροδο του χρόνου, λόγω της ανάγκης για ολοκληρωμένο έλεγχο και βελτιστοποιημένη απόδοση, τα επιχειρησιακά δίκτυα έχουν αντικαταστήσει τα ιδιόκτητα εργαλεία επικοινωνίας τα οποία βασίζονται στα πρωτόκολλα Ethernet και Internet (IP), με αποτέλεσμα τον υπερκερασμό της απομόνωσης. Οι επιτιθέμενοι είναι εξοικειωμένοι με το χειρισμό ανοιχτών πρωτοκόλλων καθιστώντας τα δίκτυα του πλοίου περισσότερο ευάλωτα. Ειδικότερα, τα συστήματα IT και ΟΤ είναι ως επί το πλείστων αλληλένδετα, ακόμη και σε περιπτώσεις όπου τα ΟΤ διαχωρίζονται από τα IT δίκτυα, υπάρχουν σημεία πρόσβασης από το ένα δίκτυο στο άλλο καθώς πολλά συστήματα βασίζονται στη χρήση αφαιρούμενων μέσων. IT Ένας από τους περισσότερο διαδεδομένους τρόπους επίθεσης είναι το spear fishing, στο οποίο ένα φαινομενικά ακίνδυνο e-mail περνά μέσα από τα firewall και spam filter που χρησιμοποιεί ο οργανισμός, προκαλώντας τελικά τη λήψη κακόβουλου λογισμικού που μολύνει τα συστήματα του πλοίου.

Κεφάλαιο 3.2.2: Διαφορές μεταξύ IT και ΟΤ συστημάτων

Σε πολλούς οργανισμούς, υπάρχει μια διένεξη στα περιβάλλοντα παραγωγής. Τα ΟΤ συστήματα επικεντρώνονται στην αυτοματοποίηση των μηχανημάτων, των διεργασιών και των συστημάτων μέσα σε ένα οργανισμό, ενώ τα IT εστιάζουν στα συστήματα επιχειρησιακής πληροφόρησης που απαιτούνται για την υποστήριξη του οργανισμού. Ωστόσο, οι επιχειρησιακοί στόχοι δεν είναι η μόνη διαφορά μεταξύ αυτών των δύο κατηγοριών. Οι εργαζόμενοί έχουν διαφορετικούς ρόλους, συχνά αναφέρονται σε διαφορετικά στελέχη, και τα τμήματα έχουν διαφορετικές κουλτούρες. Τα συστήματά συχνά διαχωρίζονται τόσο λογικά όσο και φυσικά και, κυρίως διαφέρει η προσέγγισή τους απέναντι στον κίνδυνο στον κυβερνοχώρο. Όταν γίνεται προσπάθεια να αξιολογηθεί ο κίνδυνος παραβίασης των συστημάτων του οργανισμού, είναι απαραίτητο να καθοριστούν και να κατηγοριοποιηθούν οι πιθανές επιπτώσεις ενός συμβάντος για τον οργανισμό. Ως γενική αρχή, οι ερευνητές στον τομέα της κυβερνό-ασφάλειας υιοθέτησαν το μοντέλο CIA, το οποίο καθορίζει τρεις στόχους ασφαλείας (CIA) όπως αναλύθηκαν σε προηγούμενο κεφάλαιο

1. Εμπιστευτικότητα (Confidentiality - C)
2. Ακεραιότητα (Integrity - I)
3. Διαθεσιμότητα (Availability - A)

Προτεραιότητα στα ΟΤ Συστήματα: Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα

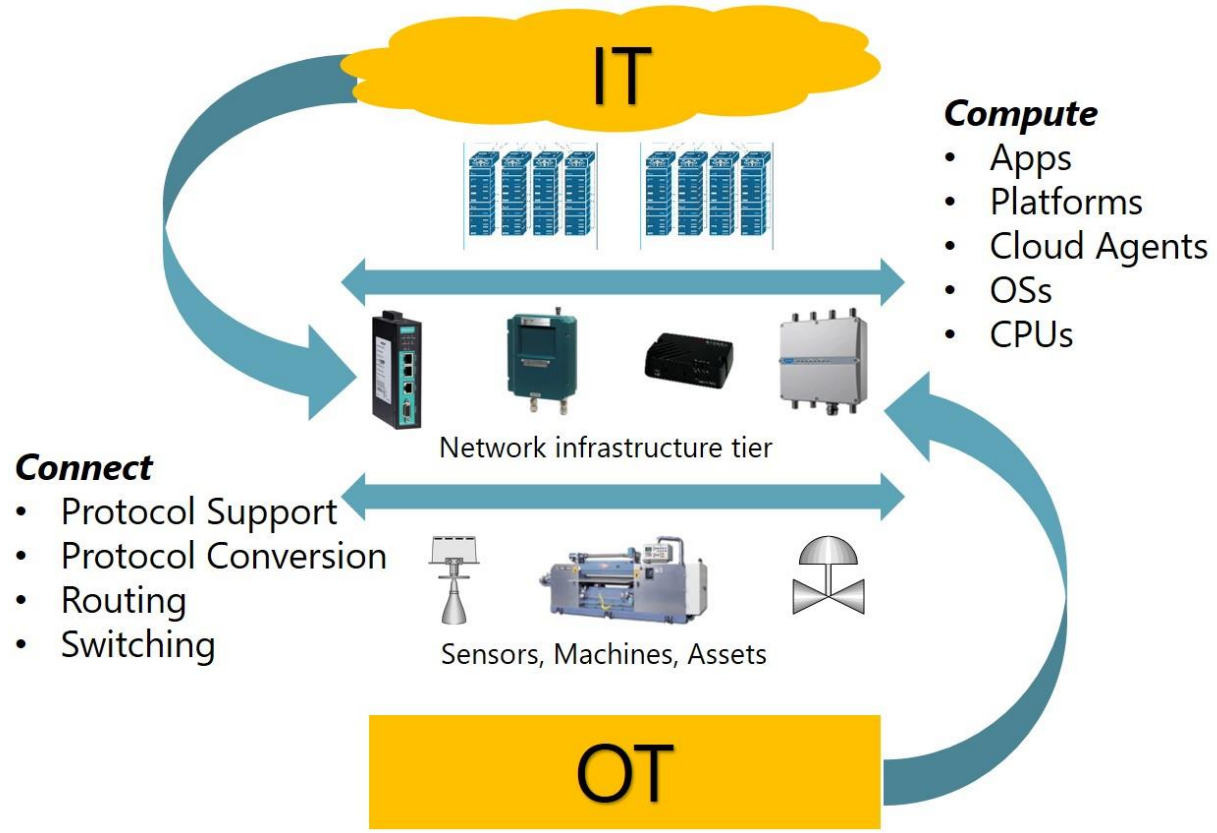
Προτεραιότητα στα IT Συστήματα:
Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα

Εικόνα 6: Προτεραιότητες IT - OT Συστημάτων

Κεφάλαιο 3.2.3: Συγκερασμός μεταξύ IT / OT συστημάτων

Για να μειωθεί ο κίνδυνος και να προστατευθούν επαρκώς και οι δύο κατηγορίες των εταιρικών συστημάτων, είναι επιτακτική η ανάγκη να δημιουργηθεί ένα ολιστικό πρόγραμμα για τα IT και OT συστήματα. Λειτουργώντας μαζί ως μια δια – τμηματική μονάδα, οι ομάδες των IT και OT μπορούν να αρχίσουν να κατανοούν τα συστήματα και να αυξήσουν τη συνολική άμυνα του οργανισμού. Η πλήρης σύγκλιση των δύο συστημάτων αποδεικνύει ότι τα IT και OT αξιοποιούν κοινά πρότυπα και προσεγγίσεις ως προς τον κίνδυνο. Λειτουργούν κάτω από μία επιχειρησιακή μονάδα με κοινούς στόχους και συνεργάζονται για την επίτευξη των στόχων του οργανισμού. Αυτό το είδος της προσέγγισης απαιτεί από τους εργαζομένους κοινή εκπαίδευση.

Η ασφάλεια στα συστήματα πληροφορικής δεν αποτελεί κάτι το καινούριο, επομένως οι IT ομάδες ασφαλείας μπορούν να αξιοποιηθούν για τη βελτίωση της ασφάλειας των OT. Οι εργαζόμενοι στα OT επικεντρώνονται στην αυτοματοποίηση των λειτουργιών και μπορούν, ως εκ τούτου, να παρέχουν τη γνώση της κρισιμότητας των συγκεκριμένων συστημάτων. Τόσο ο οργανισμός στο σύνολο του όσο και οι μεμονωμένες επιχειρησιακές μονάδες πρέπει να μάθουν ο ένας από τον άλλο δουλεύοντας μαζί για την επίτευξη κοινών στόχων.



Εικόνα 7: Συγκερασμός IT - OT Συστημάτων

Μεταξύ των πολλών οφελών της σύγκλισης των OT και IT είναι:

- Μειωμένο λειτουργικό κόστος
- Αυξημένος έλεγχος των κατανεμημένων λειτουργιών
- Βελτιωμένη ασφάλεια μέσω μιας ολοκληρωμένης προσέγγισης για την κυβερνό- ασφάλεια και στις δύο κατηγορίες συστημάτων
- Βελτιωμένη διακυβέρνηση και διαχείριση των συστημάτων
- Βελτιωμένη ασφάλεια των εγκαταστάσεων
- Μια συνεχής διαδικασία αξιολόγησης, εφαρμογής, διατήρησης και, επανάληψης της διαδικασίας

Χαρακτηριστικό	IT	OT
Εμπιστευτικότητα	Υψηλή	Χαμηλή
Ακεραιότητα	Χαμηλή -Μεσαία	Πολύ Υψηλή
Διαθεσιμότητα Συστημάτων	Χαμηλή - Μεσαία	Υψηλή
Αυθεντικοποίηση	Μεσαία - Υψηλή	Υψηλή
Μη Αποποίηση (Απόδειξη της ακεραιότητας και προέλευσης	Υψηλή	Χαμηλή - Μεσαία

των δεδομένων)		
Κρισιμότητα σε Χρόνο	Ανοχή σε Ημέρες	Κρίσιμη
Διακοπή Συστημάτων	Ανεκτή	Μη Αποδεκτή
Δεξιότητες Ασφάλειας / Ευαισθητοποίηση	Συνήθως Καλή	Συνήθως Κακή
Κύκλος ζωής Συστήματος	3-5 years	15-25 years
Διαλειτουργικότητα	Μη Κρίσιμη	Κρίσιμη
Υπολογιστικοί πόροι	Απεριόριστη	Πολύ περιορισμένη με παλαιότερους επεξεργαστές
Αλλαγές στο Λογισμικό	Συχνά	Σπάνια
Χείριστη Περίπτωση	Συχνή απώλεια δεδομένων	Καταστροφή εξοπλισμού

Πίνακας 4:Διαφορές μεταξύ IT and OT Συστημάτων [32]

Κεφάλαιο 3.3: Ευπάθειες των OT Συστημάτων

Ο όρος OT αναφέρεται σε υπολογιστικά συστήματα που διαχειρίζονται βιομηχανικά συστήματα με την παρακολούθηση ή/και τον έλεγχο φυσικών συσκευών και διεργασιών. Τα βιομηχανικά συστήματα ελέγχου (Industrial Control Systems-ICS) είναι ένα σημαντικό τμήμα στον τομέα της επιχειρησιακής τεχνολογίας. Τα OT αποτελούν το γενικό περιβάλλον των ICS's και χρησιμοποιούνται ευρέως στη ναυτιλία, τις μεταφορές, τα εργοστάσια ηλεκτροπαραγωγής, τους πυρηνικούς σταθμούς, τη βιομηχανία πετρελαίου και φυσικού αερίου, τη μεταποίηση κ.λπ. Όλα τα συστήματα που υπόκεινται στα OT είναι συνήθως κρίσιμες εφαρμογές με απαίτηση για υψηλή διαθεσιμότητα.

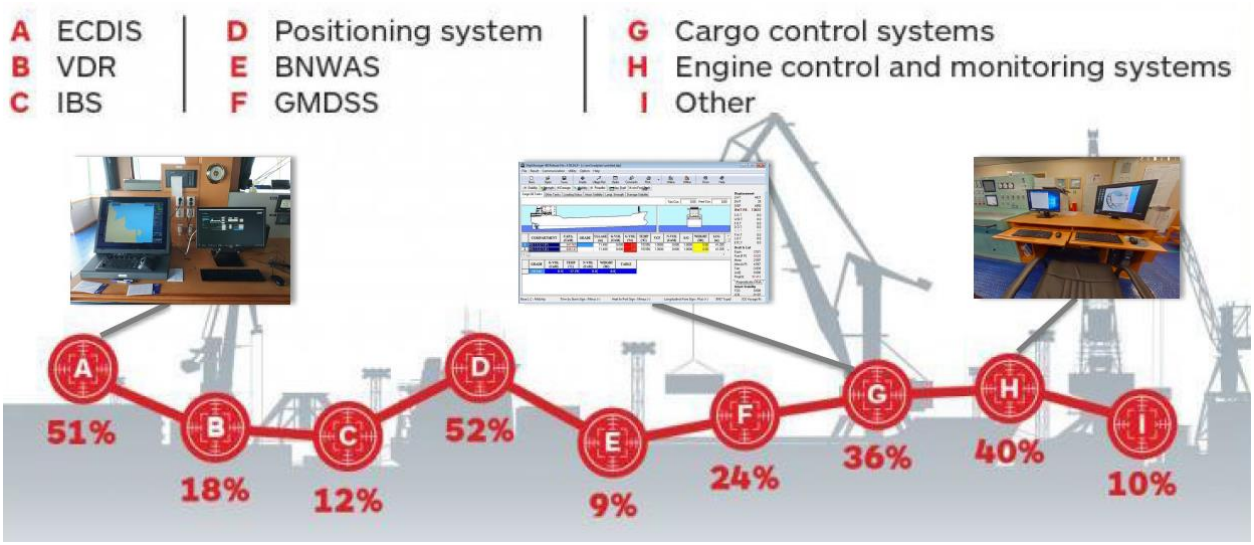
Τα ICS είναι ένας γενικός όρος που περιλαμβάνει αρκετούς διαφορετικούς τύπους συστημάτων ελέγχου, όπως τα συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων (Supervisory Control and Data Acquisition - SCADA), τα συστήματα κατανεμημένων ελέγχων (Distributed Control - DC) ή άλλα μικρότερα συστήματα ελέγχου, όπως οι Προγραμματιζόμενοι Ελεγκτές (Programmable Logic Controllers - PLC) [33]. Η συμβατική ασφάλεια των IT συστημάτων δεν επαρκεί για την προστασία από τις πολλαπλές κυβερνό- απειλές των OT. Τα ICS δίκτυα έχουν διαφορετικές επιχειρησιακές απαιτήσεις που επηρεάζουν την ικανότητα προσαρμογής και αντίδρασης σε νέες απειλές, οι οποίες τελικά αποκαλύπτουν νέες ευπάθειες. Οι στρατηγικές για την ασφάλεια έχουν σχεδιαστεί με γνώμονα την προστασία των κρίσιμων διεργασιών, χωρίς να επηρεάζουν αρνητικά τη χρήση τους.

Κεφάλαιο 3.3.1: Απειλές

Για να εντοπιστούν οι αδυναμίες που προκύπτουν από τα ICS, είναι απαραίτητο να χαρτογραφηθούν οι πιθανές απειλές. Μια ακριβής καταγραφή των κυβερνό- επιθέσεων στα συστήματα ελέγχου θα βοηθούσε προς αυτή την κατεύθυνση, αλλά τα πραγματικά περιστατικά είναι δύσκολο να προσδιοριστούν. Αυτό συμβαίνει διότι τα περιστατικά που αφορούν τα ICS συστήματα δε δημοσιοποιούνται σχεδόν ποτέ λόγω του φόβου της ζημίας που ίσως προκληθεί στη φήμη του οργανισμού. Ωστόσο, οι ερευνητές από το Kaspersky Lab παραδέχθηκαν ότι αυτές οι επιθέσεις αυξάνονται σε δημοτικότητα και πρέπει οι βιομηχανίες να αλλάξουν αυτά τα στατιστικά στοιχεία. Στο δεύτερο εξάμηνο του 2017, τα προϊόντα της εταιρείας αντιμετώπισαν περίπου το 37,8% των επιθέσεων [34]. Σύμφωνα με τις οδηγίες για την προστασία των βιομηχανικών συστημάτων σε πλοίο που

δημοσιεύθηκε από τη διεύθυνση θαλάσσιων υποθέσεων [35], οι ευπάθειες ενός συστήματος μπορούν να κατηγοριοποιηθούν σε επτά τομείς:

1. **Έλλειψη ασφαλούς ανάπτυξης λογισμικού:** Εσωτερική ανάπτυξη λογισμικού, έλλειψη ενοποίησης ασφάλειας, μη ασφαλής συνδέσεις
2. **Χαμηλό επίπεδο προστασίας πρόσβασης:** Απλός έλεγχος πρόσβασης με χρήστη ή κωδικό πρόσβασης πολύ αδύναμο ή ανύπαρκτο, χωρίς antivirus σε σταθμούς εργασίας και διακομιστές, χρήστες με δικαιώματα διαχειριστή
3. **Η έλλειψη διαχωρισμού μεταξύ συστημάτων διαχείρισης πληροφοριών και μη ασφαλών βιομηχανικών συστημάτων:** Αυτό το χαρακτηριστικό είναι ο στόχος πολλών επιθέσεων. Αυτές οι γέφυρες χρησιμοποιούνται για την ανάκτηση πληροφοριών μέσω των συστημάτων ελέγχου. Αυτή η μέθοδος πρόσβασης επιτρέπει τόσο τη συλλογή πληροφοριών όσο και το σαμποτάζ
4. **Η απουσία εποπτείας του συστήματος:** Αν και πολλές εταιρείες συλλέγουν δεδομένα των συστημάτων τους για να εξάγουν πληροφορίες σχετικά με τις επιδόσεις τους, δεν υπάρχει ειδική διαδικασία ή εκπαιδευμένο προσωπικό για τον έλεγχο μη φυσιολογικής δραστηριότητας
5. **Μη ενημερωμένα και αδύναμα πρωτόκολλα διαχείρισης:** Χρησιμοποιούνται πρωτόκολλα χωρίς κρυπτογράφηση που επιτρέπουν τη μη εξουσιοδοτημένη πρόσβαση στα συστήματα
6. **Αυξανόμενη χρήση μη ασφαλών συστημάτων:** Αυτά τα προϊόντα επιτρέπουν τη μείωση του κόστους και τη διαλειτουργικότητα (TCP/IP, Ethernet: Λόγω της απλότητάς τους, το κόστος αυτών των τεχνολογιών έχει καταστήσει τη χρήση τους αναπόφευκτη). Επομένως, τα συστήματα αυτά είναι ευάλωτα σε επιθέσεις με κακόβουλο λογισμικό
7. **Έλλειψη ελέγχου των τρίτων μερών στα βιομηχανικά συστήματα:** Η παρακολούθηση των υπεργολάβων είναι συχνά ανεπαρκής. Οι συνέπειες αυτής της έλλειψης ελέγχου μπορεί να είναι η απώλεια δεδομένων, η βλάβη του εξοπλισμού, η διακινδύνευση του πληρώματος του πλοίου και του περιβάλλοντος



Εικόνα 8: Πιθανότητα απειλών στα OT Συστήματα

Κεφάλαιο 3.3.2: Stuxnet

Ο ιός Stuxnet ήταν μια πολύ επινοητική και περίπλοκη επίθεση που στόχευε σε ένα συγκεκριμένο σύνολο συστημάτων ελέγχου της Siemens. Αυτά τα συστήματα της Siemens χρησιμοποιήθηκαν για τον έλεγχο των φυγοκεντρικών εγκαταστάσεων στο εργοστάσιο εμπλουτισμού ουρανίου του Ιράν. Ανακαλύφθηκε το 2010, αφού είχε προκαλέσει ζημιά σε σχεδόν 1000 φυγοκεντρητές στο ιρανικό εργοστάσιο [36]. Μολύνοντας το λογισμικό της Siemens, ο Stuxnet κατάφερε να αποκτήσει πρόσβαση στα συστήματα του εργοστασίου και να διαταράξει τη λειτουργία. Ήταν τόσο επεμβατικός ο ιός, ώστε αν ένα USB συνδεόταν στα επηρεαζόμενα συστήματα, ο ιός μπορούσε να διεισδύσει στη συσκευή και να εξαπλωθεί σε άλλα συστήματα όπου μπορούσε το USB να συνδεθεί [37]. Αν και ο Stuxnet σχεδιάστηκε για να επιτεθεί σε ένα συγκεκριμένο σύστημα, ερευνητές όπως ο Ralph Langner επεσήμαναν ότι το κακόβουλο λογισμικό θα μπορούσε εύκολα να χρησιμοποιηθεί για να επιτεθεί σε άλλα βιομηχανικά συστήματα σε όλο τον κόσμο [38]. Ο ιός αυτός επισημάνθηκε ως το πιο εξελιγμένο και πολύπλοκο λογισμικό που έχει γραφτεί ποτέ, στοχεύοντας σε υποδομές κρίσιμης σημασίας και αποκάλυψε ότι μεταξύ των ICS, οι ευπάθειες είναι υπαρκτές και η απειλή είναι πραγματική.

Κεφάλαιο 3.3.3: Διαδίκτυο των Πραγμάτων και Μεγάλα Δεδομένα

Το Διαδίκτυο των πραγμάτων και η ψηφιακή εποχή ανοίγουν νέες δυνατότητες στη ναυτιλιακή βιομηχανία. Με τα ICS συστήματα να συνδέονται στο cloud, οι ιδιοκτήτες, τα ενδιαφερόμενα μέρη, οι προμηθευτές και οι κατασκευαστές είναι σε θέση να έχουν καλύτερη επίβλεψη των συστημάτων, να αυξήσουν την αποτελεσματικότητά και να συλλέγουν δεδομένα για να συνεχίσουν την έρευνά τους στοχεύοντας στη βελτιστοποίηση των επιδόσεων του οργανισμού. Επενδύοντας σε αισθητήρες και συστήματα, οι ναυτιλιακές εταιρείες επωφελούνται από τη βελτιωμένη αποδοτικότητα του πλοίου, μειώνοντας το κόστος λειτουργίας και συντήρησης. Ωστόσο, η βιομηχανία πρέπει να εκλογικεύσει αυτή την ανάγκη για τη συλλογή δεδομένων, καθώς τα μεγάλα δεδομένα αποκρύπτουν μεγάλα ζητήματα, όπως της ποιότητας των δεδομένων. Σύμφωνα με τον DNV GL, το 2017 μόνο στις ΗΠΑ το κόστος της επιχείρησης των λανθασμένων δεδομένων ήταν 3.1 τρις δολάρια. Με τον όρο εσφαλμένα δεδομένα, ο νηογνώμονας καθορίζει τις κακές αποφάσεις λόγω λανθασμένων πρακτικών διαχείρισης και εκτίμησης δεδομένων.

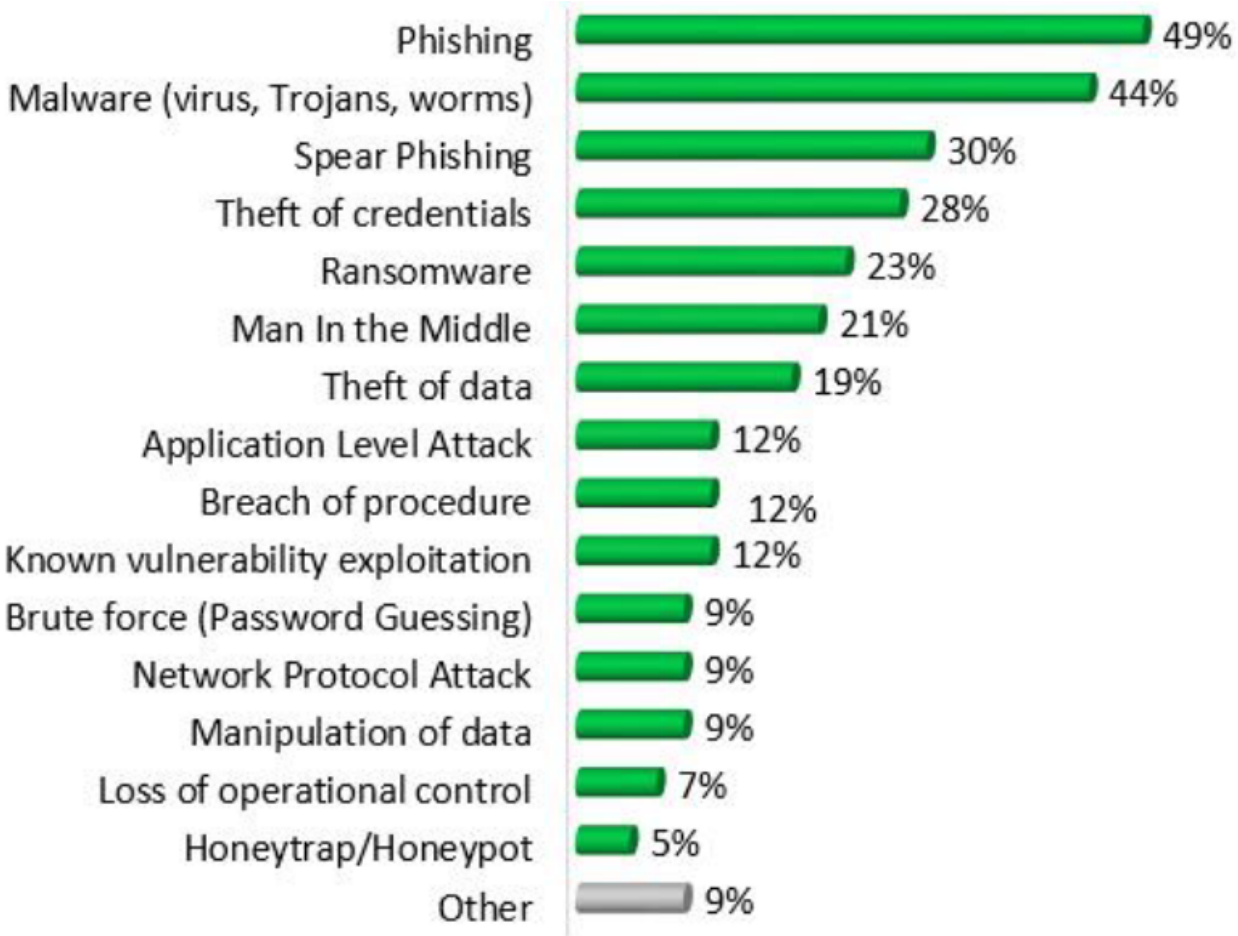
Επιπλέον, αυτή η αυξημένη συνδεσιμότητα, δημιουργεί νέες απειλές για την ασφάλεια στη θάλασσα, καθιστώντας τη βιομηχανία πιο ευάλωτη στις κυβερνό- επιθέσεις. Παρακολουθώντας συνεχώς τις κρίσιμες υποδομές στο πλοίο, οι κατασκευαστές δημιουργούν πολλές ανεξέλεγκτες συνδέσεις μεταξύ του πλοίου και των εγκαταστάσεων στη στεριά. Με τον αριθμό των συσκευών που συνδέονται με το cloud να αυξάνεται συνεχώς, πολλές εταιρείες συμφωνούν ότι η σύνδεση δεν πρέπει να υφίσταται πριν από την εφαρμογή των κατάλληλων ελέγχων, καθώς και την εφαρμογή διασφαλίσεων.

Εν κατακλείδι, η χρήση του IoT φαίνεται να αυξάνεται γρήγορα στον τομέα της ναυτιλίας, καθώς επιτρέπει στις εταιρείες να λαμβάνουν αποφάσεις, με βάση τα δεδομένα, για την εκπλήρωση των στόχων του οργανισμού. Μέσα από μια εκτεταμένη επιστημονική έρευνα που πραγματοποιήθηκε από το MIT και την IBM, διαπιστώθηκε ότι οι κορυφαίες εταιρείες είναι πιθανότερο να είναι εξελιγμένοι χρήστες αναλυτικών στοιχείων από τις μικρομεσαίες εταιρείες και πιο πιθανό να δουν τη χρήση της

ανάλυσης δεδομένων σαν στοιχείο διαφοροποίησης [39]. Ωστόσο, οι προκλήσεις που προκύπτουν από αυτές τις καινοτομίες θα πρέπει να αντιμετωπιστούν προσεκτικά, προκειμένου να αυξηθεί η παραγωγή και να δημιουργηθεί υψηλότερη αξία για τον οργανισμό.

Κεφάλαιο 4: Ανάλυση Κινδύνων στη Ναυτιλιακή Βιομηχανία

Η συνεχώς αυξανόμενη συνδεσιμότητα των συστημάτων έχει αλλάξει δραματικά το επιχειρείν. Αυτή η εξάρτηση από την ψηφιακή τεχνολογία και τα δίκτυα υπολογιστών θέτει τους οργανισμούς σε κινδύνους στο διαδίκτυο που μέχρι σήμερα ήταν άγνωστοι. Προκειμένου να αυξηθεί η ευαισθητοποίηση στον τομέα της κυβερνό- ασφάλειας, το 2016 IHS Fairplay σε συνεργασία με την BIMCO διεξήγαγε έρευνα για τη διερεύνηση των διαφόρων τύπων απειλών στις οποίες είναι περισσότερο επιρρεπής η ναυτιλιακή βιομηχανία [40].



Εικόνα 9: Έρευνα της IHS Fairplay

Από τους 300 οργανισμούς που πήραν μέρος στην έρευνα, οι 65 δήλωσαν ότι είχα πέσει θύμα κυβερνό- επίθεσης. Η παραπάνω εικόνα περιγράφει ποια ήταν η φύση της επίθεσης όσων ανταποκρίθηκαν στην έρευνα. Το κακόβουλο λογισμικό φαίνεται να είναι η κύρια επίθεση, με το

ποσοστό να ανέρχεται στο 44% των ερωτηθέντων. Ένα ενδιαφέρον συμπέρασμα της έρευνας ήταν το γεγονός ότι το ποσοστό 49% των phishing επιθέσεων, το οποίο πραγματοποιήθηκε κυρίως μέσω ηλεκτρονικού ταχυδρομείου και ένα 30% μέσω spear phishing επιθέσεων. Οι επιθέσεις Spear phishing αποτελούν εξειδικευμένες επιθέσεις, με συγκεκριμένους στόχους. Ένα ακόμα ενδιαφέρον σημείο της έρευνας είναι οι Ransomware επιθέσεις, οι οποίες αποτελούν μία δημοφιλή τακτική επίθεσης εναντίον της βιομηχανίας, με το 23% των ερωτηθέντων να δηλώνουν ότι έχουν αντιμετωπίσει ένα τέτοιο είδος επίθεσης.

Υπάρχουν διαφορετικοί τύποι απειλών που υπάρχουν στα βιομηχανικά περιβάλλοντα και πιο συγκεκριμένα στον ναυτιλιακό κλάδο. Αυτοί μπορούν να είναι είτε εκούσιοι, είτε τυχαίοι (ακούσιοι), μη στοχευμένοι ή στοχευμένοι σε μια συγκεκριμένη εταιρεία, πλοίο ή στόλο. Παρακάτω περιγράφονται οι κατηγορίες των κυβερνό- επιθέσεων που μπορούν να επηρεάσουν τη ναυτιλιακή βιομηχανία:

- **Στοχευμένες**: Μία εταιρεία ή τα συστήματα και τα δεδομένα ενός πλοίου αποτελούν τον επιδιωκόμενο στόχο
- **Μη στοχευμένες**: Μία εταιρεία ή τα συστήματα και τα δεδομένα ενός πλοίου είναι ένας από τους πολλούς δυνητικούς στόχους
- **Σκόπιμες:** Η παραβίαση προέρχεται από εσκεμμένες κακόβουλες ενέργειες
- **Ακούσιες:** Η παραβίαση είναι αποτέλεσμα αμέλειας ή άγνοιας

	Σκόπιμες	Ακούσιες
Στοχευμένες	Brute force Denial of service Spear-Phishing Port scanning	Social Engineering , Pentest
Μη στοχευμένες	Malware Phishing Water holing Scanning	User Error

Πίνακας 5: Κατηγοριοποίηση απειλών

Κεφάλαιο 4.1: Είδη Επιθέσεων

Malware: Το malware είναι κακόβουλο λογισμικό που έχει σχεδιαστεί για να αποκτήσει πρόσβαση ή να προκαλέσει βλάβη σε έναν υπολογιστή, διακομιστή ή δίκτυο χωρίς τη γνώση του θύματος. Ο όρος χρησιμοποιείται αυτός για να προσδιορίσει διάφορες απειλές του Διαδικτύου και περιέχει μοναδικά χαρακτηριστικά. Οι χάκερς, οι άνθρωποι που χρησιμοποιούν τις γνώσεις τους στον κώδικα για να παρακάμπτουν τα μέτρα ασφαλείας, δημιουργούν κακόβουλο λογισμικό. Ο σκοπός του κακόβουλου λογισμικού είναι να κλέψει πόρους από έναν υπολογιστή και να εκμεταλλευτεί γνωστές ελλείψεις ή προβλήματα του δικτύου (για παράδειγμα, ένα ξεπερασμένο ή μη ενημερωμένο λογισμικό). Malware μπορεί να είναι ένας ιός (virus), ένα Trojan horse, ένα ransomware ή ένα spyware:

- **Ιός (Virus):** Ο ιός είναι ένα πρόγραμμα που μπορεί να δημιουργήσει ένα αντίγραφο του εαυτού του και να εξαπλωθεί σε άλλους συνδεδεμένους υπολογιστές. Οι ιοί συχνά εξαπλώνονται σε

άλλους υπολογιστές, σε νόμιμα προγράμματα ή έγγραφα, εκτελώντας κώδικα όταν ένας χρήστης εκκινεί ένα από αυτά τα προγράμματα

- **Trojan Horse:** Αυτά τα κομμάτια του malware κρύβονται στο νόμιμο λογισμικό. Υπάρχουν διαφορετικοί τύποι τέτοιων malwares. Κάποια από τα πιο δημοφιλή Trojans έχουν πλήξει τραπεζικές εφαρμογές. Στην πραγματικότητα είναι malwares που εστιάζουν σε τραπεζικές συναλλαγές και μπορούν να μείνουν στο παρασκήνιο ενός μηχανήματος κλέβοντας κωδικούς πρόσβασης και δημιουργώντας ένα ψεύτικο περιβάλλον όπου ο χρήστης νομίζει ότι είναι το πραγματικό περιβάλλον της Τράπεζας. Υπάρχει, επίσης άλλο είδος Trojan κύριος στόχος του οποίου είναι να εκμεταλλευτεί μία ευπάθεια στον υπολογιστή του θύματος επιτρέποντας στον επιτιθέμενο να αποκτήσει πρόσβαση στον υπολογιστή και να πάρει τον έλεγχό του. Τελευταίο αλλά όχι λιγότερο σημαντικό είδος Trojan, έχει ως κύριο στόχο να κλέψει δεδομένα από τον υπολογιστή του θύματος
- **Ransomware:** Σύμφωνα με την αναφορά της Symantec για την ασφάλεια στο διαδίκτυο, το 2017 μόνο, υπήρξε αύξηση 90% των ransomwares που στοχεύουν το επιχειρηματικό περιβάλλον [41]. Τα Ransomwares μπορούν να κλειδώνουν έναν υπολογιστή, να κρυπτογραφούν αρχεία και να αναγκάζουν τους χρήστες να πληρώνουν χρηματικά ποσά για να πάρουν το κλειδί αποκρυπτογράφησης των αρχείων τους
- **Spyware:** Αυτός ο τύπος κακόβουλου λογισμικού έχει σχεδιαστεί για να κρυφτεί σε έναν υπολογιστή και να παρακολουθεί όλες τις δραστηριότητες του χρήστη. Μπορεί να παρακολουθήσει τη δραστηριότητα στο διαδίκτυο, να αποκτήσει πρόσβαση στο ηλεκτρονικό ταχυδρομείο, ακόμα και να κλέψει ονόματα χρηστών και κωδικούς πρόσβασης
- **Worms:** Κύριος στόχος ενός worm είναι να κάνει όσο το δυνατόν περισσότερα αντίγραφα του εαυτού του με οποιονδήποτε τρόπο από υπολογιστή σε υπολογιστή. Ένας τέτοιος ιός μπορεί να αναπαραχθεί χωρίς ανθρώπινη αλληλεπίδραση και δεν χρειάζεται να προσκολλάται σε ένα πρόγραμμα για να προκαλέσει ζημιές. Μπορεί να τροποποιήσει και να διαγράψει αρχεία, ακόμη και να εισάγει επιπλέον κακόβουλο λογισμικό στον υπολογιστή
- **Social Engineering:** Όπως συμβαίνει με κάθε συσκευή, οι χρήστες είναι ο πιο αδύναμος κρίκος στην αλυσίδα ασφαλείας. Οι ενέργειές τους παρουσιάζουν μια τρύπα ασφαλείας που δεν μπορεί ποτέ να αντιμετωπιστεί πλήρως. Επίσης, μία επίθεση από το εσωτερικό του οργανισμού δημιουργεί μεγαλύτερη απειλή για τη συνολική ασφάλεια. Το χειρότερο σενάριο δημιουργείται όταν ένας εκ των έσω εισβολέας, συνήθως ένας εργαζόμενος, δεν γνωρίζει ότι είναι η πηγή του κινδύνου
- **Phishing:** Η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μεγάλο αριθμό πιθανών στόχων, ζητώντας ευαίσθητες πληροφορίες. Έχει σχεδιαστεί για να ξεγελάσει το χρήστη και να διεκδικήσει εμπιστευτικά δεδομένα. Ένα τέτοιο e-mail υπάρχει περίπτωση να ζητήσει το όνομα χρήστη, τον κωδικό πρόσβασης, τον αριθμό PIN της τραπεζικής κάρτας του χρήστη ή να κάνει το θύμα να επισκεφτεί έναν ψεύτικο ιστότοπο
- **Water Holing**: Αυτό το είδος της επίθεσης έχει στόχο να υπονομεύσει μια συγκεκριμένη ομάδα τελικών χρηστών μολύνοντας ιστοσελίδες που είναι γνωστό ότι επισκέπτονται τα μέλη της ομάδας. Ο στόχος είναι να μολύνει τον υπολογιστή ενός χρήστη και να αποκτήσει πρόσβαση στο δίκτυο του οργανισμού. Ουσιαστικά πρόκειται για επιθέσεις που εστιάζουν σε νόμιμες

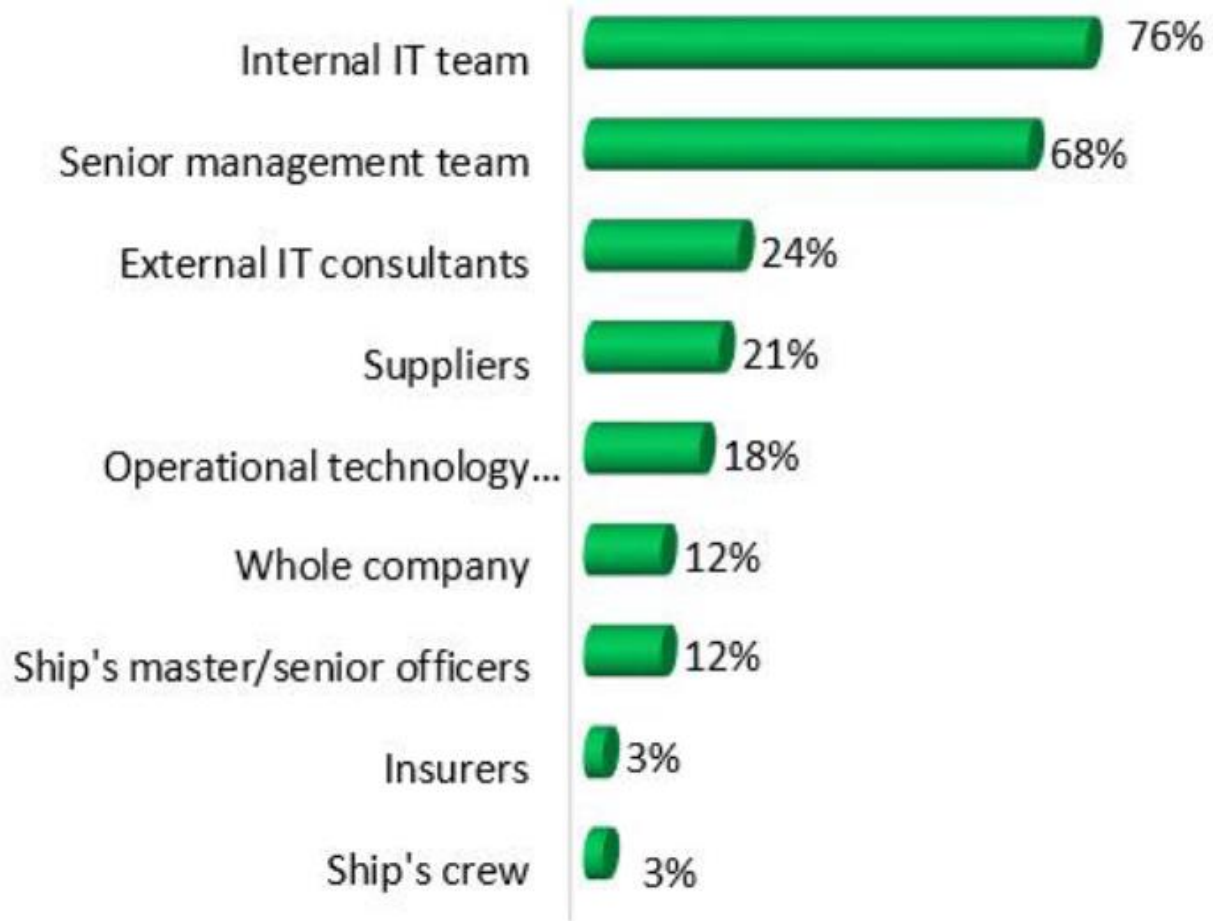
ιστοσελίδες με σκοπό να αποκτήσουν πρόσβαση σε άλλες πληροφορίες. ο επιτιθέμενος αρχικά σκιαγραφεί τους στόχους του--οι οποίοι είναι συνήθως υπάλληλοι μεγάλων επιχειρήσεων, ομάδες ανθρωπίνων δικαιωμάτων ή κυβερνητικές υπηρεσίες--για να καθορίσουν το είδος των ισότοπων που συχνά επισκέπτονται. Στη συνέχεια, ο εισβολέας αναζητά ευπάθειες στις συγκεκριμένες τοποθεσίες και εισάγει κακόβουλο κώδικα JavaScript ή HTML, ανακατευθύνοντας το στόχο σε μια ξεχωριστή τοποθεσία όπου φιλοξενείται το κακόβουλο λογισμικό. Αυτή η Web τοποθεσία είναι έτοιμη να μολύνει τον στόχο με κακόβουλο λογισμικό κατά την πρόσβαση. Ενώ οι συγκεκριμένες επιθέσεις είναι ασυνήθιστες, αποτελούν σημαντική απειλή, δεδομένου ότι είναι δύσκολο να εντοπιστούν και συνήθως στοχεύουν οργανισμούς υψηλής ασφάλειας μέσω των εργαζομένων χαμηλής ασφάλειας, των συνεργατών τους, των προμηθευτών ή ενός μη ασφαλούς ασύρματου Δικτύου. Η τεχνική αυτή αποτελεί μία εσκεμμένη και μη στοχευμένη επίθεση

- **Port Scanning**: Οι θύρες είναι λογισμικό που θα χρησιμοποιήσει μια εφαρμογή για να επικοινωνήσει μέσω του λειτουργικού συστήματος, ενός υπολογιστή, με το Διαδίκτυο. Μια επίθεση σάρωσης θυρών παρουσιάζεται όταν ένας επιτιθέμενος αποστέλλει πακέτα σε έναν υπολογιστή, αλλάζοντας τη θύρα προορισμού. Ο κύριος στόχος αυτής της επίθεσης είναι να εξετασθεί ποιες θύρες έχει ανοίξει ο χρήστης για τις εισερχόμενες συνδέσεις
- **Built-in Software Weaknesses:** Θέματα ευπάθειας που σχετίζονται με ανεπαρκή έλεγχο των χρηστών που έχουν πρόσβαση στα συστήματα
- **Third Party Contribution:** Έχοντας πρόσβαση στα συστήματα της εταιρίας, οι προμηθευτές ή οι τεχνικοί, είναι δυνατόν να δημιουργηθούν ευπάθειες στα συστήματα αυτά εν αγνοία του οργανισμού
- **Brute Force:** Μια επίθεση που δοκιμάζει πολλούς κωδικούς πρόσβασης με την ελπίδα τελικά να βρεθεί ο σωστός. Ο επιτιθέμενος ελέγχει όλους τους πιθανούς κωδικούς πρόσβασης μέχρι να βρεθεί ο σωστός. Αυτός είναι ο λόγος για τον οποίο σχεδόν όλοι οι ιστότοποι απαιτούν κωδικούς πρόσβασης με τυχαίους συνδυασμούς γραμμάτων και αριθμών και αξιολογούν το επίπεδο ασφαλείας τους
- **Denial of Service (Dos):** Η άρνηση εξυπηρέτησης (Denial of Service) έχει σχεδιαστεί για να εμποδίζει τους νόμιμους και εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε πληροφορίες, συνήθως κατακλύζοντας το δίκτυο-στόχο με μια συνεχή ροή κυκλοφορίας από διαφορετικές πηγές. Μια επίθεση DDoS στοχεύει στη διακοπή της κανονικής λειτουργίας ενός συγκεκριμένου διακομιστή ή δικτύου. Μόλις ένα τερματικό μηχάνημα έχει μολυνθεί με malware, γίνεται ένα bot (ρομπότ) που μπορεί να είναι μέρος ενός μεγαλύτερου botnet. Αυτά τα botnets χρησιμοποιούνται συχνά για να κατακλύσουν το διακομιστή-στόχο ή το δίκτυο με τεράστιες ποσότητες δικτυακής κίνησης. Αυτό η τεχνική είναι γνωστή ως κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service - DDoS). Τα bots δεν είναι ο στόχος, και συχνά αγνοούν τη μόλυνση, αλλά είναι αποτελεσματικά εργαλεία που πρέπει να χρησιμοποιηθούν. Μερικοί τρόποι για να μειωθεί ο κίνδυνος από μία DoS επίθεση είναι να απενεργοποιηθούν οι περιττές υπηρεσίες, η χρησιμοποίηση firewall και συνεχής ενημέρωση του υλικού και του λογισμικού που χρησιμοποιεί ο οργανισμός

- **Spear Phishing:** Αποτελεί ίδια τεχνική επίθεσης με το phishing, ωστόσο τα θύματα προσεγγίζονται μέσω προσωπικών emails τα οποία περιέχουν κακόβουλο λογισμικό ή υπερσύνδεσμο
- **Subverting the supply chain:** Επίθεση σε εταιρεία ή πλοίο αποκτώντας τον έλεγχο εξοπλισμού, λογισμικού ή υποστηρικτικών υπηρεσιών που παραδίδονται στην εταιρεία ή το πλοίο. Αυτός ο τύπος επίθεσης είναι εξαιρετικά δημοφιλής στον τομέα της ναυτιλίας. Λόγω της σύνδεσης σε πραγματικό χρόνο μεταξύ των μελών της αλυσίδας εφοδιασμού, οι επιθέσεις σε λιμένες ή τερματικούς σταθμούς ή ακόμη και σε άλλους οργανισμούς, είναι ακόμη ένας επιτυχημένος τρόπος χειραγώγησης ενός συστήματος

Κεφάλαιο 4.2: Ανθρώπινος Παράγοντας- Το πιο Αδύναμο Σημείο

Τα πλοία εξελίσσονται όλο και περισσότερο και τα συστήματα με τα οποία διασυνδέονται αυξάνονται συνεχώς. Η επικοινωνία, σήμερα, μεταφέρει περισσότερα δεδομένα και πιο γρήγορα σε σχέση με το παρελθόν. Τα τελευταία χρόνια, τα πλοία θεωρούνταν απρόσβλητα από επιθέσεις, επειδή η ροή των δεδομένων ήταν σημαντικά αργή και, επομένως, δεν ήταν ελκυστική για τους κακόβουλους χρήστες. Ωστόσο, καθώς τα συστήματα βελτιώνονται, η βιομηχανία γίνεται όλο και πιο ευάλωτη. Ακόμη και στα πιο ασφαλή συστήματα, υπάρχει μια ευπάθεια η οποία δεν μπορεί να διορθωθεί. Ενώ οι άνθρωποι συνεχίζουν να αλληλεπιδρούν με τα συστήματα στην ξηρά και στο πλοίο, το ανθρώπινο στοιχείο εξακολουθεί να διαδραματίζει σημαντικό ρόλο στην πλειονότητα των περιστατικών ασφάλειας. Η εκπαίδευση και η ευαισθητοποίηση του προσωπικού είναι το πρώτο μεγάλο βήμα που θα πρέπει να κάνει η βιομηχανία για την ενίσχυση της ασφάλειας. Κατά τη διάρκεια της συνόδου κορυφής για τις θαλάσσιες μεταφορές, ο επικεφαλής του κανονισμού για τις θαλάσσιες τεχνολογίες της BIMCO ανέφερε ότι: “το 80% των περιστατικών κυβερνό- ασφάλειας θα μπορούσε να είχε αποτραπεί εάν οι ίδιοι χρήστες μπορούσαν να αναγνωρίσουν την απειλή. Είναι ζωτικής σημασίας η εκπαίδευση του πληρώματος προκειμένου να ευαισθητοποιηθεί σχετικά με τις ευπάθειες που προκύπτουν από το ανθρώπινο σφάλμα”. Σύμφωνα με έρευνα που διεξήχθη το 2018, σε περισσότερα από 6.000 μέλη πληρωμάτων, μόνο το 15% είχε λάβει οποιαδήποτε μορφή εκπαίδευσης και ένα 20% των ναυτικών εντόπισαν αυτό το χάσμα, καθώς “αισθάνονται ότι η εκπαίδευση σχετικά με την ασφάλεια στον κυβερνοχώρο λείπει από το πλοίο”. Η έρευνα κατέδειξε επίσης ότι το 60% των ναυτικών επιθυμεί καλύτερη εκπαίδευση για τη διαχείριση της κυβερνό- ασφάλειας και το 49% παραδέχθηκε ότι δεν γνωρίζει τις πολιτικές ασφαλείας του οργανισμού.



Εικόνα 10: Εμπλεκόμενα μέρη

Η έρευνα αποκάλυψε ότι το 47% των ναυτικών έχει υπάρξει σε πλοίο που είχε γίνει στόχος κυβερνό-επίθεσης και το 85% του πληρώματος πλοίου που έχει δεχθεί επίθεση, δεν είχε λάβει σχετική εκπαίδευση. Επίσης μόνο το 18% των ερωτηθέντων δήλωσε ότι η εταιρεία για την οποία εργάστηκαν είχε θεσπίσει πολιτική για να αλλάξει τους προεπιλεγμένους κωδικούς πρόσβασης στο πλοίο. Οι ναυτικοί με την κατάλληλη εκπαίδευση είναι μια πρώτη γραμμή άμυνας και με τα κατάλληλα εργαλεία είναι ικανοί να προστατεύσουν το πλοίο και να διατηρήσουν τον εαυτό τους αλλά και το ευρύτερο θαλάσσιο οικοσύστημα ασφαλή. Εν κατακλείδι, τα συστήματα και τα δεδομένα της εταιρείας είναι επιρρεπή σε κίνδυνο από το προσωπικό, στο πλοίο ή στην ακτή. Σε γενικές γραμμές, το μεγαλύτερο ποσοστό αυτών των περιστατικών είναι ακούσια και προκαλούνται από ένα ανθρώπινο σφάλμα κατά τη λειτουργία και τη διαχείριση των συστημάτων (IT / OT). Η εταιρεία θα πρέπει να έχει επίγνωση της ελλιπής γνώσης του πληρώματος σχετικά με τα τεχνικά και διαδικαστικά μέτρα προστασίας. Ωστόσο, υπάρχει πιθανότητα οι κακόβουλες αυτές ενέργειες να αποτελούν μια εσκεμμένη απόπειρα εναντίον της εταιρείας και του στόλου, από έναν δυσαρεστημένο υπάλληλο.

Τα άτομα που μπορούν να επιχειρήσουν μία επίθεση είναι συνήθως αυτά που χειρίζονται τα IT/ OT συστήματα όπως:

- Μέτοχοι/ Ιδιοκτήτες

- Διοίκηση
- Εργαζόμενοι
- Συνεργάτες
- Πάροχοι Υπηρεσιών
- Υπεργολάβοι
- Πελάτες

Η σοβαρότητα και η πολυπλοκότητα της απειλής καθορίζεται από τις δυνατότητες του επιτιθέμενου, για παράδειγμα [43]:

- **Ένας απρόσεκτος εργαζόμενος:** Όταν δεν ακολουθεί τις πολιτικές ασφαλείας υπονομεύει την ασφάλεια του συστήματος
- **Ένας απογοητευμένος εργαζόμενος:** Η πρόθεση του μπορεί να είναι η κλοπή ή η διαρροή ευαίσθητων πληροφοριών, η δολιοφθορά ή η διατάραξη της λειτουργίας του πλοίου. Το μέγεθος της ζημιάς που μπορεί να προκληθεί θα εξαρτηθεί από τον ρόλο του, τα δικαιώματα πρόσβασης στα συστήματα και την αποτελεσματικότητα των αντιμέτρων που έχουν εφαρμοσθεί στα συστήματα και τα δεδομένα του πλοίου. Ειδικότερα, εάν ο εργαζόμενος αυτός έχει σημαντικές IT γνώσεις και δικαιώματα διαχειριστή στα συστήματα του πλοίου, έχει τη δυνατότητα να προκαλέσει σημαντική ζημιά. Μπορεί να έχει επαρκείς γνώσεις και ικανότητα να παρακάμπτει τους ελέγχους, τα προστατευτικά μέτρα και μπορεί να είναι ικανός να αφαιρεί αποδεικτικά στοιχεία για τις κακόβουλες ενέργειες του, για παράδειγμα, διαγράφοντας ή τροποποιώντας τις καταχωρήσεις στα αρχεία καταγραφής του συστήματος (system log files)
- **Script Kiddies:** Μεμονωμένοι χάκερς με περιορισμένες γνώσεις που χρησιμοποιούν τεχνικές και εργαλεία που επινοήθηκαν και αναπτύχθηκαν από άλλους ανθρώπους. Η διαθεσιμότητα των εργαλείων παραβίασης και άρνησης εξυπηρέτησης σημαίνει ότι το επίπεδο της τεχνικής κατανόησης που απαιτείται για την έναρξη μιας επίθεσης έχει μειωθεί σημαντικά
- **Μοναχικός Λύκος:** Πρόκειται για άτομα εκτός του οργανισμού που διαθέτουν προηγμένες τεχνικές γνώσεις. Αυτή η κατηγορία κακόβουλων χρηστών μπορεί να είναι έμπειρη στην κατάργηση αποδεικτικών στοιχείων για τις δραστηριότητές τους, για παράδειγμα διαγράφοντας ή τροποποιώντας καταχωρήσεις στα αρχεία καταγραφής συστήματος. Μπορούν επίσης να έχουν επαρκείς γνώσεις και ικανότητα να παρακάμπτουν τους ελέγχους και τα προστατευτικά μέτρα. Ο αριθμός αυτών των ατόμων είναι ακόμα μικρός αλλά μπορεί να αυξηθεί σημαντικά τα επόμενα χρόνια

Τα εργαλεία που χρησιμοποιούν για να αποκτήσουν πρόσβαση στα συστήματα αφορούν κυρίως:

- Υποδομή δικτύου
- Λογισμικό Εφαρμογών
- Επίπεδο Φυσικής Ασφάλειας
- Συσκευές Πρόσβασης

Κεφάλαιο 4.2.1: Bring Your Own Device

Σήμερα το πλήρωμα ή πιο συγκεκριμένα οι προσωπικές συσκευές που χρησιμοποιούν στο πλοίο είναι η πηγή πολλών από τις επιθέσεις που δέχονται τα συστήματα των πλοίων. Το πλήρωμα έχει τη δυνατότητα να φέρει τις δικές του συσκευές (BYOD) στο πλοίο και να έχει πρόσβαση στο σύστημα ή στο δίκτυο των πλοίων. Αν και αυτή η πρακτική μπορεί να είναι χρήσιμη για τα πληρώματα και οικονομική για τις εταιρείες, αυτές οι συσκευές δεν μπορεί να είναι πλήρως ελεγχόμενες γεγονός που αυξάνει σημαντικά τα τρωτά σημεία των συστημάτων. Για την αντιμετώπιση αυτής της απειλής, θα πρέπει να εφαρμοστούν πολιτικές και διαδικασίες, όπως ο διαχωρισμός του δικτύου, προκειμένου να αντιμετωπιστούν ο έλεγχος, η χρήση και η επίδρασή τους στο ευάλωτο επιχειρησιακό δίκτυο. Όσο περισσότερες συσκευές φέρνουν τα πληρώματα στο πλοίο, τόσο περισσότερα είναι τα ευάλωτα σημεία για τους κακόβουλους χρήστες, προκειμένου να φτάσουν στο δίκτυο του πλοίου. Κοινωνική μηχανική, εξαπάτηση, κλοπή ταυτότητας, δωροδοκία, και εκβιασμός αποτελούν τα κυριότερα προβλήματα για τη βιομηχανία. Είναι πιο δημοφιλής από ποτέ οι επιθέσεις που διενεργούνται από κακόβουλους χρήστες εναντίον επιχειρήσεων ή κυβερνήσεων σε όλο τον κόσμο για τρομοκρατία ή οικονομικούς λόγους.

Πρέπει να δοθεί ιδιαίτερη προσοχή όταν δεν υπάρχει έλεγχος για το ποιος έχει πρόσβαση στα συστήματα του πλοίου. Αυτό θα μπορούσε, για παράδειγμα, να συμβεί κατά τη διάρκεια του δεξαμενισμού ή κατά την παραλαβή ενός νέου πλοίου. Σε τέτοιες περιπτώσεις, δεν είναι γνωστό αν έχει απομείνει κακόβουλο λογισμικό στα συστήματα. Για το λόγο αυτό, συνίσταται να αφαιρούνται ευαίσθητα δεδομένα από το πλοίο και να γίνεται η εγκατάσταση τους κατά την επιστροφή στο πλοίο. Όπου είναι δυνατόν, τα συστήματα θα πρέπει να σαρωθούν για κακόβουλο λογισμικό πριν από τη χρήση. Τα OT συστήματα θα πρέπει να ελέγχονται για να εξασφαλισθεί ότι οι λειτουργίες είναι ακόμα ανέπαφες. Παρά τον κίνδυνο που προκύπτει, οι υπηρεσίες επικοινωνίας, είναι μία από τις πιο επιθυμητές λειτουργίες για το πλήρωμα του πλοίου. Το 75% των ναυτικών ανέφεραν ότι το επίπεδο συνδεσιμότητας που παρέχεται επί του πλοίου επηρέασε την απόφαση τους για την εταιρία στην οποία θα εργαστούν.

Κεφάλαιο 4.2.2: Εκπαίδευση και Ευαισθητοποίηση του πληρώματος

Η κατανόηση είναι μια κρίσιμη πτυχή της μείωσης του κινδύνου. Υπάρχουν θέματα και πιθανές απειλές ασφαλείας που πρέπει να γίνουν κατανοητά από τους εργαζόμενους, να αποκτήσουν την ικανότητα να τα αντιμετωπίσουν και να ανταποκριθούν όταν ο οργανισμός κινδυνεύει. Κάθε πλοίο ανεξάρτητα από το μέγεθος και τον τομέα στον οποίο δραστηριοποιείται είναι δυνητικά ευάλωτο, και οι απειλές είναι παρούσες και αυξάνονται. Αρχικά, για να αυξηθεί η ευαισθητοποίηση του πληρώματος, θα πρέπει να παρουσιάζονται όλοι οι πιθανοί φορείς επίθεσης και να καθορίζονται οι τρόποι αντιμετώπισης των τρωτών σημείων που προκαλούνται από την αμέλεια του πληρώματος. Είναι ζωτικής σημασίας να γνωρίζει όλο το πλήρωμα τις απειλές που μπορεί να εισαγάγει στο πλοίο:

- **E-mail:** Οι κίνδυνοι σχετικά με τα μηνύματα ηλεκτρονικού ταχυδρομείου και τις απάτες phishing θα πρέπει να δηλώνονται και τα παραδείγματα χρηστών που επιλέγουν κακόβουλους συνδέσμους πρέπει να προσομοιώνονται
- **Πλοήγηση στο Διαδίκτυο:** Η μη ασφαλής πλοήγηση στο Διαδίκτυο θα πρέπει να αποφεύγεται από το πλήρωμα. Κάθε μέλος του πλοίου θα πρέπει να είναι σε θέση να αναγνωρίζει μη

ασφαλείς ιστότοπους, να αποτρέπει και να μαθαίνει να αναφέρει ύποπτες ή κακόβουλες ιστοσελίδες

- **Χρήση Προσωπικών Συσκευών:** Οι συσκευές που χρησιμοποιούνται από το πλήρωμα δεν είναι πάντα συνδεδεμένες σε διαφορετικό δίκτυο από το επιχειρησιακό. Εάν αυτές οι συσκευές δεν ελεγμένες από antivirus μπορεί να δημιουργήσουν προβλήματα στο περιβάλλον στο οποίο συνδέονται
- **Εγκατάσταση Λογισμικού:** Κίνδυνοι που σχετίζονται με την εγκατάσταση και τη συντήρηση λογισμικού στο δίκτυο, ξεκινώντας από μολυσμένο υλικό (αφαιρούμενα μέσα) ή λογισμικό (μολυσμένο πακέτο)
- **Αφαιρούμενα Μέσα:** Τα μολυσμένα USB μπορούν να αποδειχθούν εξαιρετικά επικίνδυνα. Σήμερα τα USB δεν χρησιμοποιούνται μόνο για τη μεταφορά δεδομένων, αλλά και για την ενημέρωση κρίσιμων συστημάτων του πλοίου, όπως το σύστημα ECDIS. Έχουν καταγραφεί αρκετά περιστατικά καθυστερήσεων στο ταξίδι λόγω απώλειας των ηλεκτρονικών χαρτών, και αυτός είναι ο λόγος για τον οποίο οι εταιρείες διατηρούν τουλάχιστον 2 ή 3 αντίγραφα ασφαλείας στο πλοίο [44]. Είναι απαραίτητο να τεθούν σε εφαρμογή πολιτικές προστασίας για τα αφαιρούμενα μέσα πριν πραγματοποιηθεί η σύνδεση με τα συστήματα του πλοίου, και το πλήρωμα θα πρέπει να είναι ικανό να εντοπίζει και να αναφέρει ύποπτες ενέργειες
- **Μολυσμένοι Φορτιστές:** Σύμφωνα με τον DNV GL [30], υπήρξαν περιστατικά στα οποία το πλήρωμα συνέδεσε φορτιστές στις θύρες USB του επιχειρησιακού δικτύου και δημιούργησε τρωτά σημεία στο πλοίο [45]
- **Μέσα Κοινωνικής Δικτύωσης:** Η δύναμη της κοινωνικής δικτύωσης μπορεί να αποδειχθεί εξαιρετικά επικίνδυνη. Η εμπιστευτική ανταλλαγή πληροφοριών ή η αποθήκευση στο cloud, όπου τα δεδομένα είναι λιγότερο ελεγχόμενα και παρακολουθούνται, είναι δυνατόν να αποκαλύψουν πολύτιμες πληροφορίες για το πλοίο και να το καταστήσουν ευάλωτο σε απειλές. Υπάρχουν παραδείγματα όπου κατά τη διάρκεια μιας σύγκρουσης, μιας διαρροής λαδιού ή ενός ατυχήματος ενός μέλους του πληρώματος κατά τη διάρκεια του ταξιδιού, το προσωπικό αντί για την αντιμετώπιση της κατάστασης δημοσίευε φωτογραφίες στα μέσα κοινωνικής δικτύωσης βλάπτοντας τη φήμη της εταιρείας
- **Κοινωνική Μηχανική:** Η κοινωνική μηχανική είναι η τέχνη της χειραγώγησης ενός ατόμου, ή μιας ομάδας ανθρώπων, αποσκοπώντας στην παροχή πληροφοριών ή υπηρεσιών που σε διαφορετική περίπτωση δεν θα μπορούσαν να αποκτήσουν και χωρίζονται σε δύο κατηγορίες: 1) με βάση τον άνθρωπο και 2) τον υπολογιστή. Η πρώτη κατηγορία απαιτεί φυσική πρόσβαση στο θύμα μέσω αλληλεπίδρασης με συνομιλία, ηλεκτρονικό ταχυδρομείο ή τηλέφωνο. Ο στόχος της επίθεσης είναι συνήθως ένας κωδικός πρόσβασης ή εμπιστευτικές πληροφορίες, ισχυριζόμενος ότι είναι αξιόπιστος συνάδελφος ή διαχειριστής δικτύου. Αρκετά διαδομένα για τη βιομηχανία, αποτελούν παραδείγματα ανθρώπων που προσποιούνται ότι είναι προσωπικό τεχνικής υποστήριξης για πείσουν το πλήρωμα να τους χορηγήσει πρόσβαση στο επιχειρησιακό δίκτυο. Στη δεύτερη κατηγορία, οι επιθέσεις πραγματοποιούνται με τη χρήση ενός υπολογιστή ή άλλης συσκευής επεξεργασίας δεδομένων και ειδικά κατασκευασμένα αναδυόμενα παράθυρα, με σκοπό την εξαπάτηση του χρήστη ώστε να επισκεφθεί μια κακόβουλη ιστοσελίδα ή να απαντήσει σε κακόβουλα μηνύματα SMS.

Θα πρέπει να αναλυθούν οι κίνδυνοι που σχετίζονται με τη χρήση του Διαδικτύου, συμπεριλαμβανομένης της περιήγησης στο Διαδίκτυο και της χρήσης των μέσων κοινωνικής δικτύωσης. Επιπλέον, είναι εξαιρετικά σημαντικό η εταιρεία να καθορίσει τους κινδύνους που σχετίζονται με E-mails και επιθέσεις phishing. Επίσης, θα πρέπει να παρουσιαστούν παραδείγματα εξαπάτησης καθώς και πιθανές συνέπειες των χρηστών που επιλέγουν σύνδεσμο σε μια κακόβουλη ιστοσελίδα. Από την εκπαίδευση δεν θα πρέπει να λείπουν οι αναφορές στις πολιτικές προστασίας από ιούς για τις προσωπικές συσκευές των εργαζομένων. Οι μη ενημερωμένες συσκευές μπορούν να αποτελέσουν πηγή κινδύνου για το περιβάλλον στο οποίο συνδέονται. Το πλήρωμα και το προσωπικό θα πρέπει να γνωρίζουν ότι χρησιμοποιώντας ευάλωτο υλικό ή λογισμικό, ο κίνδυνος μπορεί να εξαπλωθεί σε όλο το δίκτυο.

Κεφάλαιο 4.2.3: Ανθρώπινος Παράγοντας vs Αδυναμίες της Τεχνολογίας

Σε ένα σύγχρονο πλοίο, Τα IT συστήματα, βοηθούν ή ακόμη και αντικαθιστούν τον παραδοσιακό Ναυτικό και τα καθήκοντα που βασίζονται στην ξηρά και καθιστούν το πλοίο λειτουργικό και ασφαλές για να εκτελεί τις εμπορικές ανάγκες της βιομηχανίας. Για να εφαρμοστούν αυτές οι δυνατότητες, η βιομηχανία θα πρέπει να επικεντρωθεί στο σχεδιασμό των πλοίων με σκοπό την αντιμετώπιση των ζητημάτων που δημιουργούνται από την αλληλεπίδραση των συστημάτων με τα πληρώματα. Ο σχεδιασμός, η κατασκευή και η διαχείριση των IT συστημάτων πρέπει να επιτρέπουν τόσο στους ναυτικούς όσο και στο προσωπικό της ξηράς να εργάζονται με ασφάλεια και αποτελεσματικότητα. Τα καθήκοντα τόσο των πληρωμάτων όσο και του προσωπικού της ξηράς πρέπει να επανεξετάζονται προκειμένου να λαμβάνουν υπόψη τις νέες ή τροποποιημένες αρμοδιότητες, συμπεριλαμβανομένης της υποστήριξης και συντήρησης των συστημάτων. Επιπλέον, πρέπει να εξετάζεται η επίδραση όλων των παραπάνω αλλαγών στην απόδοση του προσωπικού. Τέλος, οι δραστηριότητες του πλοίου πρέπει να παρακολουθούνται για να διασφαλιστεί ότι το πλήρωμα διαχειρίζεται τα συστήματα αποδοτικά και σύμφωνα με τις προτάσεις του κατασκευαστή.

Η αντιμετώπιση των παραπάνω προκλήσεων απαιτεί μια δομημένη, ανθρωποκεντρική προσέγγιση για την ανάπτυξη και τη λειτουργία του συστήματος – όπως ορίζεται στο πρότυπο ISO 9241-210 (Human-Centred Design - HCD). Ένα πλοίο σχεδιασμένο κατά το πρότυπο HCD είναι ένα ασφαλέστερο και πιο παραγωγικό για το πλήρωμα [46].

Εν κατακλείδι, είναι συχνό φαινόμενο να κατηγορούνται οι άνθρωποι που αφήνουν τους κακόβουλους χρήστες να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα δίκτυα πλοίων. Οι διαχειριστές των συστημάτων και οι κατασκευαστές θα πρέπει να εξετάζουν όλες τις παραπάνω πτυχές πριν από τον σχεδιασμό μιας δομής. Η ασφάλεια των δικτύων δεν πρέπει να στηρίζεται στον ανθρώπινο παράγοντα, καθώς είναι λανθασμένη πρακτική ένα σύστημα να εξαρτάται από το χρήστη. Αντίθετα, τα συστήματα πρέπει να στηρίζουν τους χρήστες τους.

Κεφάλαιο 4.3: Παράγοντες Απειλής

Υπάρχουν διαφορετικοί παράγοντες απειλής με ποικίλα κίνητρα για την εκτέλεση κακόβουλων πράξεων εναντίον μιας εταιρείας. Το αξιοσημείωτο είναι ότι ορισμένες ομάδες έχουν ως κίνητρο τη

δημιουργία εσόδων από το έγκλημα στον κυβερνοχώρο, ενώ άλλες ομάδες παρακινούνται από πολιτικά, ιδεολογικά ή θρησκευτικά αίτια. Η επιτυχία της επίθεσης εξαρτάται από το σκοπό και το ενδιαφέρον των ομάδων αυτών [43].

Κεφάλαιο 4.3.1: Ακτιβιστές

Οι ομάδες αυτές υποκινούνται από ιδεολογικά κίνητρα και συνήθως δρουν σχηματίζοντας ομάδες. Συχνά οι ενέργειές τους είναι αποτέλεσμα διαμαρτυρίας, οι οποίες μπορεί να έχουν ως στόχο την διατάραξη της λειτουργίας των συστημάτων ή την απόκτηση εμπιστευτικών και ευαίσθητων πληροφοριών, στοχεύοντας στη δυσφήμηση του στόχους τους. Ο αντίκτυπος των μικρών αυτών ομάδων μπορεί να αυξηθεί σημαντικά όταν στρατολογούν τρίτα μέρη να συμμετάσχουν, επιτρέποντας την εγκατάσταση κακόβουλου λογισμικού στους υπολογιστές τους και δημιουργώντας με αυτόν τον τρόπο ευπάθειες στα συστήματα. Συγκεκριμένα, στον τομέα της ναυτιλίας, οι επιτιθέμενοι αναζητούν δημοσιότητα ή να δημιουργήσουν τετελεσμένα γεγονότα για ένα συγκεκριμένο σκοπό ή για να προκαλέσουν, για παράδειγμα, την αποτροπή της διακίνησης συγκεκριμένων φορτίων ή την διατάραξη της λειτουργίας του πλοίου. Στόχος των ομάδων αυτών μπορεί να είναι είτε το ίδιο το πλοίο, είτε ο διαχειριστής του πλοίου, ή ακόμα και οι πελάτες του οργανισμού.

Κεφάλαιο 4.3.2: Ανταγωνιστές

Στην κατηγορία αυτή ανήκουν, συνήθως, μεγάλες εταιρείες που επιδιώκουν να δημιουργήσουν ανταγωνιστικό πλεονέκτημα. Μπορούν να ενεργούν απευθείας ή μέσω τρίτων, με σκοπό να βλάψουν έναν ανταγωνιστή κλέβοντας πνευματική ιδιοκτησία, συλλέγοντας ανταγωνιστικές πληροφορίες για προσφορές ή διαταράσσοντας την ομαλή λειτουργία του οργανισμού για να προκαλέσουν οικονομική ζημία ή πλήξη της φήμης. Ανάλογα με το μέγεθος, τον τομέα, τη γεωγραφική θέση και την πολυπλοκότητα των δυνατοτήτων της, η ανταγωνίστρια εταιρεία μπορεί να είναι σε θέση να εκτελέσει εξελιγμένες κακόβουλες δραστηριότητες για να στοχεύσει και να διεισδύσει στους ανταγωνιστές της.

Κεφάλαιο 4.3.3: Κυβερνό- έγκλημα

Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν προηγμένες μεθόδους, εργαλεία και λογισμικό για να επωφεληθούν από τις παράνομες δραστηριότητές τους. Πρόκειται για εγκληματικές ομάδες υψηλής ειδίκευσης που προσπαθούν να εκμεταλλευτούν ένα ευρύ φάσμα πόρων, χρησιμοποιώντας εξελιγμένες τεχνικές. Κίνητρο συνήθως αποτελεί το κέρδος κυρίως μέσω της απάτης και της κλοπής, καθώς και η τάση για “επίδειξη δεξιοτήτων”. Ωστόσο, οι εγκληματικές αυτές δραστηριότητες περιλαμβάνουν εκβιασμό μέσω της κρυπτογράφησης δεδομένων ή επιθέσεις άρνησης εξυπηρέτησης στις εταιρικές ιστοσελίδες. Οι μέθοδοι και οι τεχνικές εξελίσσονται με την πρόοδο της, αφορούν όμως κυρίως την ηλεκτρονική χρηματοδότηση, το ηλεκτρονικό εμπόριο και τις ηλεκτρονικές πληρωμές. Η ανωνυμία, η κρυπτογράφηση και τα εικονικά νομίσματα, όπως το BitCoin, κάνουν τους εγκληματίες δύσκολο να εντοπιστούν και τις επιθέσεις τους μη ανιχνεύσιμες. Όσον αφορά τους λιμένες, οι ομάδες αυτές επιδιώκουν την παρενόχληση της ομαλής λειτουργίας τους ή την πρόσβαση σε πληροφορίες σχετικά με τις αποστολές φορτίου ή τις ρυθμίσεις ασφαλείας με σκοπό τη μελλοντική τέλεση εγκληματικών δραστηριοτήτων σε αυτούς τους χώρους. Στην πραγματικότητα έχει δημιουργηθεί μια

επιχείρηση γύρω από το κυβερνό- έγκλημα που μπορεί δυνητικά να μετατραπεί σε κατασκοπεία [46]. Η πολυπλοκότητα του κακόβουλου λογισμικού που χρησιμοποιείται από αυτές τις ομάδες αυξάνεται και υπάρχουν ενδείξεις για δημιουργία μίας αγοράς σχετικής με το κυβερνό- έγκλημα. Οι προγραμματιστές δημιουργούν, προμηθεύουν και χρησιμοποιούν εξελιγμένα εργαλεία κακόβουλης λειτουργίας σε εμπορική βάση, καθιστώντας τα εργαλεία τους διαθέσιμα σε τρίτους κακόβουλους χρήστες.

Κεφάλαιο 4.3.4: Τρομοκράτες

Η τρομοκρατία στον κυβερνοχώρο αποτελεί μεγάλο κίνδυνο κυρίως λόγω της αυξημένης εξάρτησης από των οργανισμών από τα συστήματα πληροφορικής. Οι τρομοκράτες γίνονται όλο και περισσότερο γνώστες των νέων τεχνολογιών και έχουν ως κύριο σκοπό την εξάπλωση της δραστηριότητας τους. Ο στόχος πίσω από μια τέτοια επίθεση είναι:

- Να αποκτήσουν τον έλεγχο κρίσιμης υποδομής,
- Να διαδώσουν ένα κακόβουλο λογισμικό,
- Να κρυπτογραφήσουν ή να κλέψουν εμπιστευτικά δεδομένα,
- Να διαπράξουν απάτη

Γενικά, να εκτελέσουν σχεδόν οποιαδήποτε πράξη με σκοπό την καταστροφή των περιουσιακών στοιχείων του οργανισμού. Υπάρχουν περιπτώσεις όπου καλά χρηματοδοτούμενες ομάδες θα μπορούσαν να επωφεληθούν από τις υπηρεσίες που προσφέρουν οι κυβερνό- εγκληματίες, να αναζητήσουν υποστήριξη από κρατικές υπηρεσίες και να υιοθετήσουν αυτές τις μεθόδους επίθεσης. Με την εκτεταμένη χρήση ηλεκτρονικών συστημάτων στη ναυτιλιακή βιομηχανία, οι τρομοκρατικές ομάδες θα μπορούσαν να βασιστούν στα διαθέσιμα εργαλεία για να διαταράξουν ή να βλάψουν τα πλοία επιτιθέμενοι στα πλοία ή/και στα συνδεδεμένα συστήματα στην ξηρά. Οι ομάδες αυτές μπορούν επίσης να εκμεταλλευτούν τα μη ασφαλή δεδομένα των πλοίων για να επιτρέψουν την απομακρυσμένη εχθρική αναγνώριση των στόχων, μειώνοντας έτσι το χρόνο που χρειάζονται για να πετύχουν το στόχο τους. Ένα πλοίο με βενζίνη θα μπορούσε να είναι ένας εξαιρετικά ελκυστικός στόχος για τρομοκράτες που θέλουν να σπείρουν το φόβο και να προκαλέσουν οικονομικές απώλειες σε ένα λιμάνι ή σε ένα άλλο πλοίο.

Κεφάλαιο 4.3.5: Κρατικά Υποκινούμενες Επιθέσεις

Σύμφωνα με την έκθεση του φόρουμ για την ασφάλεια πληροφοριών "Η τρομοκρατία υπό την αιγίδα του κράτους θα αποτελέσει κορυφαία απειλή μέχρι το 2020 – και όλοι οι οργανισμοί θα πρέπει να προετοιμαστούν κατάλληλα". Είναι αποδεκτό ότι ορισμένα κράτη συμμετέχουν ενεργά σε επιθέσεις στον κυβερνοχώρο σε ένα ευρύ φάσμα οργανισμών, προκειμένου να αποκτήσουν κρατικές πληροφορίες ή ευαίσθητες βιομηχανικές πληροφορίες. Μπορούν επίσης να απειλήσουν τη διαθεσιμότητα κρίσιμης υποδομής σε άλλα κράτη. Κατά τη διάρκεια περιόδων αυξημένων εντάσεων ή συγκρούσεων, αυτές οι δραστηριότητες ενδέχεται να περιλαμβάνουν πιο εκτεταμένες επιθέσεις, όπως αποδεικνύεται από κακόβουλα λογισμικά όπως το Stuxnet και το WannaCry.

Οι επιθέσεις αυτές πραγματοποιούνται από ομάδες που απειλούν ή επιτίθενται σε επιχειρήσεις και υποδομές άλλων εθνικών κρατών. Οι επιτιθέμενοι μπορούν να θεωρηθούν ως ένας τύπος hacktivist, αλλά το ενδιαφέρον τους είναι η υποστήριξη ενός εθνικού κράτους και ως εκ τούτου, μπορούν να χρησιμοποιήσουν σημαντική και εξειδικευμένη τεχνική υποστήριξη από αυτό το κράτος.

Κεφάλαιο 5: Χαρτογράφηση των Επιθέσεων

Κεφάλαιο 5.1: Στοιχεία του Πλοίου

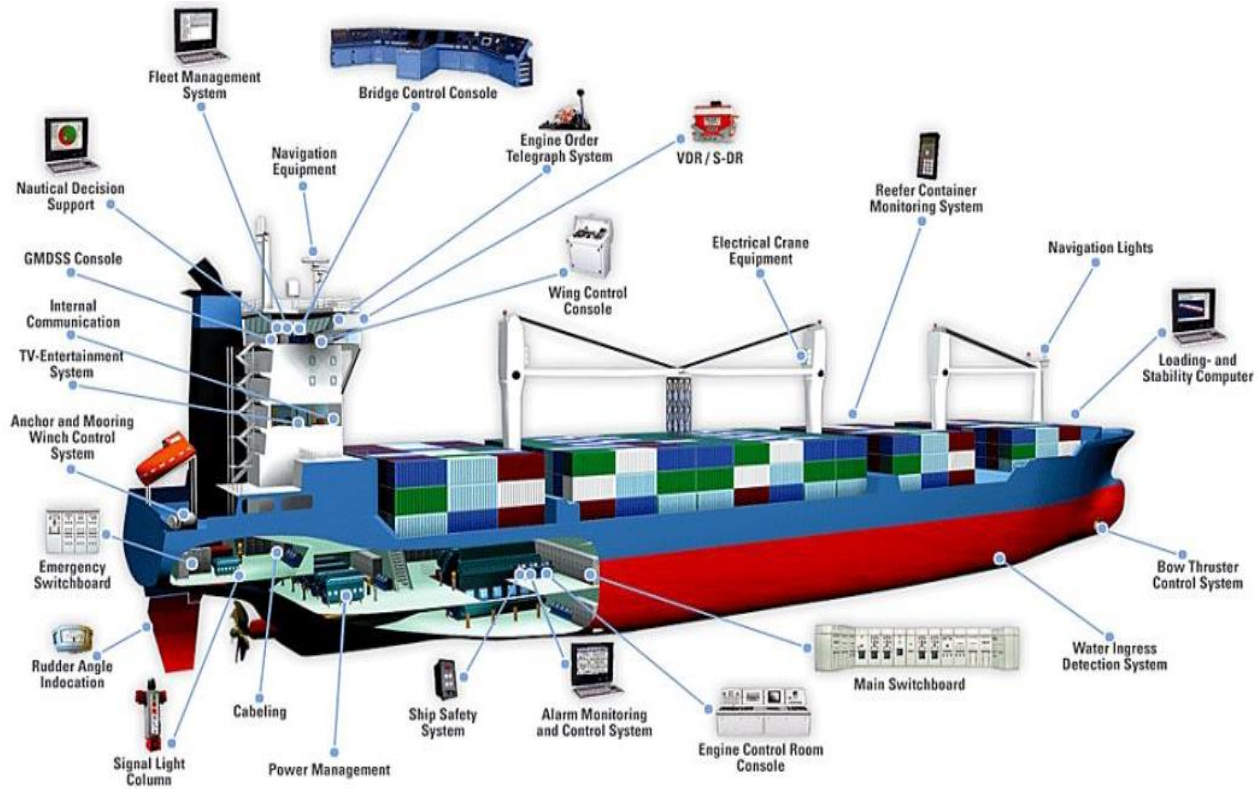
Για να αντιμετωπιστεί το συνεχώς αυξανόμενο επίπεδο απειλής, είναι απαραίτητο να εντοπιστούν τα συστήματα που είναι κρίσιμα για την ασφαλή λειτουργία του πλοίου, και να διασφαλιστεί ότι θα είναι λειτουργικά ακόμα και όταν παρουσιαστεί κάποια δυσλειτουργία. Για να επιτευχθεί αυτό, πρέπει να εντοπιστούν τα συστήματα που είναι κρίσιμα για τη λειτουργία του οργανισμού. Ο καθορισμός των κρίσιμων συστημάτων μπορεί να γίνει με μια προσέγγιση βασισμένη στον κίνδυνο ή με τη χρήση προτύπων όπως το πρότυπο του Εθνικού Ινστιτούτου προτύπων και τεχνολογίας (National Institute of Standards and Technology – NISYT), όπως είναι το SP 800-64 για τον κύκλο ζωής του συστήματος [49] ή από τις οδηγίες της BIMCO. Οι διασυνδέσεις μεταξύ των συστημάτων έχουν αυξήσει την πολυπλοκότητα και αυτό πρέπει να εξετάζεται κατά τον προσδιορισμό της κρισιμότητας – για παράδειγμα, στα δίκτυα επικοινωνιών ενός πλοίου μπορεί να έχει πρόσβαση ο κατασκευαστής. Επιπλέον, εάν χρησιμοποιούνται εμπορικά προϊόντα, υποσυστήματα ή προγράμματα, πρέπει να διασφαλίζεται ότι πληρούνται οι απαιτήσεις που έχουν καθοριστεί.

Μια τυπική προσέγγιση βασισμένη στον κίνδυνο μπορεί να είναι η παρακάτω:

1. Προσδιορισμός του συστήματος ή των υποσυστημάτων και τον τρόπο λειτουργίας τους
2. Προσδιορισμός των πιθανών αποτυχιών των συστημάτων και τις αιτίες τους
3. Αξιολόγηση των αποτελεσμάτων των αποτυχιών στο σύστημα
4. Προσδιορισμός μέτρων για τη αντιμετώπιση των κινδύνων
5. Προσδιορισμός μέτρων για μετριασμό των επιπτώσεων της αποτυχίας
6. Προσδιορισμός των αναγκαίων για την απόδειξη των συμπερασμάτων

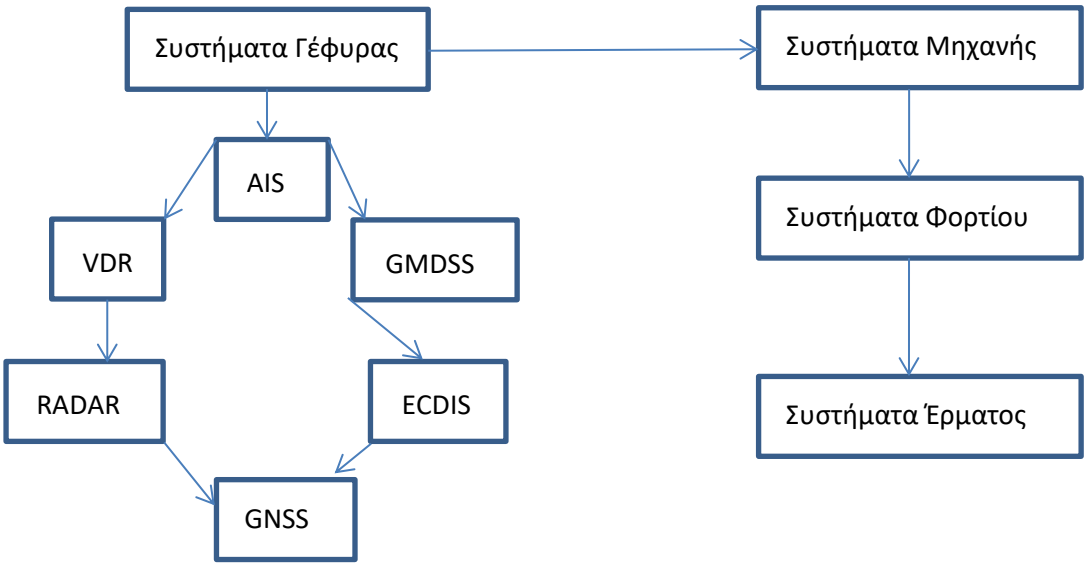
ID	Όνομα έργου	Κόστος	Συστήματα
2018-TE-2	**Cyber-security for OT systems**	**TBA**	**Εφαρμογή σε**: Συστήματα Εντοπισμού (ECDIS, AIS, Radar, GPS), Συστήματα Επικοινωνιών (INM-C, VHF, SATCOM), Συστήματα Ασφάλειας (VDR, AMS, Fire detection ,BNWAS, Gas detection), Συστήματα Διαχείρισης Ελέγχου (Maneuvering & steering), Συστήματα Παραγωγής (Cargo management, PMS), IT Συστήματα (Telemetry, Hermes)

Πίνακας 6: Προσέγγιση εστιασμένη στον κίνδυνο

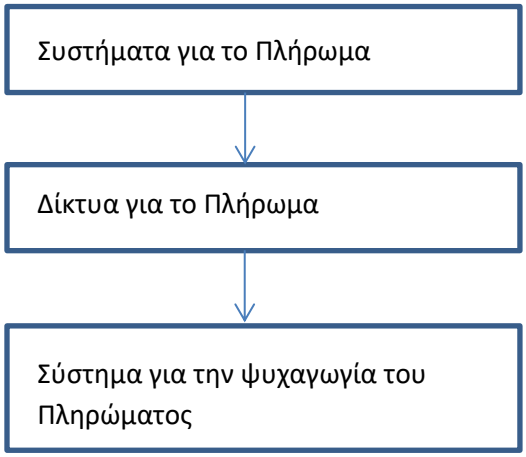


Εικόνα 11: ΟΤ Συστήματα

Τα σχήματα 5.1 και 5.2 είναι μια γενική απεικόνιση της ενσωμάτωσης κρίσιμων και μη κρίσιμων συστημάτων ενός πλοίου. Τα συστήματα αυτά δεν θα πρέπει να συνδέονται στο ίδιο δίκτυο. Το επιχειρησιακό δίκτυο θα πρέπει να περιέχει όλα τα κρίσιμα, για τη λειτουργία του πλοίου, συστήματα ενώ το δίκτυο ψυχαγωγίας τα μη κρίσιμα. Το δίκτυο ψυχαγωγίας είναι πιο ευάλωτο σε επιθέσεις και θα πρέπει να αντιμετωπίζεται διαφορετικά από το επιχειρησιακό δίκτυο.



Εικόνα 12: Κρίσιμα Συστήματα στο Πλοίο



Εικόνα 13: Μη Κρίσιμα Συστήματα στο Πλοίο

Κεφάλαιο 5.2: Integrated Bridge System (IBS)

Το ολοκληρωμένο σύστημα γέφυρας διαχειρίζεται όλα τα εξαρτήματα της γέφυρας. Παρέχει κεντρική πρόσβαση στις πληροφορίες από όλα τα εξαρτήματα της γέφυρας.

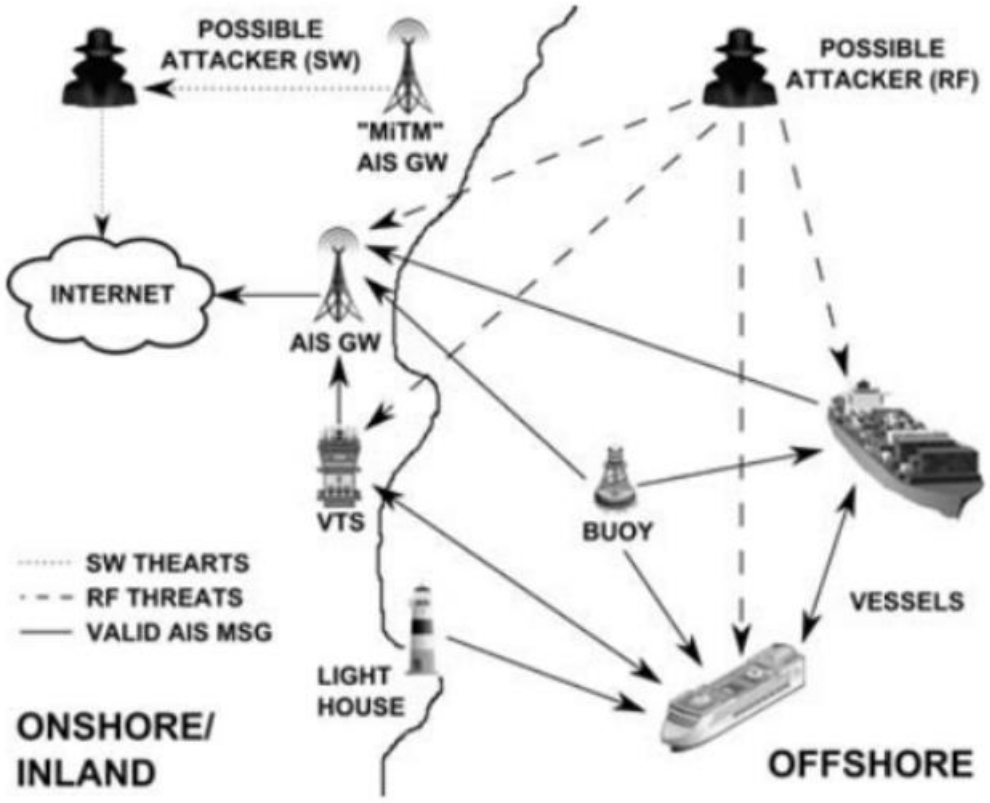
Κεφάλαιο 5.2.1: Automatic Identification System (AIS)

Το σύστημα αυτόματης ταυτοποίησης είναι ένα σύστημα που χρησιμοποιείται συνήθως στη ναυτιλιακή βιομηχανία για την παρακολούθηση της κυκλοφορίας των πλοίων. Το σύστημα έγινε υποχρεωτικό το 2002, για όλα τα πλοία που έχουν χωρητικότητα τουλάχιστον 300 τόνων και όλα τα επιβατηγά πλοία ανεξάρτητα του μεγέθους τους. Το AIS λειτουργεί χρησιμοποιώντας τις συντεταγμένες από το GPS και ανταλλάσσοντας, μέσω ραδιοφωνικών μεταδόσεων, πληροφορίες σε πραγματικό χρόνο μεταξύ πλοίων και ναυτιλιακών αρχών. Επιπλέον, τα δεδομένα από το AIS συλλέγονται και μεταδίδονται στους παρόχους (Vessel Finder, Marine Traffic, AisHub). Η παραπάνω διαδικασία προσφέρει απεικόνιση, παρακολούθηση και αναφορά της διαθεσιμότητας των πλοίων. Το σύστημα χρησιμοποιείται για να βοηθήσει τα πλοία να αποφύγουν τις συγκρούσεις, να ενημερώσει τις λιμενικές και ναυτικές αρχές σχετικά με τη θέση τους, να μετρήσει την απόσταση από τα άλλα πλοία που πλέουν στην περιοχή και να εξασφαλίσει την ασφάλεια στη θάλασσα παρακολουθώντας την κυκλοφορία. Ορισμένα από τα δεδομένα που λαμβάνει και μεταδίδει η συσκευή AIS είναι το όνομα του πλοίου, ο αριθμός IMO του πλοίου, το μέγεθος, ο τύπος, η σημαία, η ταχύτητα, το επόμενο λιμάνι και η εκτιμώμενη ώρα άφιξης. Κάποια από τα πλεονεκτήματα της χρήσης του AIS είναι οι έρευνες σχετικά με τα ατυχήματα και οι επιχειρήσεις έρευνας και διάσωσης, όπως οι αναμεταδότες AIS- SART’s (Search and Rescue Transpoders), αδιάβροχες συσκευές που προορίζονται για επείγουσες καταστάσεις, κυρίως για να βοηθήσουν στην ανίχνευση της θέσης των πλοίων που βρίσκονται σε κίνδυνο. Η επικοινωνία διεξάγεται σε ραδιοσυχνότητες (RF) και το σύστημα δεν χρησιμοποιεί ελέγχους ταυτότητας ή ακεραιότητας, επομένως οποιοσδήποτε χρησιμοποιώντας ένα απλό δέκτη RF έχει τη δυνατότητα να λάβει αυτά τα μηνύματα. Το σύστημα είναι ευάλωτο σε παρεμβολές σήματος, σε ψευδή ανταλλαγή πληροφοριών και σε κακόβουλο λογισμικό, καθώς η σύνδεση με τους παρόχους AIS διενεργείται μέσω του Διαδικτύου. Επίσης, είναι πολύ σημαντικό το πρόβλημα της εμπιστευτικότητας, καθώς μπορεί να γίνει επιλογή των πλοίων από τους πειρατές.

Όπως φαίνεται στην Εικόνα 5.3 ακόμη και μέσω RF οι επιτιθέμενοι έχουν 4 φορείς επίθεσης:

1. Πομπός AIS
2. Υπηρεσία Κυκλοφορίας των Πλοίων
3. Πλοία

Οι αναγνωρισμένες ευπάθειες είναι αρκετές. Το AIS μπορεί να χρησιμοποιηθεί για την αναμετάδοση "κατασκευασμένων" πληροφοριών. Στόχος αυτών των ψευδών μηνυμάτων (σήμα κινδύνου, ψευδής θέση πλοίου) είναι να προσελκύσουν την προσοχή και να παγιδεύσουν τα στοχευμένα πλοία. Ο επιτιθέμενος, για παράδειγμα, μπορεί να στείλει μηνύματα που θα μπορούσαν να μιμούνται τη θέση ενός πραγματικού πλοίου, ή ακόμη και να δημιουργήσει ένα ψεύτικο πλοίο και να του αποδώσει μία εικονική πορεία. Αυτή η τεχνική ονομάζεται AIS Spoofing. Με αυτόν τον τρόπο, οι επιτιθέμενοι μπορούν να ενεργοποιήσουν ειδοποιήσεις αναζήτησης και διάσωσης για να δελεάσουν ένα πλοίο και να το οδηγήσουν σε έναν εχθρικό και ελεγχόμενο θαλάσσιο χώρο. Οι επιτιθέμενοι μπορούν να καταγράφουν και να αποθηκεύουν δεδομένα AIS και να μεταδίδουν πλαστά μηνύματα οδηγώντας πλοία εκτός πορείας.



Εικόνα 14: Επίθεση σε AIS

Επιπλέον, οι επιτιθέμενοι μπορούν να τροποποιήσουν τα δεδομένα από το AIS, όπως τη θέση του πλοίου, το λιμάνι ή την εκτιμώμενη ώρα άφιξης κλπ., υποβάλλοντας τα στην υπηρεσία AIS. Επιπλέον, δεδομένου ότι δεν υπάρχουν έλεγχοι ταυτότητας και ακεραιότητας, το σύστημα AIS είναι ευάλωτο σε επιθέσεις άρνησης εξυπηρέτησης (DDoS). Δεδομένου ότι στη θάλασσα ενεργοποιείται το AIS

μεταδίδοντας σήμα για έρευνα και διάσωση ανθρώπων που βρίσκονται σε κίνδυνο, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το σύστημα αυτό για να μεταδώσουν επιθυμητές συντεταγμένες. Τα πλοία απαιτείται από το νόμο να συμμετέχουν σε μια επιχείρηση έρευνας και διάσωσης.

Κεφάλαιο 5.2.2: Electronic Chart Display Information System (ECDIS)

Ένα ηλεκτρονικό σύστημα εμφάνισης χαρτών (ECDIS) είναι ένα σύστημα απεικόνισης εμφάνισης πληροφοριών και γραφημάτων που αντικατέστησε τους παραδοσιακούς χάρτες στα πλοία. Το ECDIS δείχνει τη θέση του πλοίου σε πραγματικό χρόνο σε ένα χάρτη που εμφανίζεται σε μια οθόνη. Παρέχει στους ναυτικούς όλες τις πληροφορίες που μπορεί να χρειαστούν για να ταξιδέψουν με ασφάλεια, όπως η στιγμιαία θέση του πλοίου (GPS), τα εμπόδια και οι φάροι. Επίσης, συνδέεται με το σύστημα αυτόματης σχεδίασης (Automatic Radar Plotting Aid - ARPA) και όλα τα πλοία υποχρεούνται (από τον Αύγουστο του 2017) να το διαθέτουν σύμφωνα με τις οδηγίες του IMO. Τα πλοία θα πρέπει να διατηρούν χάρτες για τον προγραμματισμό και την παρακολούθηση της πορείας τους.

Το ECDIS βασίζεται σε ένα σύστημα χαρτογράφησης που χρησιμοποιεί ένα IT σύστημα για την ψηφιακή εμφάνιση των ναυτικών διαγραμμάτων και την ακριβή θέση του πλοίου.

Τα δεδομένα από το ECDIS σχετίζονται με:

- Τις οδούς ναυσιπλοΐας
- Τις καιρικές συνθήκες
- Τις τελευταίες ανακοινώσεις προς ναυτιλλόμενους (NAVTEX)

Το ECDIS παρουσιάζει ευπάθειες στο λογισμικό του συστήματος που θα μπορούσαν να οδηγήσουν σε καταστροφικά αποτελέσματα για τα πλοία. Δεδομένης της εξάρτησης του συστήματος στο λογισμικό, το ECDIS είναι ευάλωτο σε επιθέσεις Malware. Οι ηλεκτρονικοί χάρτες, θα μπορούσαν επίσης να αναβαθμιστούν μέσω αφαιρούμενων δίσκων, οπότε σημαντικό κίνδυνο αποτελούν οι ιοί. Το προηγούμενο περιστατικό αποτελεί έναν κοινό τρόπο επίθεσης απέναντι στο ECDIS και θα μπορούσε να προκαλέσει αρκετά σημαντικά προβλήματα στη λειτουργία του οργανισμού. Η μικρότερη επίπτωση θα μπορούσε να είναι μία μικρή καθυστέρηση στο δρομολόγιο του πλοίου - μέχρι τη συνολική καταστροφή του συστήματος, και οι επιπτώσεις να είναι πολύ σημαντικές είτε σε οικονομικούς όρους είτε στη φήμη του οργανισμού.

Οι ευπάθειες του συστήματος μπορεί να είναι:

1. Το χρησιμοποιούμενο μέσο για την ενημέρωση του συστήματος (CD / USB stick / Internet connection)
2. Η έλλειψη ενημέρωσης του λειτουργικού συστήματος του σταθμού εργασίας
3. Αυτό το σύστημα είναι συνδεδεμένο με διάφορους αισθητήρες του πλοίου: ραντάρ, AIS, ταχύμετρο, ανεμόμετρο κλπ. Οι αισθητήρες αυτοί συχνά συνδέονται σε ένα τοπικό δίκτυο στο πλοίο

Ο ΙΜΟ λαμβάνοντας υπόψη τους κινδύνους που προκύπτουν από την αποτυχία του ECDIS απαίτησε την ύπαρξη εφεδρικών ηλεκτρονικών χαρτών στο πλοίο. Αυτά τα αντίγραφα ασφαλείας δεν ικανοποιούν ολοκληρωμένα τη λειτουργία του ECDIS, ως εκ τούτου, θα πρέπει να χρησιμοποιούνται μαζί με τους παραδοσιακούς χάρτες. Πολλές ναυτιλιακές εταιρείες για να ελαχιστοποιήσουν τον κίνδυνο αποτυχίας του ECDIS, επιλέγουν να εγκαταστήσουν ένα ολοκληρωμένο δεύτερο σύστημα ECDIS στο πλοίο.

Εικόνα 15: ECDIS

Κεφάλαιο 5.2.3: Voyage Data Recorder (VDR)

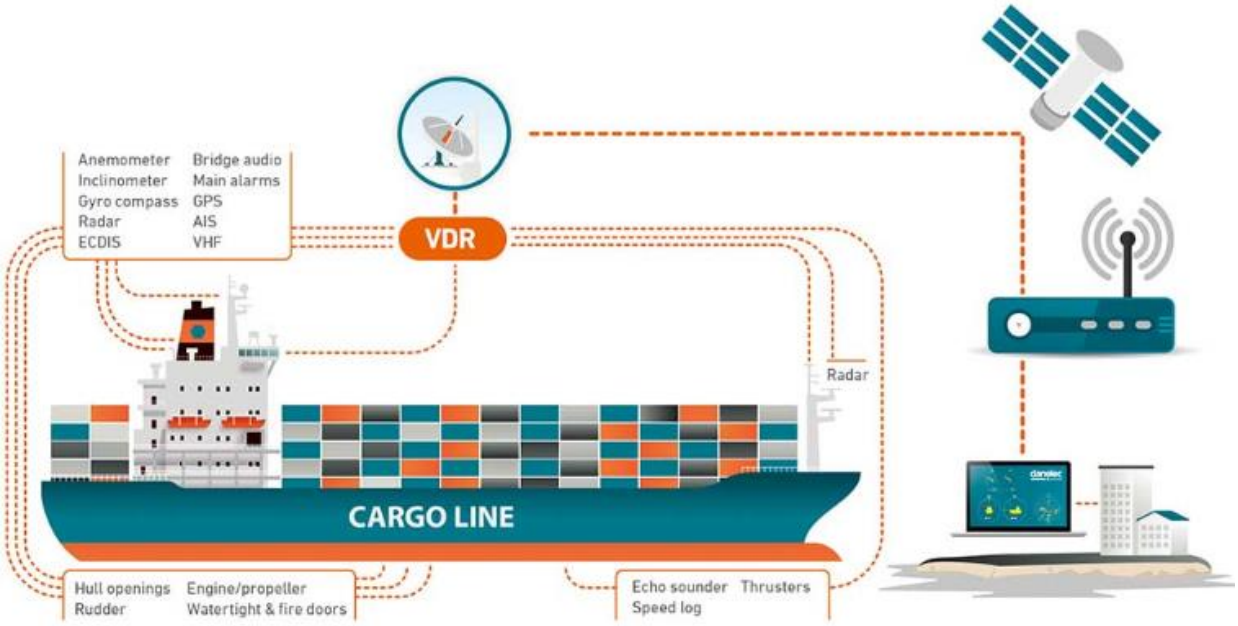
Το σύστημα καταγραφής δεδομένων ταξιδιού είναι το "Μαύρο κουτί των αεροπλάνων". Είναι υποχρεωτικό από την 1η Ιουλίου 2002 για όλα τα επιβατηγά πλοία και φορτηγά πλοία με φορτίο άνω των 3.000 τόνων. Το σύστημα αυτό έχει ως στόχο την ανάλυση των καταστάσεων που οδήγησαν σε ατύχημα, εξετάζοντας τα καταγεγραμμένα δεδομένα.

Οι τυπικές ρυθμίσεις ενός VDR είναι οι εξής:

1. Η μονάδα απόκτησης δεδομένων είναι η καρδιά του συστήματος: Λειτουργεί στη ζώνη συχνοτήτων VHF, Δέχεται δεδομένα από ραντάρ, διαθέτει σκληρό δίσκο ή USB stick, έχει αυτόνομη μπαταρία έκτακτης ανάγκης, μικρόφωνα, δυνατότητα εγγραφής δεδομένων, μονάδα συναγερμού γέφυρας (Bridge Alarm Unit - BAU), μονάδα διασύνδεσης αισθητήρων (Sensor Interface Unit - SIU) που συλλέγει όλα τα άλλα δεδομένα, τα κωδικοποιεί και τα στέλνει στη μονάδα απόκτησης δεδομένων
2. Καταγραφή Δεδομένων: Το σύστημα αυτό καταγράφει την ημερομηνία και την ώρα, την τοποθεσία του πλοίου, την ταχύτητα, τη γυροπυξίδα, τη μαγνητική πυξίδα, την εικόνα του ραντάρ, τις συνομιλίες στη γέφυρα του πλοίου, τις ραδιοεπικοινωνίες, τις βασικές

προειδοποιήσεις (πυρκαγιά, κατάσταση μηχανοστασίου κλπ), την κατάσταση των υδατοστεγών θυρών και των θυρών πυρκαγιάς, τη γωνία του πηδαλίου, την πρόωση του πλοίου, την πραγματική ή σχετική ταχύτητα ανέμου

Ακριβώς όπως το σύστημα ECDIS, του VDR έχει τις ίδιες ευπάθειες.



Εικόνα 16: VDR

Κεφάλαιο 5.2.4: Global Navigation Satellite System (GNSS)

Το παγκόσμιο δορυφορικό σύστημα πλοήγησης, μέσω ενός συνόλου δορυφόρων και ενός δέκτη, εμφανίζει τη θέση (2D και 3D), την ταχύτητα του πλοίου, τη διαδρομή και την ώρα. Ως εκ τούτου, επιτρέπει τον προσανατολισμό και την πλοήγηση στη θάλασσα. Υπάρχουν διάφοροι τύποι συστημάτων GNSS στον κόσμο σήμερα. Το σύστημα προσφέρει παγκόσμια κάλυψη, και αυτό που χρησιμοποιείται περισσότερο είναι το GPS που διαθέτει 24 δορυφόρους σε υψόμετρο 20.000 χιλιομέτρων και μετατοπίζονται σε 6 σχεδόν κυκλικές τροχιές με κλίση στις 55 ° στον Ισημερινό. Η λειτουργία του βασίζεται σε αλγόριθμους υπολογισμού της απόστασης μεταξύ του δέκτη GPS και αρκετών δορυφόρων. Η ακρίβεια του GPS μπορεί να φτάσει τα 10 μέτρα, ωστόσο η ατμοσφαιρική αναταραχή μπορεί να μειώσει αυτή την ακρίβεια. Η κρυπτογράφηση δεν προστατεύει τα δορυφορικά σήματα. Είναι, επομένως, δυνατόν να γίνει παρεμβολή και τροποποίηση του σήματος.

Μερικές από τις ευπάθειες του συστήματος αναφέρονται παρακάτω:

1. Ένα αδύναμο σήμα
2. Η πιθανότητα ακούσιας παρεμβολής
3. Η πιθανότητα εσκεμμένης παρεμβολής
4. Τεχνική ανεπάρκεια του δορυφορικού σχηματισμού

Κεφάλαιο 5.2.5: Radio Detection and Ranging (RADAR/ ARPA)

Σκοπός του συστήματος είναι η ανίχνευση και η παρακολούθηση της θέσης και της ταχύτητας ενός αντικειμένου ή ενός εμποδίου μέσω της εκπομπής και της λήψης ηλεκτρομαγνητικών παλμών. Το σήμα επιστροφής (που ονομάζεται ηχώ ραντάρ) λαμβάνεται και αναλύεται από τον δέκτη. Το σύστημα σχεδίασης (Automatic Radar Plotting Aid - ARPA) είναι ο εξοπλισμός που συνδέεται με το ραντάρ πλοήγησης και επιτρέπει την παρακολούθηση της αντήχησης, υπολογίζοντας το πλησιέστερο σημείο προσέγγισης και βοηθάει το πλήρωμα να αποφύγει μία πιθανή σύγκρουση.

Μερικές από τις ευπάθειες του συστήματος παρουσιάζονται παρακάτω:

1. Η Άρνηση υπηρεσίας (DDoS Attacks)
2. Η πιθανότητα παρεμβολής του σήματος
3. Η πιθανότητα κλοπής και τροποποίησης του σήματος επιστροφής

Κεφάλαιο 5.2.6: Global Maritime Distress and Safety System (GMDSS)

Στόχος του GMDSS είναι η εξασφάλιση ταχείας και αυτοματοποιημένης ειδοποίησης σε περίπτωση έκτακτης ανάγκης. Μεταδίδει και λαμβάνει τα μηνύματα κινδύνου και ασφαλείας μέσω δορυφόρων. Τα μεταδιδόμενα μηνύματα αποτελούνται από τον τύπο του πλοίου και τον μοναδικό αριθμό του πλοίου (Maritime Mobile Service Identity - MMSI). Τα μηνύματα αυτά σχετίζονται συνήθως με βύθιση , προσάραξη ή έκρηξη σε ένα πλοίο.

Κεφάλαιο 5.3: Συστήματα Μηχανής

Τα συστήματα στο μηχανοστάσιο περιλαμβάνουν όλα τα υποσυστήματα για την παραγωγή ενέργειας και την πρόωση του πλοίου. Συγκεντρώνουν δεδομένα που σχετίζονται με την ταχύτητα του πλοίου, τη γωνία του πηδαλίου (steering gear) και την προπέλα. Επιπλέον, παρακολουθούν το φορτίο της μηχανής, την κατανάλωση καυσίμου και την στάθμη του νερού στη δεξαμενή έρματος (water ballast tank). Ανάλογα με τις πληροφορίες από το σύστημα ελέγχου στη γέφυρα, στέλνει εντολή στο σύστημα ελέγχου πρόωσης για να αυξήσει ή να μειώσει την ταχύτητα του πλοίου. Επιπλέον, δίνει την εντολή να αυξήσει ή να μειώσει το επίπεδο του νερού στη δεξαμενή έρματος ανάλογα με τις πληροφορίες από το σύστημα της γέφυρας. Ωστόσο, η χρήση ψηφιακών συστημάτων για την παρακολούθηση και τον έλεγχο των μηχανημάτων, της πρόωσης και της διεύθυνσης του πλοίου - καθιστούν τα συστήματα αυτά ευάλωτα σε κυβερνό- επιθέσεις. Η ευπάθεια των συστημάτων μπορεί να αυξηθεί όταν χρησιμοποιούνται μαζί με εξοπλισμό ναυσιπλοΐας και επικοινωνιών, σε πλοία που είναι εφοδιασμένα με ολοκληρωμένα συστήματα γέφυρας.

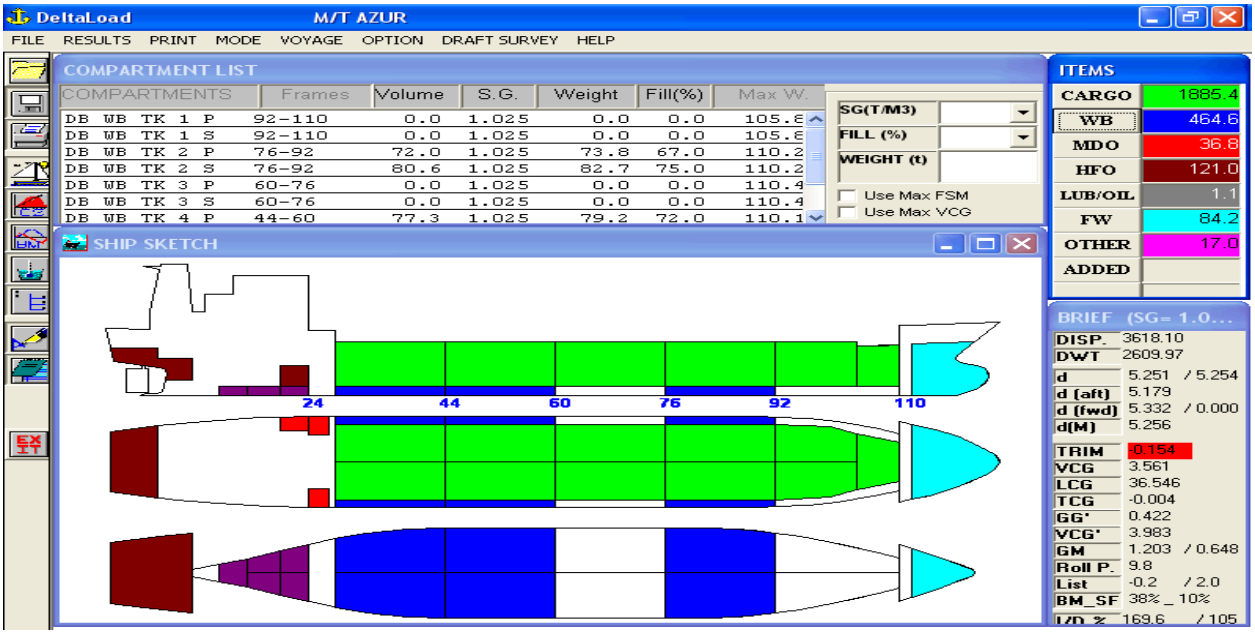
Εικόνα 17: Συστήματα Μηχανής

Εικόνα 18: AMS

Εικόνα 19: Σύστημα Πρόωσης

Κεφάλαιο 5.4: Συστήματα Διαχείρισης Φορτίου

Τα συστήματα υπολογιστών που χρησιμοποιούνται για τη διαχείριση και τον έλεγχο του φορτίου μπορεί να συνδέονται με μεγάλο αριθμό άλλων συστημάτων στην ξηρά. Αυτό το σύστημα μπορεί να περιλαμβάνει στοιχεία παρακολούθησης φορτίου που είναι διαθέσιμα στους αποστολείς μέσω του Διαδικτύου. Οι διασυνδέσεις αυτού του είδους καθιστούν τα συστήματα διαχείρισης φορτίου και τα δεδομένα ευάλωτα σε κυβερνό- επιθέσεις.



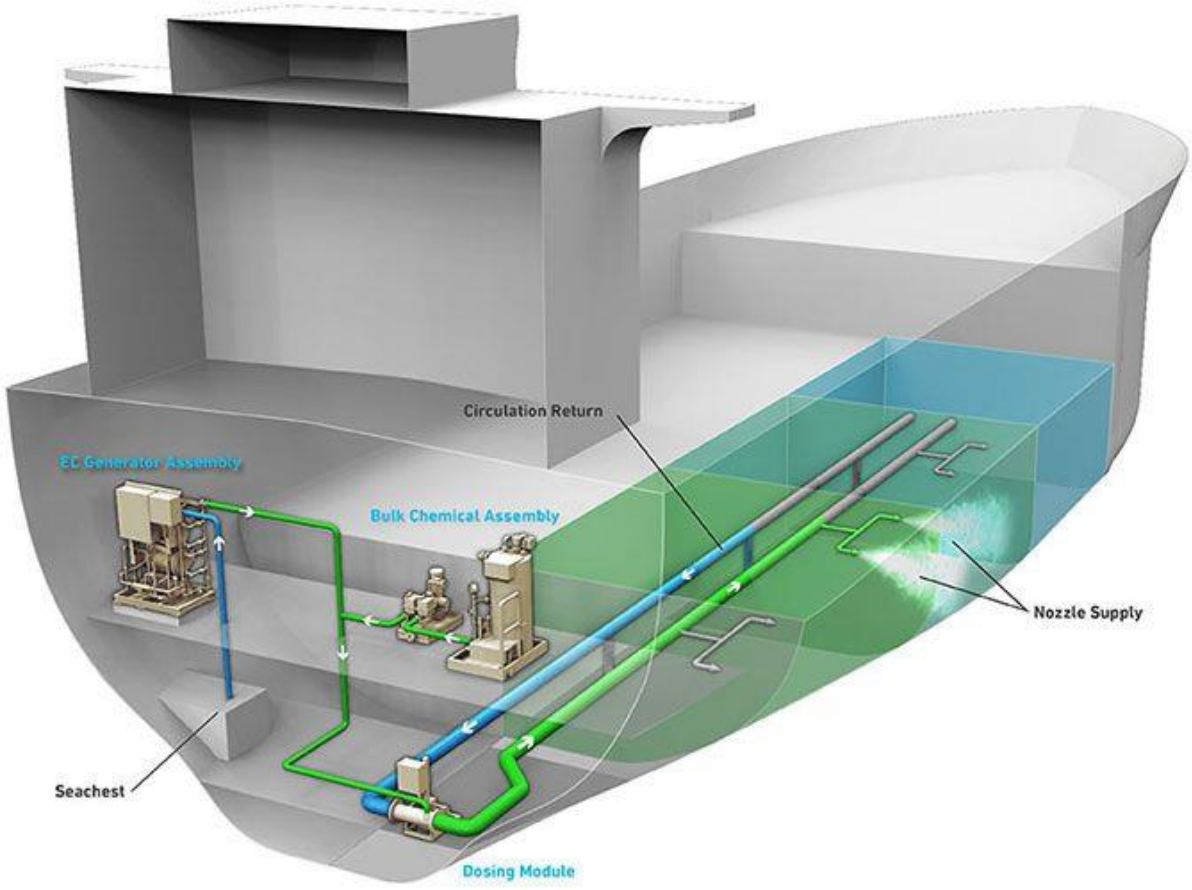
Εικόνα 20: Loadicator

Κεφάλαιο 5.5: Σύστημα Διαχείρισης Θαλάσσιου Έρματος

Πρόκειται για μία δεξαμενή μέσα σε ένα πλοίο που κρατά το νερό ως έρμα για την παροχή σταθερότητας. Η χρήση νερού σε μια δεξαμενή επιτρέπει την ευκολότερη προσαρμογή του βάρους. Επιτρέπει επίσης να αντληθεί το έρμα για να μειωθεί προσωρινά το βάρος του πλοίου όταν απαιτείται να εισέλθει σε πιο ρηχά νερά.

Οι κίνδυνοι του συστήματος σχετίζονται με:

1. Τα ICS δίκτυα: Διαχείριση αισθητήρων και κυκλωμάτων
2. SCADA: Τα ICS τερματικά που παρακολουθούν την επιχειρησιακή λειτουργία



Εικόνα 21: BWT 1

Εικόνα 22: BWT 2

Εικόνα 23: BWT 3

Κεφάλαιο 5.6: Passenger and Crew System

Το σύστημα ψυχαγωγίας και η πρόσβαση του επιβάτη στο διαδίκτυο αντιμετωπίζεται σαν ένα δημόσιο δίκτυο. Εάν η πρόσβαση στο διαδίκτυο για τους επιβάτες παρέχεται μέσω του ίδιου καναλιού που ελέγχει τα κρίσιμα συστήματα του πλοίου, τότε γίνεται ευκολότερο για τους κακόβουλους χρήστες να επιτεθούν στα συστήματα ελέγχου, ξεκινώντας από το σύστημα ψυχαγωγίας των επισκεπτών. Τα συστήματα αυτά θα πρέπει να θεωρούνται μη ελεγχόμενα και θα πρέπει να διαχωρίζονται από το

επιχειρησιακό δίκτυο. Όπως και για το σύστημα ψυχαγωγίας των επιβατών, η ευημερία του πληρώματος είναι ιδιαίτερα ευάλωτη όταν παρέχει πρόσβαση στο διαδίκτυο και στο ηλεκτρονικό ταχυδρομείο. Μπορεί να αξιοποιηθεί από τους επιτιθέμενους για να αποκτήσουν πρόσβαση σε συστήματα και ευαίσθητα δεδομένα του πλοίου. Τα συστήματα αυτά θα πρέπει επίσης να θεωρούνται μη ελεγχόμενα και να μην συνδέονται με κανένα κρίσιμο σύστημα ασφαλείας. Το δίκτυο που χρησιμοποιείται σύμφωνα με την πολιτική BYOD θα πρέπει να διαχωρίζεται από το επιχειρησιακό δίκτυο του πλοίου. Τέλος, είναι πολύ σημαντικά και τα ευαίσθητα δεδομένα των επιβατών (προσωπικές ή τραπεζικές πληροφορίες). Τα συστήματα που χρησιμοποιούνται για τη διαχείριση των δεδομένων των επιβατών αποτελούν πηγή κινδύνου, καθώς τα συλλεγόμενα δεδομένα μεταβιβάζονται σε κάποιο άλλο σύστημα.

Κεφάλαιο 5.7: Ευπάθειες και Επίδραση των επιθέσεων στα Πλοία

Τα συστήματα στα πλοία δεν είναι πλήρως απομονωμένα. Σε περίπτωση πιθανής παραβίασης, η αρχιτεκτονική δικτύου, έτσι όπως έχει υλοποιηθεί στο πλοίο, θα οδηγήσει την απειλή στα κρίσιμα συστήματα. Διερευνώντας τις ευπάθειες που δημιουργούνται από κάθε υπό- σύστημα, αυτό το τμήμα της εργασίας επικεντρώνεται στους κινδύνους που προκύπτουν από την μεταξύ τους διασύνδεση. Κάθε πλοίο σχεδιάζεται με μια μοναδική αρχιτεκτονική δικτύου που μπορεί να αλλάξει κατά τη διάρκεια του κύκλου ζωής του πλοίου. Ένας από τους σημαντικότερους παράγοντες κατά την αξιολόγηση της απειλής είναι η αντιστοίχιση των διασυνδέσεων των συστημάτων στο πλοίο, προκειμένου να διερευνηθεί η ενδεχόμενη διάδοση ενός περιστατικού. Με τη χαρτογράφηση των συστημάτων του πλοίου, ο οργανισμός μπορεί να δημιουργήσει μια ολιστική προσέγγιση των δικτύων, προκειμένου να κάνει καταστήσει τα συστήματα ασφαλή και να γνωρίζει τις επιπτώσεις σε περίπτωση επίθεσης. Το παρακάτω σχήμα απεικονίζει μια γενική τοπολογία της υποδομής των κρίσιμων συστημάτων και τις ευπάθειες οι οποίες δημιουργήθηκαν από αυτά τα συστήματα [52].

Το ολοκληρωμένο σύστημα γέφυρας (Integrated Bridge Systems) διαχειρίζεται όλα τα συστήματα της γέφυρας που παρέχουν τις πληροφορίες για την πλοήγηση του πλοίου. Αποτελείται από διαφορετικά συστήματα, όταν παραβιαστεί το IBS, είναι πολύ πιθανή η διάδοση του κινδύνου και στα υπόλοιπα συστήματα. Λόγω της άμεσης σύνδεσης ανάμεσα στο IBS και το σύστημα της μηχανής, οι λανθασμένες πληροφορίες από το AIS μπορούν να οδηγήσουν στην αποστολή τροποποιημένων εντολών ελέγχου στα συστήματα της μηχανής και, κατά συνέπεια, στην εκτροπή του πλοίου σε μεγαλύτερες διαδρομές και στην αύξηση ή μείωση της ταχύτητας. Λανθασμένες πληροφορίες σε σχέση με τη θέση και την ταχύτητα άλλων πλοίων, μπορούν να οδηγήσουν σε σύγκρουση. Εάν το AIS έχει παραβιαστεί από έναν εισβολέα με τη μετάδοση ψευδών δεδομένων, μπορεί να χρησιμοποιηθεί για την παροχή πλαστών πληροφοριών που σχετίζονται με το πλοίο. Ένα εκτεθειμένο AIS μπορεί είτε να παρέχει ψευδείς πληροφορίες για άλλα πλοία είτε να μεταδίδει λανθασμένες λεπτομέρειες για τη θέση και την κατάσταση του. Το ραντάρ παρέχει πληροφορίες σχετικά με το περιβάλλον του πλοίου και είναι ευάλωτο σε παρεμβολές και DDoS επιθέσεις. Αυτές οι συσκευές παρέχουν λανθασμένες πληροφορίες σχετικά με το αντικείμενο λόγω των ψευδών σημάτων που προκαλούνται από εξωτερικά ραντάρ. Αυτά τα εσφαλμένα μηνύματα μπορεί να προκαλέσουν τη σύγκρουση μεταξύ των πλοίων, δημιουργώντας

καθυστερήσεις στην εκφόρτωση φορτίου στο λιμάνι ή ακόμα και τη βύθιση των πλοίων με αποτέλεσμα την απώλεια φορτίου και ανθρώπινων ζωών.

Το Global Maritime Distress System (GMDSS) χρησιμοποιείται για τη μετάδοση των μηνυμάτων κινδύνου που σχετίζονται με τη σύγκρουση, την πτώση, τη βύθιση, την έκρηξη κλπ. Εάν το σύστημα αυτό υπονομευθεί από κακόβουλους χρήστες τότε μπορεί να χρησιμοποιηθεί για τη μετάδοση ψευδών μηνυμάτων κινδύνου σε άλλα πλοία ή στο κέντρο ελέγχου.

Το Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης (Global Navigation Satellite System - GNSS) είναι επίσης ευάλωτο σε επιθέσεις. Τα σήματα και τα δεδομένα του GNSS μπορούν να τροποποιηθούν, πράγμα που μπορεί να οδηγήσει σε λάθος θέση του πλοίου. Η ανίχνευση δεδομένων από το GNSS μπορεί επίσης να προκαλέσει επίθεση στο σύστημα ECDIS. Δεδομένου ότι το σύστημα ECDIS χρησιμοποιεί δεδομένα από το GNSS για την εμφάνιση των διαδρομών και της θέσης των πλοίων.

Το ECDIS χρησιμοποιείται αντί των παραδοσιακών χαρτών για τη δρομολόγηση του πλοίου. Τα συστήματα υπολογιστών που χρησιμοποιούνται για το ECDIS είναι ευάλωτα σε επιθέσεις με κακόβουλο λογισμικό. Οι επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο αυτές τις συσκευές αντικαθιστώντας τον αρχικό χάρτη με έναν τροποποιημένο. Κατά συνέπεια, το IBS μπορεί να δώσει εντολή στο σύστημα μηχανής για αλλαγή της διαδρομής του πλοίου. Αυτή η αλλαγή στην πορεία του πλοίου μπορεί να το οδηγήσει σε απαγορευμένη περιοχή ή μέσω άλλης μεγαλύτερης διαδρομής να προκληθεί καθυστέρηση στην άφιξη στο λιμένα προορισμού, και να υπάρξει καθυστέρηση στην εκφόρτωση. Επιπλέον, μπορεί να υπάρξει αλλαγή στο λιμένα προορισμού σε αντίθεση με ό, τι είχε προγραμματιστεί από τα μέλη του πληρώματος. Είναι γεγονός είναι ότι τα συστήματα αυτά είναι κακώς σχεδιασμένα σε επίπεδο πρωτοκόλλου και εφαρμογής, με αποτέλεσμα να είναι δυνατή η απόκτηση του ελέγχου ενός πλοίου ή ακόμα και η καταστροφή του ή άλλων δομών, από κακόβουλους χρήστες. Ένα πλοίο που έχει παραβιασθεί μπορεί να οδηγηθεί από τον επιτιθέμενο σε σύγκρουση με ένα άλλο πλοίο ή άλλο στόχο. Η επίθεση αυτή μπορεί να πραγματοποιηθεί είτε σε άλλα πλοία, σε πετρελαϊκές εγκαταστάσεις ή ακόμα και σε δομές που συνδέονται με χερσαίες εγκαταστάσεις.

Τα συστήματα της Μηχανής είναι επίσης ευάλωτα στις κυβερνό- επιθέσεις. Συγκεκριμένα, τα συστήματα ηλεκτρονικών υπολογιστών που συμμετέχουν στον έλεγχο της μηχανής είναι ευάλωτα σε επιθέσεις μέσω κακόβουλου λογισμικού. Εάν το σύστημα αυτό παραβιασθεί τότε μπορεί να χρησιμοποιηθεί για την αποστολή ψευδών πληροφοριών σχετικά με την ταχύτητα, την κατανάλωση καυσίμου, το φορτίο της μηχανής, τη στάθμη νερού στη δεξαμενή έρματος έως και το IBS. Αυτό μπορεί να οδηγήσει τα AIS και GMDSS να μεταδώσουν ψευδείς πληροφορίες. Επιπλέον, ο επιτιθέμενος μπορεί να τροποποιήσει τη διαδρομή του πλοίου, ή ακόμα και να ξεκινήσει ή να σταματήσει το κύριο σύστημα πρόωσης. Επιπλέον, ο επιτιθέμενος μπορεί να στείλει ψευδείς πληροφορίες σχετικά με έκρηξη στο πλοίο, βύθιση ή σύγκρουση, με αποτέλεσμα το IBS να μεταδώσει τις πληροφορίες αυτές στις αρχές μέσω του GMDSS.

Με την αύξηση ή τη μείωση της στάθμης του νερού στη δεξαμενή έρματος μέσω του αντίστοιχου συστήματος (Ballast Water Treatment System), ο επιτιθέμενος μπορεί να προκαλέσει ακόμη και βύθιση του πλοίου, εκτρέποντας τα δεδομένα σταθερότητας και τροποποιώντας τις ρυθμίσεις φόρτωσης και

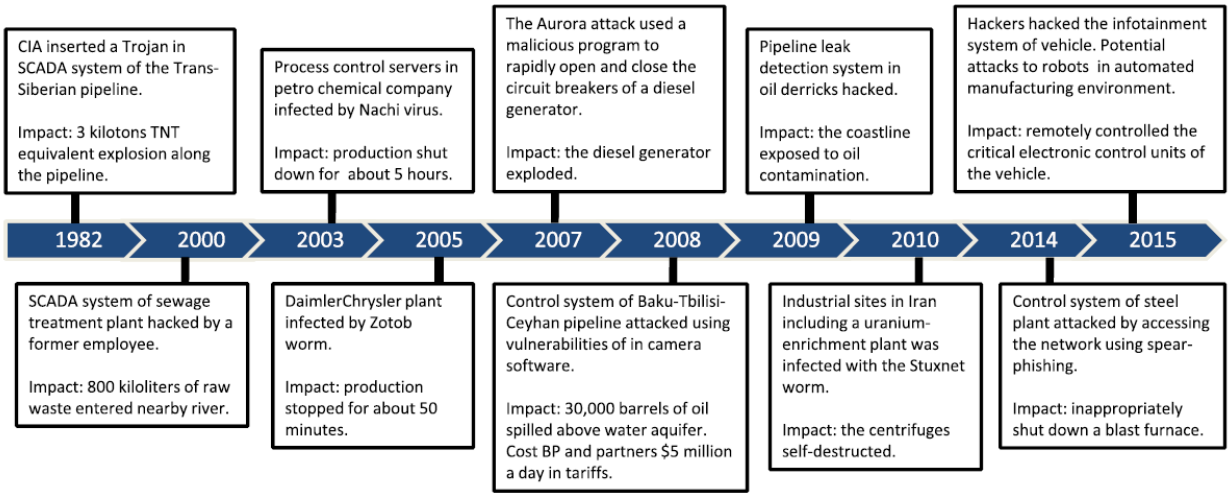
εκφόρτωσης του συστήματος. Η διακοπή της κανονικής λειτουργίας οδηγεί στην καθυστέρηση της άφιξης του πλοίου στον λιμένα προορισμού, της παράδοσης του φορτίου και συνεπώς σε προβλήματα στην εφοδιαστική αλυσίδα.

Το σύστημα διαχείρισης φορτίου είναι επίσης ευάλωτο σε επιτιθέμενους λόγω αυτής της αλληλεπίδρασης. Με την πρόσβαση σε αυτά τα συστήματα οι επιτιθέμενοι μπορούν να τροποποιήσουν τα δεδομένα που σχετίζονται με τα ποσοστά, τη φόρτωση, τον αριθμό του φορτίου, την ημερομηνία και τον τόπο παράδοσης προκαλώντας από οικονομική ζημιά για τον οργανισμό, έως περιβαλλοντική καταστροφή.

Από την παραπάνω ανάλυση προκύπτει ότι αρχιτεκτονική του δικτύου στα πλοία διαδραματίζει αναπόσπαστο ρόλο στη διατήρηση της ασφάλειας. Ωστόσο, οι οργανισμοί δεν υιοθετούν πολιτικές ασφαλείας σχετικά με το BYOD στα πλοία. Με τη χρήση προσωπικών συσκευών, τα τρωτά σημεία αυξάνονται ακόμη περισσότερο. Προκειμένου να αντιμετωπιστεί επιτυχώς ο κίνδυνος της ασφάλειας, οι οργανισμοί πρέπει να αρχίσουν να σχεδιάζουν την τοπολογία των συστημάτων τους και να καταγράφουν κάθε νέα καταχώρηση με ασφαλή και δομημένο τρόπο.

Κεφάλαιο 6: Περιστατικά Ασφαλείας

Τα περιστατικά ασφαλείας, σήμερα, έχουν γίνει πολύ δημοφιλή στους τίτλους των εφημερίδων. Μια ρεαλιστική προοπτική είναι απαραίτητη για την εξέταση της σοβαρότητας του περιστατικού. Ωστόσο, τίθεται το ερώτημα εάν η ασφάλεια είναι μία από τις κορυφαίες απειλές για τον ναυτιλιακό τομέα ή η επίδραση των απειλών τονίζεται υπερβολικά επειδή οι εταιρείες ασφαλείας επιθυμούν την εμπλοκή τους στο ναυτιλιακή βιομηχανία; Για να απαντηθεί η ερώτηση, αυτό το κεφάλαιο εστιάζει σε μερικά από τα σημαντικότερα περιστατικά στον ναυτιλιακό τομέα τα τελευταία χρόνια.



Εικόνα 24: Περιστατικά Ασφάλειας

Κεφάλαιο 6.1: Λιμάνι Αμβέρσας

Από το 2011 έως το 2013, στο βελγικό λιμάνι της Αμβέρσας υπήρξε περιστατικό παραβίασης ασφαλείας με στόχο τη διακίνηση ναρκωτικών. Οι επιτιθέμενοι μισθώθηκαν από εμπόρους ναρκωτικών για να παραβιάσουν τα συστήματα πληροφορικής που ελέγχουν την κίνηση και τη θέση των εμπορευματοκιβωτίων στο λιμάνι. Για μια περίοδο, περίπου δύο ετών, τα συστήματα των εταιρειών που λειτουργούσαν στο λιμένα ελέγχονταν συνεχώς από τους κακόβουλους χρήστες. Έχοντας πρόσβαση σε διαβαθμισμένα δεδομένα σχετικά με την τοποθεσία και την κίνηση των εμπορευματοκιβωτίων, οι επιτιθέμενοι ήταν ικανοί να στείλουν μη εξουσιοδοτημένους οδηγούς να κλέψουν το φορτίο πριν ο νόμιμος ιδιοκτήτης φτάσει στον προορισμό. Η παραβίαση εντοπίστηκε όταν άρχισαν να λείπουν ολόκληρα φορτία. Οι εγκληματίες έστειλαν στο προσωπικό του λιμένα, κακόβουλο λογισμικό μέσω ηλεκτρονικού ταχυδρομείου, το οποίο τους επέτρεψε να αποκτήσουν απομακρυσμένη πρόσβαση στα δεδομένα του λιμένα. Παρόλο που αυτή η πρώτη προσπάθεια εντοπίστηκε και εγκαταστάθηκαν firewalls στα συστήματα, οι επιτιθέμενοι κατάφεραν να παρακάμψουν τα μέτρα προστασίας του λιμένα και να εγκαταστήσουν λογισμικό key- logging στους νόμιμους υπολογιστές. Με αυτόν τον τρόπο, απέκτησαν ασύρματη πρόσβαση στα δεδομένα που πληκτρολογούσε το προσωπικό και έπαιρναν στιγμιότυπα από τις οθόνες τους. Όταν η επιχείρηση αποκαλύφθηκε, η αστυνομία κατέσχεσε περισσότερο από ένα εκατομμύριο τόνους κοκαΐνης, αξίας περισσότερο από 170 εκ. δολάρια, παρόμοια ποσότητα ηρωίνης, ένα εκατομμύριο ευρώ σε μετρητά και πολλά όπλα. Η χρησιμοποίηση αυτού του είδους επίθεσης για τέτοιο σκοπό δεν είναι κάτι καινούριο, ωστόσο η συγκεκριμένη μέθοδος υλοποίησης είναι πρωτόγνωρη για τη Ναυτιλία και έχει περιγραφεί ως: “Πλοίο φάντασμα”

Κεφάλαιο 6.2: Επίθεση στις Ναυτιλιακές Αρχές της Δανίας

Το 2014, οι ναυτιλιακές αρχές της Δανίας ανακάλυψαν ότι τα συστήματα τους είχαν παραβιασθεί το 2012 και ευαίσθητες πληροφορίες δανέζικων επιχειρήσεων είχαν υποκλαπεί από επιτιθέμενους, οι οποίοι υποστηρίζονταν με κρατικές χρηματοδοτήσεις. Παρόλο, που οι Δανέζικες αρχές υποστήριζαν ότι οι επιθέσεις είχαν υποστηριχθεί από τη Λαϊκή Δημοκρατία της Κίνας, η Κινεζική Πρεσβεία στην Κοπεγχάγη απέρριπτε κατηγορηματικά κάθε εμπλοκή με το συγκεκριμένο περιστατικό. Όταν το αρχείο αυτό ανοίχθηκε από έναν υπάλληλο, οι επιτιθέμενοι κατάφεραν να πάρουν τον έλεγχο όχι μόνο του υπολογιστή του υπαλλήλου, αλλά και των υπολοίπων στο δίκτυο της υπηρεσίας. Με αυτόν τον τρόπο απέκτησαν πρόσβαση στα συστήματα του Υπουργείου Εμπορίου. Έτσι, ο ιός αυτός μεταδόθηκε σε όλους τους υπολογιστές του δικτύων των οργανισμών και αντιμετωπίστηκε με χρήση ενός καινούργιου antivirus λογισμικού και μόνο όταν όλα τα συστήματα τέθηκαν εκτός λειτουργίας για αρκετές μέρες.

Κεφάλαιο 6.3: Κόλπος του Μεξικό

Το 2013, στον Κόλπο του Μεξικό, συνέβη περιστατικό ασφαλείας στην πλατφόρμα εξόρυξης πετρελαίου. Τα συστήματα της πλατφόρμας μολύνθηκαν με ιούς, όταν το πλήρωμα συνέδεσε προσωπικές συσκευές σε κρίσιμα συστήματα της πλατφόρμας. Το κακόβουλο λογισμικό απενεργοποίησε τα σήματα από το σύστημα πλοήγησης, με αποτέλεσμα τη βύθιση της πλατφόρμας.

Κεφάλαιο 6.4: Saudi Aramco

Το 2012, όταν ένας υπάλληλος της Saudi Aramco επισκέφθηκε μία μολυσμένη ιστοσελίδα, μέσω ενός e-mail, 35000 υπολογιστές του οργανισμού τέθηκαν μερικώς ή και ολοκληρωτικά εκτός λειτουργίας. Οι ηλεκτρονικοί φάκελοι άρχισαν να εξαφανίζονται και οι υπολογιστές να κλείνουν. Δεν υπήρχε πρόσβαση πλέον στο Internet, ούτε στο εταιρικό ηλεκτρονικό ταχυδρομείο ή τηλέφωνο (Ο οργανισμός αναγκάστηκε να προμηθευτεί 50000 μονάδες δίσκων αποθήκευσης. Οπότε, από το Σεπτέμβριο 2012, που πραγματοποιήθηκε η επίθεση, μέχρι τον Ιανουάριο 2013 οι τιμή των δίσκων είχε αυξηθεί σημαντικά). Η επίθεση είχε σαν αποτέλεσμα τεράστια απώλεια εσόδων για την εταιρία. Ο οργανισμός, ο οποίος προμηθεύει το 10% της παγκόσμιας ποσότητας πετρελαίου, αναγκάστηκε να αναστείλει τις δραστηριότητες του για 17 περίπου ημέρες.

Κεφάλαιο 6.5: Maersk

Στις 27 Ιουνίου 2017, η εταιρεία A.P. Moller – Maersk μολύνθηκε από τον ιό NotPetya. Έχοντας ένα στόλο με περισσότερα από 600 πλοία containers, η Maersk είναι η μεγαλύτερη ίσως ναυτιλιακή εταιρεία στον κόσμο και κατέχει περίπου το 16% της αγοράς. Η εταιρεία διαχειρίζεται το 25% του συνολικού φορτίου που διακινείται στη διαδρομή Ασίας – Ευρώπης [51]. Όπως ανακοίνωσε ο πρόεδρος της Maersk, Hagemann Snabe, στο παγκόσμιο οικονομικό φόρουμ (Ιανουάριο 2018), η εταιρεία διακινεί περίπου το 20% της παγκόσμιας αγοράς σε containers. Ένα πλοίο της εταιρείας, χωρητικότητας 15000 – 20000 containers, εισέρχεται κάθε 15 λεπτά σε κάποιο λιμάνι του κόσμου. Μετά την επίθεση η εταιρεία έπρεπε να διακόψει τη λειτουργία των IT συστημάτων επηρεάζοντας σχεδόν όλες τις επιχειρησιακές μονάδες, συμπεριλαμβανομένων των πλοίων της εταιρείας, των λιμενικών εγκαταστάσεων και παραγωγής πετρελαίου και φυσικού αερίου. Παρόλη τη σημαντική επίπτωση της επίθεσης στη λειτουργία της επιχείρησης, ο στόλος και το πλήρωμα δεν τέθηκαν σε κίνδυνο. Κατά τη διάρκεια της επίθεσης, η εταιρεία κατάφερε να συνεχίσει τις λειτουργίες της, μειώνοντας τον όγκο των παραδόσεων κατά 20% περίπου. Η εταιρία δέχθηκε επίθεση μέσω ενός Ransomware ιού που ονομάστηκε NotPetya. Επρόκειτο για ένα malware, το οποίο κρυπτογράφησε όλα τα αρχεία της εταιρείας και τροποποίησε το Master Boot Record των υπολογιστών, μην επιτρέποντας στους χρήστες να έχουν πρόσβαση στα windows. Οι επιτιθέμενοι απαιτούσαν 300 δολάρια σε BitCoins προκειμένου να επιτρέψουν την πρόσβαση των νόμιμων χρηστών στους υπολογιστές τους και την αποκρυπτογράφηση των αρχείων. Ο συγκεκριμένος ιός είχε την ικανότητα να διαδίδεται σε όλες τις συσκευές του δικτύου. Η επίθεση πραγματοποιήθηκε μέσω μίας αναβάθμισης ενός λογισμικού του λογιστηρίου (ME Doc), εκμεταλλευόμενη μία ευπάθεια των windows (SMB - EternalBlue), στα γραφεία της εταιρείας στην Ουκρανία. Κατά τον πρόεδρο της Maersk, η επίθεση σχεδιάστηκε από κρατικές υπηρεσίες και είχε ως στόχο τη Δημοκρατία της Ουκρανίας. Για να αντιμετωπιστεί η επίθεση, η εταιρεία αναγκάστηκε να διακόψει τη λειτουργία των συστημάτων της για το σύνολο των επιχειρησιακών λειτουργιών για 10 ημέρες περίπου. Στο διάστημα αυτό, έγινε εγκατάσταση 40000 εξυπηρετητών, 25000 υπολογιστών και περίπου 2500 εφαρμογών. Κατά τον πρόεδρο της εταιρείας, για να ολοκληρωθεί όλη αυτή η διαδικασία σε κανονικές συνθήκες, απαιτείται κατά προσέγγιση χρονικό διάστημα 6 μηνών. Αυτό αποδεικνύει την προσπάθεια που κατέβαλαν το προσωπικό, οι προμηθευτές και οι κατασκευάστριες εταιρίες προκειμένου να ανακάμψει η εταιρεία από την επίθεση. Ωστόσο, όσο

θα αυξάνεται η εξάρτηση των εταιρειών από τα ψηφιακά συστήματα, τόσο πιο δύσκολη θα είναι η διαδικασία της ανάκαμψης από παρόμοια περιστατικά. Η επίθεση αποτέλεσε ένα προειδοποιητικό μήνυμα για όλες τις εταιρείας υψηλής τεχνολογίας όπως τη Maersk. Πριν την επίθεση υπήρχε η πεποίθηση ότι η εταιρεία είχε υψηλό επίπεδο ασφαλείας, ωστόσο έπεσε θύμα μίας μη στοχευμένης επίθεσης πλήττοντας την όχι μόνο οικονομικά αλλά σε μεγάλο βαθμό και στη φήμη του οργανισμού. Εκτιμάται ότι το κόστος της επίθεσης ανήλθε σε 300 εκατομμύρια δολάρια.

Κεφάλαιο 6.6: GPS Spoofing

Τον Ιούλιο 2013 μία ερευνητική ομάδα από το Πανεπιστήμιο του Τέξας, πήρε τον έλεγχο των συστημάτων πλοήγησης ενός σκάφους αναψυχής αξίας 80 εκατομμυρίων δολαρίων. Αυτό το κατάφερε χρησιμοποιώντας εξοπλισμό αξίας 3000 δολαρίων. Πιο συγκεκριμένα, η ομάδα χρησιμοποιώντας μία συσκευή – στο μέγεθος βαλίτσας – τροποποίησε τα δεδομένα του GPS, στοχεύοντας τη συσκευή πλοήγησης του πλοίου. Οι ερευνητές αύξησαν την ισχύ των κυμάτων που μετέδιδαν, τόσο ώστε το σήμα τους να είναι ισχυρότερο από το σήμα του δορυφόρου. Αυτό είχε σαν αποτέλεσμα να μπορέσουν οι κακόβουλοι χρήστες να αλλάξουν την πορεία του πλοίου, χωρίς να είναι δυνατή η απεικόνιση αυτής της αλλαγής στους χάρτες του πλοίου και ο έλεγχος του πλοίου είχε πλέον περάσει στους επιτιθέμενους.

Εικόνα 25: GPS Spoofing

Κεφάλαιο 6.7: GPS Jamming

Τον Απρίλιο του 2015, η Νότια Κορέα υπέστη μία από τις σημαντικότερες επιθέσεις στο GPS, όταν επηρεάστηκαν πάνω από 1000 αεροπλάνα και 250 πλοία. Οι επιθέσεις αυτές συνοδεύτηκαν από αρκετά σήματα, αναφέροντας ότι πλοία βρίσκονται σε κατάσταση κινδύνου καθώς δεν μπορούσαν να προσδιορίσουν την ακριβή τοποθεσία τους αλλά ούτε και να γυρίσουν στο λιμάνι. Η κυβέρνηση της Νότιας Κορέας υποστήριξε ότι το περιστατικό αυτό είχε γίνει με την υποστήριξη της κυβέρνησης της Βόρειας Κορέας. Η συγκεκριμένη επίθεση είναι μία σκόπιμη παρεμβολή στο σήμα του GPS, στοχεύοντας στην πλήρη παρεμβολή του σήματος και όχι στην τροποποίηση του. Λόγω της μη διαθεσιμότητας των δεδομένων από το GPS επηρεάζεται η λειτουργία του AIS, του ECDIS και του VDR.

Εικόνα 26: GPS Jamming

Κεφάλαιο 6.8: ECDIS Compromise

Για το ECDIS αποτελεί συχνό φαινόμενο η μόλυνση από ιούς μέσω των θυρών USB, κατά τη διαδικασία αναβάθμισης των ηλεκτρονικών χαρτών ή τη χρησιμοποίηση μη εξουσιοδοτημένων συσκευών. Ένα τέτοιο περιστατικό συνέβη σε μία μεγάλη ναυτιλιακή εταιρεία , όταν μέλος πληρώματος ενός τάνκερ 80000 τόνων, συνέδεσε ένα μολυσμένο USB stick στο ECDIS για να πραγματοποιήσει αναβάθμιση των χαρτών. Το σύστημα πλοήγησης αμέσως μολύνθηκε με αποτέλεσμα να καθυστερήσει για αρκετές ώρες η αναχώρηση του πλοίου. Για το λόγο αυτό, τα μέσα που χρησιμοποιούνται για την ενημέρωση του συστήματος θα πρέπει να χρησιμοποιούνται αποκλειστικά για το σκοπό αυτό και να ελέγχονται πριν αρχίσει η διαδικασία της αναβάθμισης [54].

Εικόνα 27: Σφάλμα σε ECDIS

Εικόνα 28: Επίθεση σε ECDIS

Κατά το αγκυροβόλιο του πλοίου στο Novorossiysk, σύμφωνα με το ECDIS η θέση του πλοίου ήταν στη στεριά. Αιτία του φαινομένου αυτού ήταν η παρεμβολή στο σήμα GPS του πλοίου από στρατιωτικούς πομπούς. Το GPS 1 επηρεάστηκε ενώ το GPS 2 όχι, για το λόγο αυτό το πλήρωμα τροποποίησε την πηγή από την οποία τροφοδοτείται το ECDIS (GPS 2)

Κεφάλαιο 7: Αντιμετώπιση των Κινδύνων

Στα προηγούμενα κεφάλαια αναλύθηκαν οι διαφορετικοί παράγοντες που επηρεάζουν την ασφάλεια στα πλοία. Έγινε μία προσπάθεια να δημιουργηθεί μία ολιστική προσέγγιση για την κυβερνό-ασφάλεια στη ναυτιλιακή βιομηχανία. Για να συμβεί αυτό πρέπει να αναγνωριστούν τα συστήματα που είναι περισσότερο ευάλωτα, να συλλεχθούν πληροφορίες για πιθανούς κινδύνους και ευπάθειες για τα συστήματα αυτά και να αναγνωριστούν οι πιθανοί παράγοντες που απειλούν τη ναυτιλία. Για να μειωθεί ο κίνδυνος από μία κυβερνό – επίθεση είναι απαραίτητο οι ναυτιλιακοί οργανισμοί να αναδιοργανώσουν την τοπολογία του δικτύου στα πλοία. Το κεφάλαιο αυτό προτείνει κάποιες διαδικασίες προκειμένου να αντιμετωπιστούν οι ευπάθειες και οι επιπτώσεις μία κυβερνό- επίθεσης.

Η προτεινόμενη μέθοδος δημιουργεί τρεις κατηγορίες:

1. Την Ανθρωποκεντρική προσέγγιση
2. Τα δεδομένα και τα Συστήματα
3. Την αρχιτεκτονική του Δικτύου

Κεφάλαιο 7.1: Ανθρωποκεντρική Προσέγγιση

Τα αυτόνομα πλοία δημιουργούν σπουδαίες προοπτικές για τη Ναυτιλιακή Βιομηχανία. Ωστόσο, υπάρχουν ακόμα πολλά στάδια που πρέπει να υλοποιηθούν μέχρι τα μη επανδρωμένα - αυτόνομα πλοία να καταστούν πλήρως λειτουργικά. Όπως παρουσιάστηκε και στο κεφάλαιο 4.2, προς το παρόν, ο άνθρωπος είναι αυτός που αλληλεπιδρά με τα συστήματα του πλοίου και για το λόγο αυτό το μη ενημερωμένο προσωπικό είναι μία από τις κύριες αιτίες αύξησης των κυβερνό- επιθέσεων. Επομένως, για τη σωστή αντιμετώπιση των επιθέσεων αυτών στα πλοία, είναι απαραίτητη η υιοθέτηση μιας ανθρωποκεντρικής προσέγγισης, λαμβάνοντας υπ’ όψη την αλληλεπίδραση του ανθρώπου με τα συστήματα. Ο Παγκόσμιος Οργανισμός Προτυποποίησης (International Organization for Standardization - ISO) έχει αναπτύξει πρότυπα για την ενίσχυση της συμβολής του ανθρώπου σε όλο τον κύκλο ζωής των συστημάτων. Το πρότυπο ISO 9241-210: 2010, παρέχει τις απαιτήσεις που θα πρέπει να υλοποιηθούν από τις εταιρείες που σχεδιάζουν και αναπτύσσουν το υλικό και το λογισμικό που χρησιμοποιείται στη βιομηχανία ώστε το τελικό σύστημα να δουλεύει σε αρμονία με τους τελικούς χρήστες.

Κεφάλαιο 7.1.1: Σκοπός

Σκοπός της ανθρωποκεντρικής προσέγγισης είναι η παροχή μιας δομής, η οποία θα βοηθήσει στη μείωση των κινδύνων που προκύπτουν από τα ανθρώπινα σφάλματα. Αρχικά, το προσωπικό που έρχεται σε επαφή με τα συστήματα, θα πρέπει να έχει πλήρη γνώση των λειτουργικών απαιτήσεων των συστημάτων. Από τα αρχικά στάδια της πρόσληψης στον οργανισμό, οι υπάλληλοι θα πρέπει να γνωρίζουν όλες τις λεπτομέρειες των συστημάτων των πλοίων με τα οποία θα έρθουν σε επαφή, καθώς και να λαμβάνουν εκπαιδεύσεις για την ασφαλή χρήση των συστημάτων αυτών. Ωστόσο, η Ναυτιλία θα πρέπει να λάβει υπ’ όψη το γεγονός ότι καθώς η τεχνολογία εξελίσσεται με ταχείς ρυθμούς, θα πρέπει να υπάρχει συνεχής αξιολόγηση και βελτίωση των διαδικασιών. Δεν είναι αρκετή η εκπαίδευση του

προσωπικού πριν την επιβίβαση στο πλοίο. Η πρόκληση για τη Βιομηχανία έγκειται στη διατήρηση της κουλτούρας μέσω των συνεχών σεμιναρίων και εκπαιδεύσεων προκειμένου το προσωπικό να αντιληφθεί τη σημασία της ασφάλειας. Επιπλέον, για την επιτυχία της προσέγγισης αυτής, ο οργανισμός θα πρέπει να είναι σε θέση να αναγνωρίσει ποιοι υπάλληλοι είναι κατάλληλοι για την εκτέλεση των εργασιών, σύμφωνα με τις ικανότητες τους. Τοποθετώντας τον κατάλληλο υπάλληλο στη σωστή θέση, η εταιρεία θα είναι σε θέση να δημιουργήσει συγκεκριμένο σχέδιο αξιολόγησης, για να αντιμετωπίσει τους πιθανούς κινδύνους.

Κεφάλαιο 7.1.2: Πλάνο

Μετά την κατανόηση και την αποδοχή της απόφασης για ενίσχυση της ανθρώπινης συμβολής στη προσπάθεια μείωσης των επιπτώσεων των κυβερνό- επιθέσεων, η Βιομηχανία πρέπει να αναπτύξει ένα πλάνο το οποίο θα επικεντρώνεται στον ανθρώπινο παράγοντα. Αναπτύσσοντας και εντάσσοντας μία ανθρωποκεντρική προσέγγιση σε όλο το φάσμα λειτουργίας των συστημάτων, μπορεί να δημιουργηθεί μία αποτελεσματική λίστα απαιτήσεων και στόχων για την σωστή χρήση των συστημάτων.

Τα στοιχεία στα οποία πρέπει να δοθεί έμφαση είναι:

- Η συνεχής εκπαίδευση των πληρωμάτων και του προσωπικού στη στεριά, καθώς και η υιοθέτηση κουλτούρας από τον οργανισμό σχετικά με την κυβερνό- ασφάλεια
- Κατά το σχεδιασμό των συστημάτων θα πρέπει να λαμβάνονται υπ’ όψη οι χρήστες που θα λειτουργούν και θα συντηρούν τα συστήματα αυτά
- Οι αρμοδιότητες των πληρωμάτων αλλά και του προσωπικού στη στεριά θα πρέπει να επανακαθοριστούν προκειμένου να ληφθεί υπ’ όψη και η ευθύνη για την υποστήριξη των συστημάτων σχετικά με την ασφάλεια
- Η δημιουργία ψηφιακής κουλτούρας σε όλα τα συνεργαζόμενα μέρη. Η κυβερνό- ασφάλεια δεν αφορά μόνο το προσωπικό στη θάλασσα αλλά και το προσωπικό στο γραφείο καθώς και τις συνεργαζόμενες εταιρείες που έχουν πρόσβαση στα συστήματα

Η λειτουργία των συστημάτων στο πλοίο πρέπει να ελέγχεται προσεκτικά ώστε να επιβεβαιώνεται η σωστή και ασφαλής χρήση τους από το πλήρωμα αλλά και η ορθή συντήρηση τους, σύμφωνα με τις προδιαγραφές του κατασκευαστή. Θα πρέπει να δημιουργηθούν οι κατάλληλες πολιτικές και διαδικασίες σχετικά με την προστασία της ανθρώπινης ζωής και των κρίσιμων συστημάτων, για τη λειτουργία του πλοίου, σε περίπτωση κυβερνό- επίθεσης. Είναι αναγκαίο να πραγματοποιούνται, ανά τακτά χρονικά διαστήματα, ειδικές ασκήσεις αντιμετώπισης καταστάσεων στις οποίες πολλαπλά συστήματα του πλοίου βρίσκονται εκτός λειτουργίας, ή λειτουργούν με τροποποιημένα δεδομένα. Εκτός από τα παραπάνω, θα πρέπει να αναπτυχθούν εξειδικευμένες εκπαιδεύσεις σε συγκεκριμένα ζητήματα ασφαλείας για όλα τα εμπλεκόμενα μέρη, από τα πληρώματα των πλοίων μέχρι τις λιμενικές αρχές.

Κεφάλαιο 7.1.3: Προειδοποίηση

Κύριος στόχος του συστήματος προειδοποίησης είναι η διασφάλιση ότι σε περίπτωση έκτακτης ανάγκης, μία ενδεχόμενη βλάβη σε κρίσιμα συστήματα του πλοίου θα ανιχνευθεί και οι απαραίτητες ενέργειες θα πραγματοποιηθούν για να μειωθεί η επίπτωση της στην ασφάλεια του πλοίου. Στην περίπτωση περιστατικού κυβερνό- ασφάλειας, ο κατάλληλος συναγερμός θα πρέπει να ειδοποιήσει το προσωπικό για το συμβάν. Στη Ναυτιλιακή Βιομηχανία οι συναγερμοί και οι προειδοποιήσεις συνδέονται με το αντίστοιχο σύστημα ή μηχάνημα και κατηγοριοποιούνται σύμφωνα με την κρισιμότητα του συστήματος (όπως αναφέρει ο IMO). Ωστόσο, το σύστημα προειδοποίησης δεν θα πρέπει να είναι πολύ αναλυτικό. Θα πρέπει να περιλαμβάνει και να δείχνει μόνο δεδομένα που είναι απαραίτητα για την ασφαλή λειτουργία του πλοίου. Αρχικά, θα πρέπει να γίνει μία ανάλυση των δεδομένων που παρέχει ο κατασκευαστής. Ακολούθως, απαιτείται η ανάμειξη των μηχανικών τόσο από τη μεριά του πλοίου όσο και της στεριάς για να αναλυθούν τα δεδομένα που χρειάζονται για τη λειτουργία των συστημάτων

Κεφάλαιο 7.1.4: Απόκριση

Ο ανθρωποκεντρικός σχεδιασμός πρέπει να περιλαμβάνει μία διαδικασία συνεχούς παρακολούθησης της χρήσης των συστημάτων. Τα κριτήρια και οι μετρήσεις αυτής της παρακολούθησης θα πρέπει να είναι τόσο ευαίσθητα, προκειμένου να γίνει αντιληπτή μία ενδεχόμενη βλάβη σε ένα σύστημα όσο πιο νωρίς γίνεται.

Η αξιολόγηση μιας ανθρωποκεντρικής προσέγγισης θα πρέπει να περιλαμβάνει:

- Τους πόρους για την έγκαιρη ανατροφοδότηση για τη βελτίωση του προϊόντος όσο και για τον προσδιορισμό αν ικανοποιήθηκαν οι απαιτήσεις
- Εκτεταμένες δοκιμές για την παροχή σημαντικών αποτελεσμάτων για το σύνολο του συστήματος με την ανάλυση των αποτελεσμάτων, την ιεράρχηση των ζητημάτων και την πρόταση λύσεων
- Οι πόροι για την αξιολόγηση θα πρέπει να διατίθενται τόσο για την έγκαιρη ανατροφοδότηση με την οποία θα βελτιωθεί το προϊόν όσο και για να επικυρωθεί, σε μεταγενέστερο στάδιο, εάν οι απαιτήσεις του χρήστη έχουν ικανοποιηθεί
- Κάθε άτομο θα πρέπει να εκπαιδεύεται σχετικά με τον τρόπο με τον οποίο η ηλεκτρονική του δραστηριότητα μπορεί να προκαλέσει ευπάθεια και τον τρόπο με τον οποίο πρέπει να αντιδράσει σε ένα ενδεχόμενο περιστατικό, με τον ίδιο τρόπο που θα συνέβαινε σε αντίξοες καιρικές συνθήκες ή πυρκαγιές στη θάλασσα

Κεφάλαιο 7.2: Σύστημα και Δεδομένα

Ο στόχος των δικτύων και των συστημάτων επικοινωνίας είναι να εξασφαλιστεί ότι παρέχεται υπηρεσία στα συστήματα που ανταποκρίνεται στις απαιτήσεις ασφάλειας και δια- λειτουργικότητας για τη λειτουργία του πλοίου. Ο στόχος αυτών των απαιτήσεων είναι να αποτελέσουν αναπόσπαστο μέρος των διαδικασιών του συστήματος διασφαλίζοντας ότι λαμβάνονται υπόψη οι ανάγκες όλων των

χρηστών. Αυτές οι απαιτήσεις επικοινωνίας θα πρέπει να παρέχονται από μια εξελιγμένη υποδομή δικτύου η οποία είναι ικανή:

- Να παρέχει τη δυνατότητα χειρισμού του απαιτούμενου φορτίου συν ένα περιθώριο για επέκταση και υπερφόρτωση
- Να είναι ανθεκτική σε βλάβες στο βαθμό που είναι απαραίτητο για την κρισιμότητα των πληροφοριών που μεταφέρει
- Να είναι ανθεκτική σε μη εξουσιοδοτημένη και ακούσια χρήση
- Να είναι σε θέση να παρέχει πληροφορίες σχετικά με τις επιδόσεις του συστήματος και να υποστηρίζει τις απαιτήσεις συνέχειας των δεδομένων
- Η διαχείριση ενός κατάλληλου συστήματος δικτύου το οποίο καθορίζει τις διαδικασίες, τους κανόνες και τις στρατηγικές για την παρακολούθηση, τον έλεγχο και τη διαχείριση του δικτύου επικοινωνιών δεδομένων

Επιπλέον, ο εντοπισμός ενός συμβάντος είναι σημαντικός για την αποτροπή της εξάπλωσης του ή ακόμη και για την παρεμπόδιση του αμέσως μόλις εντοπιστεί. Παρακολουθώντας και ανιχνεύοντας πιθανά περιστατικά στα συστήματα, ο οργανισμός είναι σε θέση να ενεργοποιήσει τους μηχανισμούς αντιμετώπισης της επίθεσης και να ανταποκριθεί κατάλληλα. Θα πρέπει να παρέχονται πληροφορίες για τη λειτουργία των αισθητήρων και των συστημάτων, συμπεριλαμβανομένων στοιχείων για την επαλήθευση και επικύρωση των επιδόσεων των συστημάτων.

Η διαδικασία προσδιορισμού των ασυνήθιστων δραστηριοτήτων πρέπει να περιλαμβάνει:

- Χρήση διαδικασιών ανάλυσης που είναι ικανές να αποκαλύπτουν μη φυσιολογικές συμπεριφορές
- Τον ορισμό ενός ατόμου ή μιας ομάδας για να αναλάβει όλες τις πτυχές που σχετίζονται με τον τομέα της ασφάλειας στον κυβερνοχώρο, για λογαριασμό της εταιρείας [43]
- Πλήρες ιστορικό περιστατικών

Η εκτίμηση κινδύνου θα πρέπει να οργανωθεί σε σχέση με τα συστήματα και τις λειτουργίες του οργανισμού. Θα πρέπει να αναλυθούν οι συνέπειες των βλαβών του συστήματος σε όλα τα επίπεδα προκειμένου να προσδιοριστούν οι επιπτώσεις στο σύνολό του συστήματος. Η διαδικασία της εκτίμησης κινδύνου θα πρέπει, επίσης, να αναγνωρίζει πιθανά μέτρα απομείωσης του κινδύνου και να καθορίζει τις απαραίτητες ενέργειες που θα πρέπει να ακολουθηθούν.

Στην εκτίμηση κινδύνου πρέπει να γίνεται:

- Μελέτη των συστημάτων του οργανισμού
- Αναγνώριση πιθανών βλαβών και τις αιτίες τους
- Αξιολόγηση των επιπτώσεων της μη διαθεσιμότητας των συστημάτων στη λειτουργία του οργανισμού
- Αναγνώριση πιθανών μέτρων για τη μείωση του κινδύνου
- Αναγνώριση μεθόδων ελέγχου για την παραγωγή συμπερασμάτων

System	Integrated Bridge System									
Assets	**ECDIS**	**Radar**	**Conning display**	**Alarm System AMS**	**AIS**	**GNSS**	**GMDSS station**	**Navtex receiver**	**VHF**	**Manual steering control**
Threat scenario. Threats TH.1, TH.2, TH.3 exploiting vulnerabilities on assets and consequence	Intruder remotely takes control of ECDIS	Intruder remotely takes control of Radar	Conning display not available as a result of interception	Alarm Management AMS not available as a result of interception	Intruder intercepts AIS	Intruder intercepts GNSS	Intruder intercepts GMDSS	Intruder intercepts Navtex	Intruder intercepts VHF	Intruder remotely takes control of manual steering
Likelihood of threat (1 to 3)	**3**	**2**	**2**	**2**	**3**	**3**	**1**	**1**	**1**	**2**

Εικόνα 29: Εκτίμηση Κινδύνου

System	Integrated Bridge System									
Assets	**ECDIS**	**Radar**	**Conning display**	**Alarm System AMS**	**AIS**	**GNSS**	**GMDSS station**	**Navtex receiver**	**VHF**	**Manual steering control**
Level of asset vulnerability (1 to 3)	**3**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**

Εικόνα 30: Εκτίμηση Κινδύνου

System	Integrated Bridge System									
Assets	**ECDIS**	**Radar**	**Conning display**	**Alarm System AMS**	**AIS**	**GNSS**	**GMDSS station**	**Navtex receiver**	**VHF**	**Manual steering control**
Asset impact value on Integrity and Availability (1-20)	**17**	**18**	**16**	**17**	**13**	**17**	**11**	**8**	**13**	**20**
Threat scenario. Threats TH.1, TH.2, TH.3 exploiting vulnerabilities on assets and consequence	Intruder remotely takes control of ECDIS	Intruder remotely takes control of Radar	Conning display not available as a result of interception	Alarm Management AMS not available as a result of interception	Intruder intercepts AIS	Intruder intercepts GNSS	Intruder intercepts GMDSS	Intruder intercepts Navtex	Intruder intercepts VHF	Intruder remotely takes control of manual steering
Likelihood of threat (1 to 3)	**3**	**2**	**2**	**2**	**3**	**3**	**1**	**1**	**1**	**2**
Level of asset vulnerability (1 to 3)	**3**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**
Likelihood of incident (1 to 9)	**9**	**2**	**2**	**2**	**6**	**6**	**1**	**1**	**1**	**2**
Asset Risk (1 to 180)	**153**	**36**	**32**	**34**	**78**	**102**	**11**	**8**	**13**	**40**
System risk value (9 to 1800)	**507**									

Εικόνα 31: Εκτίμηση Κινδύνου

Κεφάλαιο 7.2.1: Ανάκτηση Δεδομένων

Ανάκτηση δεδομένων είναι η δυνατότητα της επαναφοράς ενός συστήματος ή δεδομένων από μία ασφαλή αντιγραφή του συστήματος. Θα πρέπει να είναι διαθέσιμες βασικές πληροφορίες και

κατάλληλο λογισμικό για τη δημιουργία αντιγράφων ασφαλείας, ώστε να εξασφαλιστεί η πλήρης ανάκτηση των δεδομένων μετά από ένα περιστατικό ασφαλείας. Τα αντίγραφα ασφαλείας θα πρέπει να δημιουργούνται σε εξωτερικά μέσα ανά τακτά χρονικά διαστήματα, και να μην αποθηκεύονται στο επιχειρησιακό δίκτυο. Σε περίπτωση επίθεσης, ένα αντίγραφο ασφαλείας αποθηκευμένο στον μολυσμένο υπολογιστή θα χαθεί ή θα κρυπτογραφηθεί όπως και κάθε άλλο αρχείο. Πρέπει επίσης να καθοριστεί περίοδος διατήρησης και σενάρια αποκατάστασης, προκειμένου να αποφασιστεί σε ποια κρίσιμα συστήματα θα δοθεί προτεραιότητα καθώς η γρήγορη αποκατάσταση τους είναι απαραίτητη για την ομαλή λειτουργία του οργανισμού. Τα συστήματα που έχουν υψηλές απαιτήσεις διαθεσιμότητας δεδομένων θα πρέπει να είναι όσο το δυνατόν περισσότερο ασφαλή. Τα OT συστήματα, τα οποία είναι κρίσιμης σημασίας για την ασφαλή πλοήγηση και λειτουργία του πλοίου, θα πρέπει να διαθέτουν εφεδρικά συστήματα που θα επιτρέπουν στο πλοίο να ανακτήσει γρήγορα και με ασφάλεια τις ικανότητες πλοήγησης και λειτουργίας μετά από μία κυβερνό- επίθεση.

Εικόνα 32: Δημιουργία Back - Up

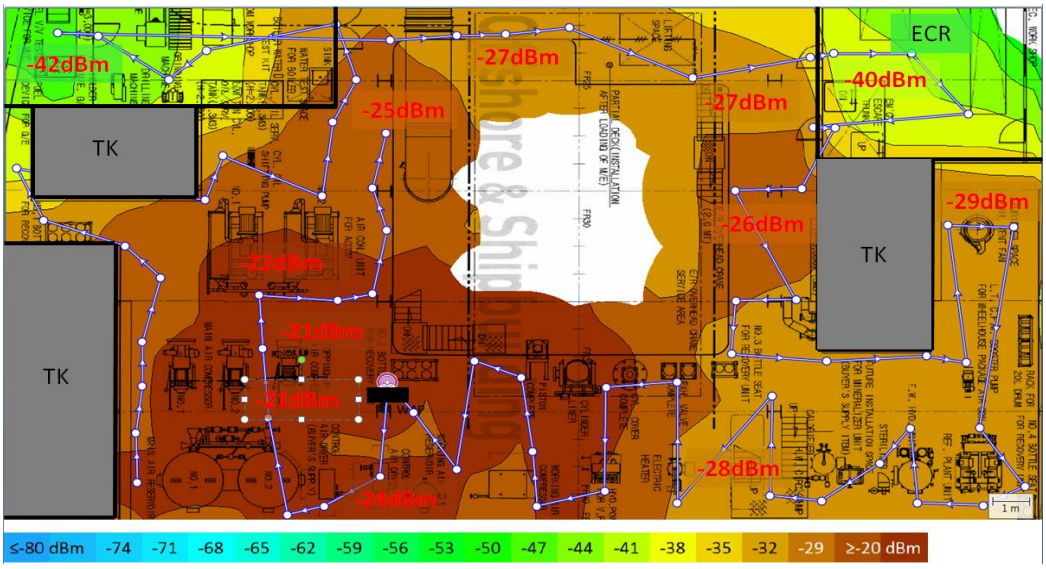
Κεφάλαιο 7.2.2: Διαχείριση Δικαιωμάτων

Η καθιέρωση διαδικασιών διαχείρισης λογαριασμών και ο περιορισμός του αριθμού των λογαριασμών με δικαιώματα διαχειριστή καθώς και η εφαρμογή πολιτικών ασφαλών κωδικών πρόσβασης μπορούν να μειώσουν τον κίνδυνο ενός περιστατικού ασφαλείας. Με τη δημιουργία και τη διατήρηση μιας λίστας ατόμων που έχουν πρόσβαση στο δίκτυο, θα πρέπει να γίνει διαμόρφωση του συστήματος, προκειμένου να διασφαλιστεί ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο. Είναι απαραίτητο οι δρομολογητές να είναι ασφαλείς απέναντι σε μη εξουσιοδοτημένη πρόσβαση στα συστήματα ή δεδομένα της εταιρείας και οι θύρες του δικτύου που δεν χρησιμοποιούνται να είναι κλειστές για να αποτρέπονται οι επιθέσεις.

Κεφάλαιο 7.2.3: Ρύθμιση Συσκευών Δικτύου

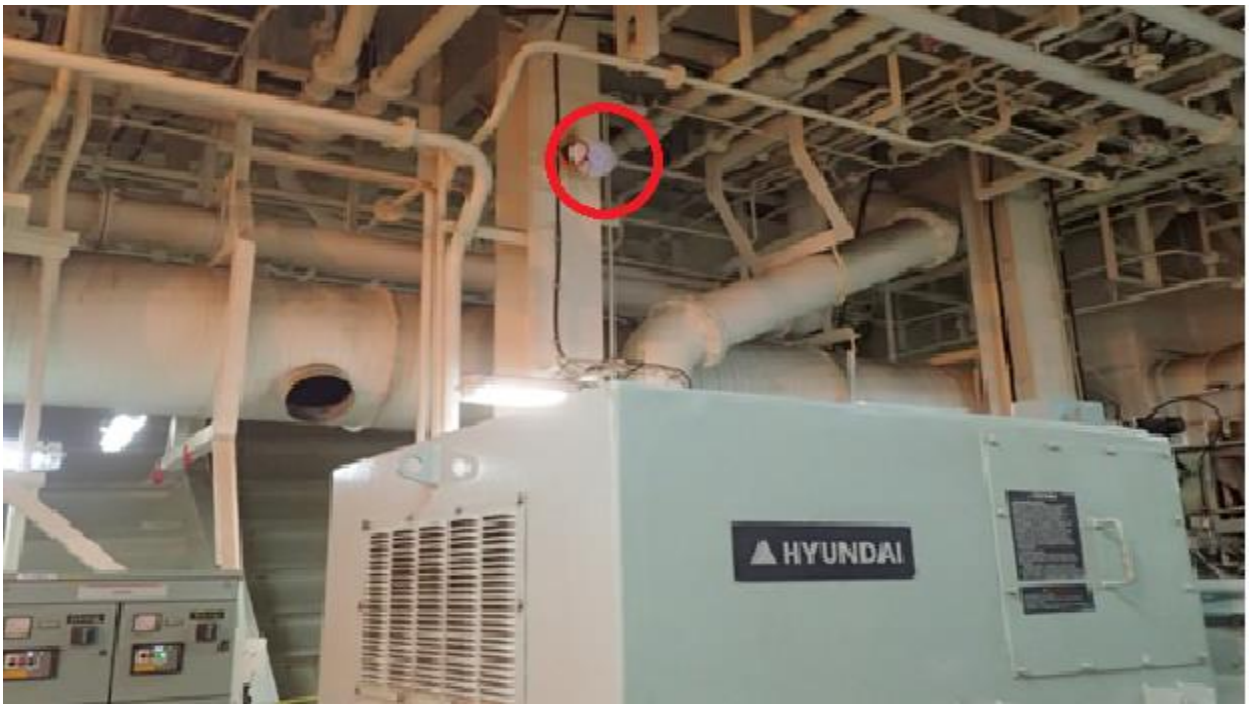
Ορισμένες άλλες προτάσεις που σχετίζονται με τις ρυθμίσεις του συστήματος είναι η εγκατάσταση προστατευτικού λογισμικού, όπως τα firewalls και τα antivirus, καθώς και η χρήση ασφαλών δορυφορικών συνδέσεων. Σύμφωνα με την BIMCO [55], τα συστήματα στο πλοίο δεν θα πρέπει να

αντιμετωπίζονται όλα με τον ίδιο τρόπο. Τα συστήματα θα πρέπει να συνδέονται με ελεγχόμενα ή μη ελεγχόμενα δίκτυα. Τα ελεγχόμενα δίκτυα έχουν σχεδιαστεί για να αποτρέπουν πιθανούς κινδύνους ασφαλείας από συνδεδεμένες συσκευές με τη χρήση firewalls, routers, switches. Τα μη ελεγχόμενα δίκτυα είναι ευάλωτα λόγω έλλειψης ελέγχου της κίνησης και θα πρέπει να απομονώνονται από τα ελεγχόμενα δίκτυα, καθώς η άμεση σύνδεση με το διαδίκτυο τα καθιστά επιρρεπή σε κακόβουλα προγράμματα. Για παράδειγμα, τα δίκτυα που είναι κρίσιμα για τη λειτουργία του πλοίου πρέπει να είναι ελεγχόμενα. Είναι κρίσιμης σημασίας τα συστήματα αυτά να έχουν υψηλό επίπεδο ασφάλειας. Επίσης, πρέπει να ελέγχονται τα δίκτυα που παρέχουν στους προμηθευτές απομακρυσμένη πρόσβαση στα συστήματα ναυσιπλοΐας και σε άλλα OT συστήματα του πλοίου. Αυτά τα δίκτυα ενδέχεται να είναι απαραίτητα για τους προμηθευτές ώστε να επιτρέπουν τη μεταφόρτωση των αναβαθμίσεων του συστήματος ή την απομακρυσμένη εκτέλεση εργασιών συντήρησης. Άλλα δίκτυα, όπως τα δίκτυα πρόσβασης επισκεπτών, ενδέχεται να είναι ανεξέλεγκτα, για παράδειγμα εκείνα που σχετίζονται με δραστηριότητες ψυχαγωγίας επιβατών ή ιδιωτική πρόσβαση στο διαδίκτυο για το πλήρωμα. Κανονικά, κάθε ασύρματο δίκτυο πρέπει να θεωρείται ανεξέλεγκτο.



Εικόνα 33: Ασύρματο Δίκτυο στο Πλοίο

Εικόνα 34: Ασύρματο στο Μηχανοστάσιο



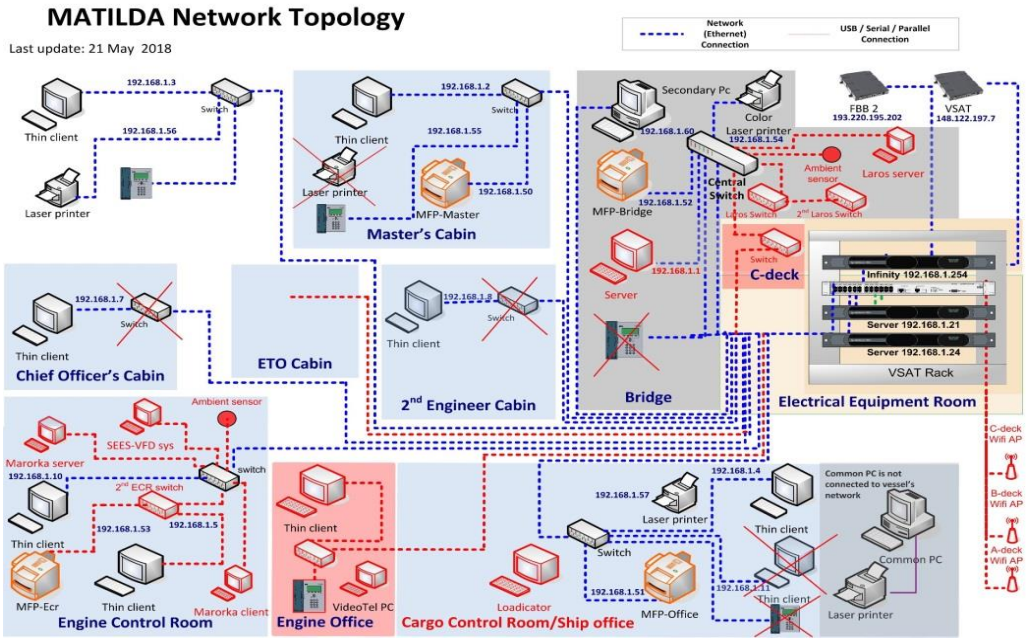
Εικόνα 35: Ασύρματο στο Μηχανοστάσιο

Κεφάλαιο 7.2.4: Ενημερώσεις Ασφαλείας

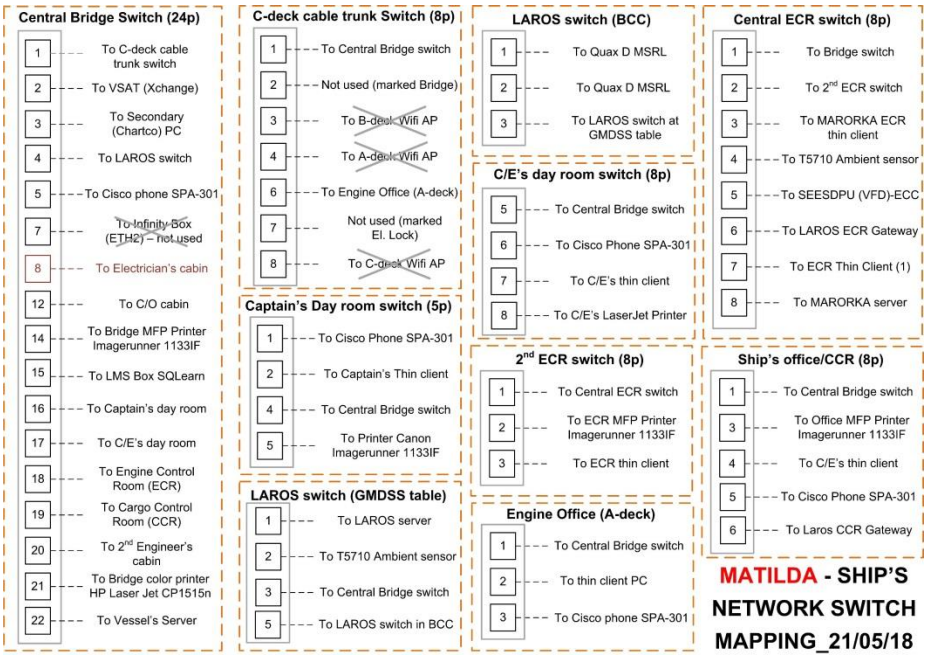
Οι ενημερώσεις ασφαλείας πρέπει να παρέχονται στα συστήματα του πλοίου. Αυτές οι ενημερώσεις θα πρέπει να εφαρμόζονται σωστά και έγκαιρα, ώστε να διασφαλίζεται ότι πιθανές ευπάθειες αντιμετωπίζονται πριν από την εκμετάλλευσή τους από κακόβουλους χρήστες. Οι αναβαθμίσεις του υλικού και του λογισμικού είναι απαραίτητες για τη διατήρηση της ασφάλειας σε υψηλά επίπεδα. Η εφαρμογή των ενημερώσεων και η διατήρηση της ασφαλούς διαμόρφωσης όλων των συστημάτων κατά τη διάρκεια του κύκλου ζωής τους είναι ένας πολύ σημαντικός παράγοντας που συμβάλλει στη διαδικασία μετριασμού του κινδύνου. Ιδιαίτερα τα ICS που έχουν κύκλο ζωής 20 έως 25 ετών θα πρέπει να αντιμετωπίζονται προσεκτικά και να ενημερώνονται τακτικά. Η ενημέρωση και η αναβάθμιση των συστημάτων επιτρέπει στον πάροχο λογισμικού να εφαρμόσει τα τελευταίες τεχνικές προστασίας στα προϊόντα του.

Κεφάλαιο 7. 3: Δικτυακή Υποδομή

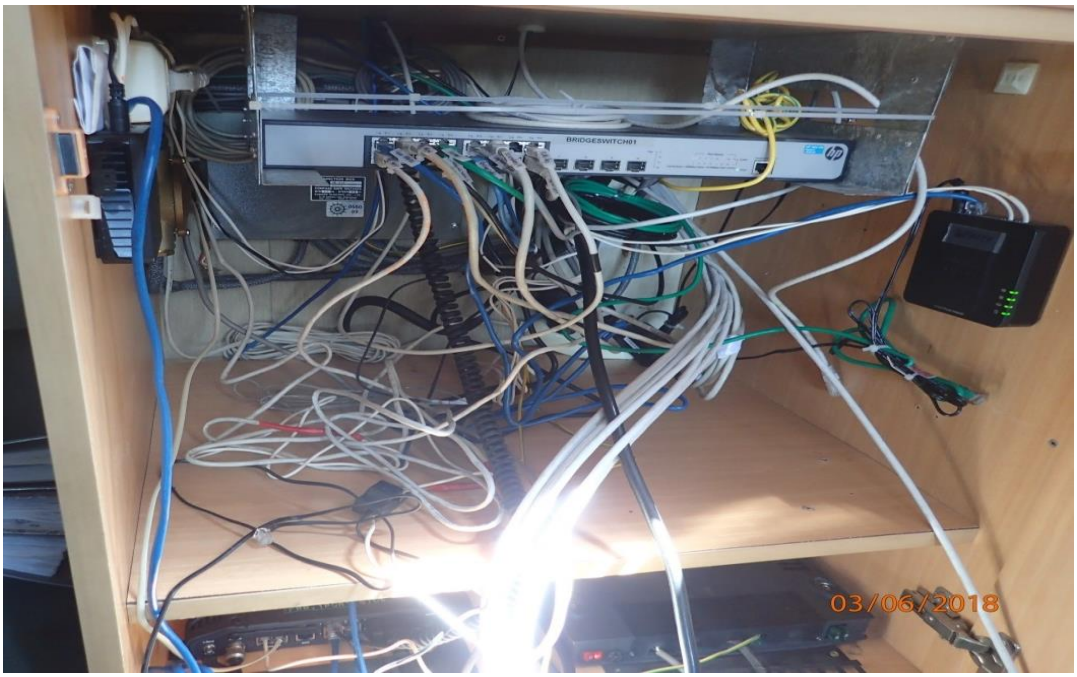
Μία κύρια ανησυχία κατά το σχεδιασμό ενός δικτύου θα πρέπει να είναι οι διασυνδέσεις μεταξύ των διαφόρων συστημάτων του πλοίου και της ξηράς. Η βασική ιδέα για τη δημιουργία μιας βελτιστοποιημένης τοπολογίας δικτύου είναι η εφαρμογή της έννοιας "Άμυνα-σε βάθος" που αυξάνει την ανθεκτικότητα του δικτύου με την κατάτμηση των στοιχείων του. Η άμυνα σε βάθος είναι μια πολιτική διασφάλισης που έχει σκοπό να προσφέρει πλεονασμό σε περίπτωση αποτυχίας ενός ελέγχου ασφαλείας ή εκμετάλλευσης μιας ευπάθειας. Παραδοσιακά, τα δίκτυα στα πλοία σχεδιάζονται σε ένα επίπεδο. Τα δίκτυα ενός επιπέδου, είναι μία προσέγγιση που έχει ως στόχο τη μείωση του κόστους συντήρησης και διαχείρισης. Τα επίπεδα δίκτυα μειώνουν τον αριθμό των δρομολογητών σε ένα δίκτυο υπολογιστών, συνδέοντας τη συσκευή σε ένα και όχι σε πολλαπλά switches. Ωστόσο, τα δίκτυα αυτού του τύπου αντιμετωπίζουν σημαντικά προβλήματα ασφαλείας. Δεν έχουν ενδιάμεσα όρια τα οποία χρησιμοποιούνται για να χωρίσουν την κίνηση του δικτύου και να ικανοποιήσουν τις απαιτήσεις της άμυνας σε βάθος [53]. Με την υλοποίηση ενός μοντέλου διαχωρισμού δικτύου, ο σχεδιαστής έχει τη δυνατότητα να ασφαλίζει κάθε ζώνη ξεχωριστά με firewalls και λίστες ελέγχου πρόσβασης (ACL), οι οποίες ελέγχουν το δίκτυο.



Εικόνα 36: Υποδομή Δικτύου



Εικόνα 37: Υποδομή Δικτύου



Εικόνα 38: Server σε Πλοίο

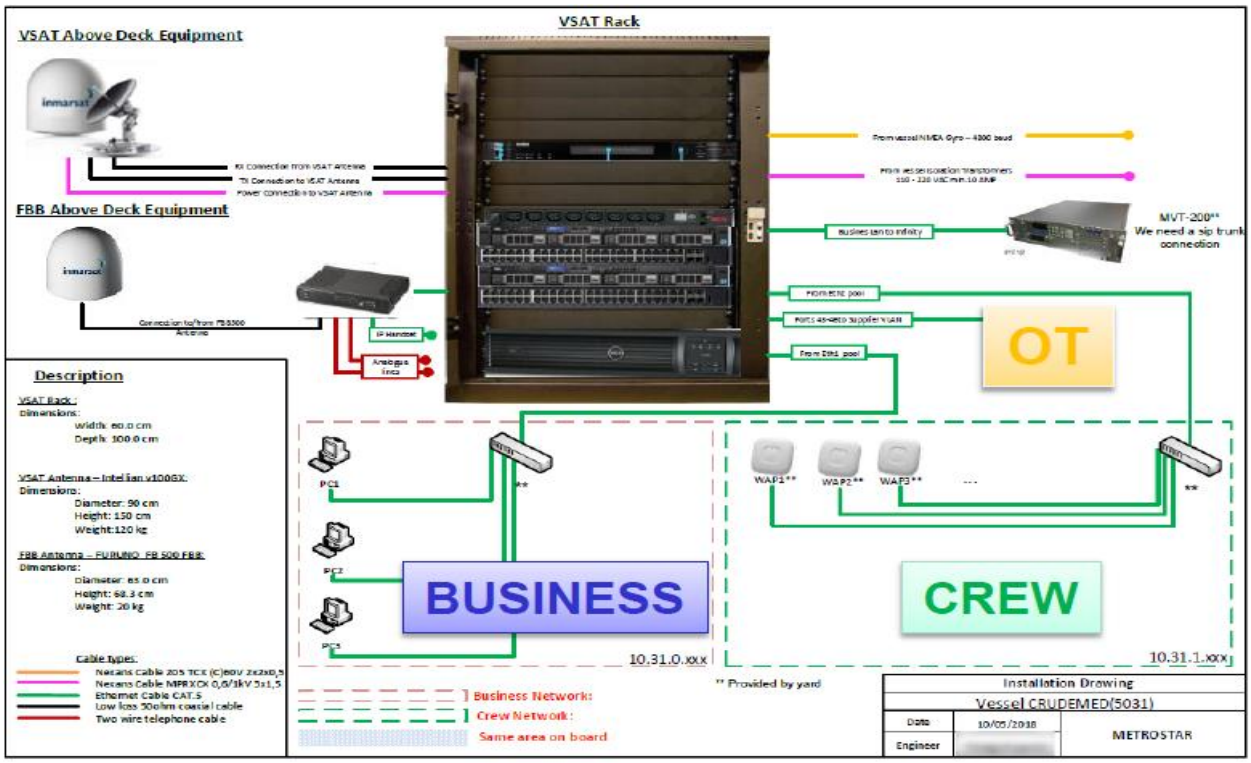
Εικόνα 39: Server σε Πλοίο

Οι ζώνες ασφαλείας είναι ένα χαρακτηριστικό της αρχιτεκτονικής δικτύου σε βάθος που εφαρμόζεται σε ένα δίκτυο πλοίου. Τα πιο κρίσιμα συστήματα του δικτύου που χρειάζονται καλύτερη προστασία βρίσκονται βαθύτερα στην τοπολογία. Με την υλοποίηση φραγμών όπως τα firewalls σε κάθε ζώνη, η

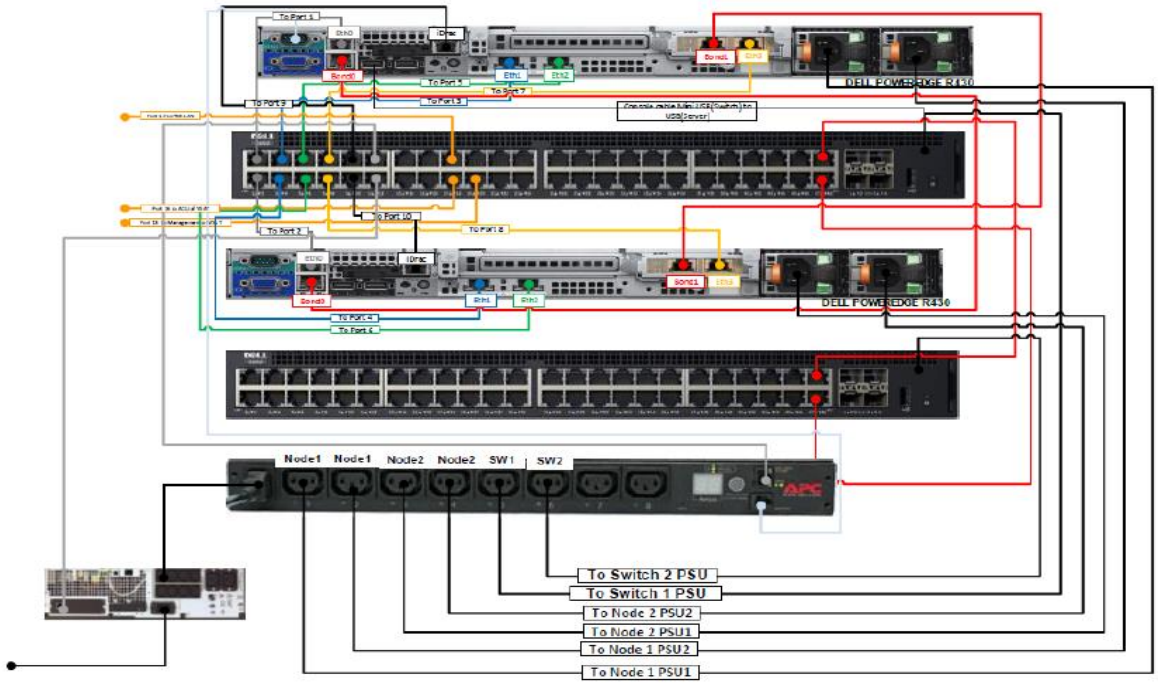
πρόσβαση στα κρίσιμα συστήματα του πλοίου απαιτεί τη διέλευση από τρία firewalls. Τα firewalls περιέχουν πολιτικές ασφάλειας που διαχειρίζονται ποιες διευθύνσεις IP επιτρέπονται ή δεν έχουν πρόσβαση σε κάθε ζώνη. Όπως αναλύθηκε στο κεφάλαιο 5, τα κρίσιμα συστήματα στο πλοίο είναι κυρίως εκείνα που συμβάλλουν στην πρόωση και πλοήγηση του. Η εκτίμηση κινδύνου πρέπει να διεξάγεται μεμονωμένα για κάθε εταιρεία, προκειμένου να προσδιοριστούν οι μοναδικές ανάγκες της για την προστασία κρίσιμων συστημάτων.

Παρόλο που η ανίχνευση σφαλμάτων είναι πολύ χρήσιμη για την προστασία του δικτύου, τα firewalls δεν μπορούν να χρησιμοποιηθούν ευρέως. Όταν δεν είναι σωστά ρυθμισμένα είναι ικανά να περιορίσουν όχι μόνο την ύποπτη αλλά και τη νόμιμη κίνηση και να προκαλέσουν επικίνδυνες συνέπειες για τα συστήματα. Αυτοί οι περιορισμοί μπορούν να μειώσουν την παραγωγικότητα και ακόμη και να αναγκάσουν τους χρήστες να προσπαθήσουν να χρησιμοποιήσουν κακόβουλους τρόπους για να μπορέσουν να εργαστούν στο δίκτυο. Επιπλέον, τα firewalls που βασίζονται σε λογισμικό έχουν το πρόσθετο μειονέκτημα της μείωσης της συνολικής απόδοσης μιας συσκευής επειδή χρησιμοποιούν την ισχύ του επεξεργαστή και τη μνήμη RAM για να λειτουργήσουν. Από την άλλη μεριά, τα firewalls που στηρίζονται στο υλικό δεν αντιμετωπίζουν το ίδιο πρόβλημα, ωστόσο είναι πολύ ακριβότερα και χρειάζονται εκπαιδευμένο προσωπικό για την εγκατάσταση, τον έλεγχο και τη συντήρησή τους σε ένα πλοίο.

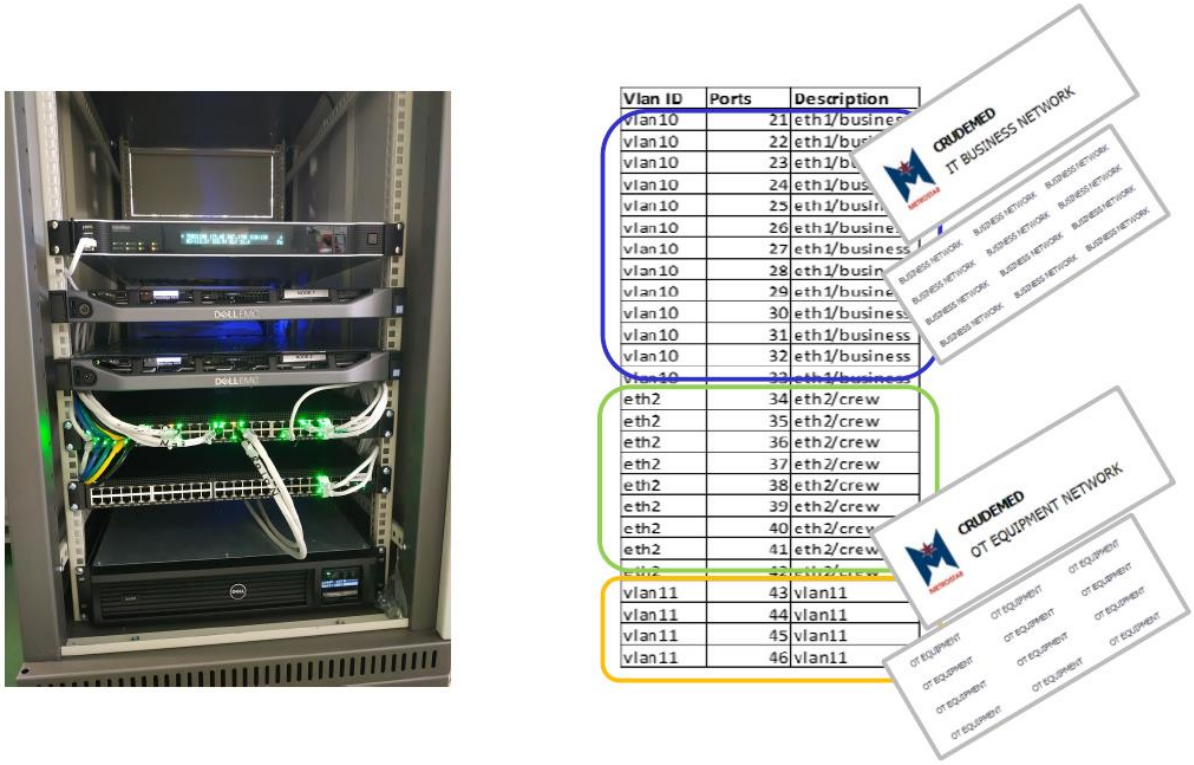
Εν κατακλείδι, η λεπτομερής εφαρμογή των βέλτιστων πρακτικών ασφαλείας στον κυβερνοχώρο θα πρέπει να στοχεύει στην "ασφάλεια κατά το σχεδιασμό" για όλα τα κρίσιμα συστήματα του πλοίου. Η αρχιτεκτονική δικτύου είναι μία από τις κύριες ανησυχίες για την διασφάλιση των συνδέσεων σε ένα πλοίο. Η επιλογή της κατάτμησης και της εφαρμογής φίλτρων στο δίκτυο θα πρέπει να σχεδιαστεί προσεκτικά και θα πρέπει να ληφθούν υπόψη όλες οι πτυχές προκειμένου να δημιουργηθεί η βέλτιστη ασφαλής λύση. Είναι πολύ σημαντικό τα πλοία να είναι ασφαλή απέναντι στις κυβερνό- απειλές από τη στιγμή σχεδιασμού τους. Αυτό σημαίνει ότι πραγματοποιείται ο σχεδιασμός της αρχιτεκτονικής με την κατανόηση των ζητημάτων ασφάλειας, κατά τρόπο τέτοιο που να ελαχιστοποιείται ο κίνδυνος σφαλμάτων που εισάγονται από κακόβουλους χρήστες.



Εικόνα 40: Διαχωρισμός Δικτύου



Εικόνα 41: Διαχωρισμός Δικτύου



Εικόνα 42: Διαχωρισμός Δικτύου

Κεφάλαιο 8: Μελλοντικές Προεκτάσεις

Η ναυτιλιακή βιομηχανία άρχισε πρόσφατα να υιοθετεί και να εφαρμόζει τις σύγχρονες τεχνολογίες, καθώς ο κύκλος ζωής των συστημάτων στα πλοία προσεγγίζει κατά μέσο όρο τα 20 χρόνια, σε ένα απαιτητικό και εχθρικό περιβάλλον. Ωστόσο, τα τελευταία χρόνια ο αριθμός των πλοίων που βασίζονται στον αυτοματισμό αυξάνεται ραγδαία, και οι εταιρείες επενδύουν σε τηλεχειριζόμενα συστήματα που επιτρέπουν την επικοινωνία οπουδήποτε και οποτεδήποτε [63]. Πρόσφατα, η Rolls-Royce ανακοίνωσε ότι μέχρι το 2020 σκοπεύει να δημιουργήσει ένα πλοίο το οποίο θα είναι εφικτό να λειτουργήσει με απομακρυσμένη πρόσβαση και ένα πλήρως αυτόνομο, μη επανδρωμένο πλοίο μέχρι το 2035 [64]. Είναι κοινά αποδεκτό ότι ένα μη επανδρωμένο πλοίο θα είναι εξαιρετικά ευάλωτο σε κυβερνό- επιθέσεις, καθώς η λειτουργία του θα εξαρτάται σε μεγάλο βαθμό από τις ICT τεχνολογίες, την υψηλή ενσωμάτωση συστημάτων και την αυξημένη συνδεσιμότητα με τα συστήματα της ξηράς και το Διαδίκτυο. Παρά την ευρεία αποδοχή ότι οι κίνδυνοι προέρχονται από την επιθυμία για αυτονομία, η βιβλιογραφία είναι σχετικά φτωχή ακόμα. Προκειμένου να αντιμετωπιστούν οι επικείμενες απειλές και να συζητηθεί λεπτομερώς το ζήτημα, θα πρέπει να υπάρξει μια συγκεκριμένη αρχιτεκτονική δικτύου βάσει της οποίας θα αξιολογηθούν τα συστήματα που αναπτύσσονται. Όπως προαναφέρθηκε, ένα από τα σοβαρότερα μειονεκτήματα της Βιομηχανίας είναι ότι το πλοίο είναι ένα πολύπλοκο σύνολο συστημάτων, διαφορετικών προμηθευτών, με μεγάλο κύκλο ζωής και είναι συχνό φαινόμενο η

ύπαρξη πλοίων που έχουν ελάχιστες ή καθόλου ομοιότητες μεταξύ τους όσον αφορά την τοπολογία του δικτύου. Επομένως, είναι δύσκολο να αναπτυχθεί και να εξεταστεί μια πιθανή αρχιτεκτονική δικτύου προκειμένου να υπάρξει μία ολιστική προσέγγιση του θέματος. Είναι πολύ σημαντικό να μπορέσει η βιομηχανία να αντιμετωπίσει αυτά τα προβλήματα προκειμένου να είναι ανθεκτική στις απειλές που προέρχονται από τον κυβερνοχώρο. Για το λόγο αυτό, θα ήταν χρήσιμη η μελέτη και αξιολόγηση διαφορετικών αρχιτεκτονικών δικτύου, εστιάζοντας στις ιδιαιτερότητες της Ναυτιλιακής Βιομηχανίας, και η παρουσίαση λύσεων στις οποίες τα συστήματα θα μπορούν να είναι ανθεκτικά απέναντι στις κυβερνό-απειλές.

Βιβλιογραφία

[1] (The Guidelines on Cyber Security Onboard Ships 2017, p. 5)

[2] DNV GL. Cyber security resilience management for ships and mobile offshore units in operation. Dnvgl-Rp-0496, (September), 2016

[3] Recommended Practice – "Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation, DNV GL, 2016,Available (10.8.2017)": https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cybersecurity-download.html

[4] (M. Lehto & A. Kähkönen, Kyberturvallisuuden kansallinen osaaminen, Jyväskylän yliopisto, 2015, 58 p. Available (19.9.2017): https://www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf/view)

[5] Guidelines on Maritime Cyber Risk Management 2017, p. 5

[6] J. Jorgensen, ABS CyberSafety™ , SOCP Webinar, 2016, 19 p. Available (20.9.2017): http://www.socp.us/images.html?file_id=40UY2UEl78k%3D

[7] The Guidelines on Cyber Security Onboard Ships 2017

[8] Recommended Practice – Cyber Security Resilience Management 2016

[9] Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016

[10] Lloyd's Register's (LR) Guidance Note "Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping

[11] Lloyd's Register's Approach to Assurance

[12] "Definition of Cybersecurity", ENISA (2016)

[13] 44 U. S. Code, Section 3542

[14] UNCTAD, Review of Maritime Transport 2017- 2018

[15] Gartner. IT glossary, digitalization, 2018 https://www.gartner.com/it-glossary/digitalization/

[16] Steinar L'ag, Peter Andersen, Bjorn-Johan Vartdal, and Knut Erik Knutsen Ship Connectivity DNV GL Strategic Research & Innovation Position Paper, 4:1–48, 2015

[17] Lloyd's Register. Hyundai heavy industries announce integrated smart ship solution - 2017

[18] Remi Eriksen and Group President: The digital era in shipping (February): 1–15 -2018

[19] The Future of Maritime Cyber Security page 34 - 2015

[20] Simon Beckett. Cyber Security, (September):18–22 - 2017

[21] Standardization Sector and O F ITU-T. 1205 - 2008

[22] TMSA-3-Cyber-Security-On-board-ships-1217, The Shipowners' Protection Limited, The Shipowners' Mutual Protection and Indemnity Association (Luxembourg)

[23] Lloyd's register, "Provisional Rules and Regulations for Software to be used in Naval Ships"- 2016

[24] "Cybersecurity, automated systems safety, data management and software assurance" (Cybersecurity – Guidance Notes for the Marine and Offshore Industries 2016, p. 2)

[25] CyberSafety – Volume 1 2016, p. 10

[26] J. Jorgensen 2016, p.11; CyberSafety™ – Volume 2 2016, p. 2-7

[27] CyberSafety – Volume 2 2016, p. 22

[28] CyberSafety – Volume 2 2016, p. 30

[29] CyberSafety - Volume 2 2016, p. 104

[30] MAERSK. A.P. Moller - Maersk A/S. (22756214), 2017

[31] Gartner. IT glossary, 2018. https://www.gartner.com/it-glossary/

[32] Information Security Audit and Control Association. The Merging of Cybersecurity and Operational Technology. pages 1–8, 2016

[33] K. Stouffer, J. Falco, and K. Kent, "Guide to Supervisory Control and Data Acquisition {(SCADA)} and Industrial Control Systems Security", {Recommendations} of the {NIST}, (800-82)- 2006

[34] Kaspersky Lab ICS CERT Threat, "Threat Landscape for Industrial Automation Systems in H2 2017, pages 1997–2018- 2018"

[35] Richard Benham and James Sproule "Cyber Security, IOD Policy Report March", (March):177, 2017

[36] Michael Holloway "Stuxnet worm attack on Iranian nuclear facilities", Retrieved 13 April 2017

[37] David Kushner, "The real story of Stuxnet, 2013, https://spectrum. ieee.org/telecom/security/the-real-story-of- Stuxnet"

[38] Lagner, "A time bomb with fourteen bytes, 2011", https: //www.langner.com/2011/07/a-time-bomb-with-fourteen-bytes/ #more-1028

[39] Steve LaValle, Michael S Hopkins, Eric Lesser, Rebecca Shockley, and Nina Kruschwitz, "Analytics: The new path to value", MIT Sloan Management Review, 52(1):1–25, 2010

[40] "Cyber security survey in association with BIMCO, (September):1017206" - 2016

[41] “Symantec, ISTR Internet Security Threat Report, Internet Security Threat Report” - 23, 2018

[42] “Futurenautics Research, Crew Connectivity 2018” Survey Report, page 36 - 2018

[43] Hugh Boyes and Roy Isbell, “Code of Practice: Cyber Security for Ships”- 2017

[44] Eugene Ternovskiy “Position sources for ecdis” - 2018, https: //www.nautinst.org/en/forums/ecdis/ecdis-issues-gen.cfm/ G3userexp

[45] Svante Einarsson, Cyber and information security applicable for the maritime sector, (June):1–20, 2016

[46] “Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems”, https://www.iso.org/standard/52075.html

[47] Louis Marinos, Adrian Belmonte, and Evangelos Rekleitis, “Enisa threat landscape 2015”, European Union Agency for Network and Information Security, page 18, 2016

[48] Richard Kissel, Kevin Stine, Matthew Scholl, Hart Rossman, Jim Fahlsing, and Jessica Gulick, NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, October, Retrieved on, 26(October):800–864, 2008

[49] Tom Bateman, “Police warning after drug traffickers’ cyber-attack” - 2013, https://www.bbc.com/news/world-europe-24539417

[50] “The Local State-sponsored hackers spied on Denmark” - 2014, https://www.thelocal.dk/20140922/ denmark-was-hacked-by-state-sponsored-spies

[51] “Jacob Gronholt-Pedersen, Maersk says global it breakdown caused by cyber attack” - 2017 ,https://www.reuters.com/article/ us-cyber-attack-maersk-idUSKBN19I1NO

[52] “Peter Sayer, Ukrainian police seize computers that spread global notpetya attack” - 2017, https://www.pcworld.idg.com.au/article/621464/ ukrainian-police-seize-computers-spread-global-notpetya-attack/

[53] “Richard Dreger, How to secure your flat network” – 2012, https://www.networkcomputing.com/networking/ how-secure-your-flat-network/1580786430

[54] “Chris Baraniuk, How hackers are targeting the shipping industry” - 2017, https://www.bbc.com/news/technology-40685821.

[55] “BIMCO, The guidelines on Cyber Security onboard ships” – 2017

[56] “Kai Hansen and Akilur Rahman, Cyber threat to ships – real but manageable” - 2013