ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ

ΕΠΙΚΟΙΝΩΝΙΩΝΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Το πλαίσιο κυβερνοασφάλειας NIST στην ναυτιλία Nist Cybersecurity framework in maritime environment
Ονοματεπώνυμο Φοιτητή	ΙΩΑΝΝΗΣ ΜΙΣΣΑΣ
Πατρώνυμο	ΚΩΝΣΤΑΝΤΙΝΟΣ
Αριθμός Μητρώου	Π/ 19105
Επιβλέπων	ΔΟΥΛΗΓΕΡΗΣ ΧΡΗΣΤΟΣ

Ημερομηνία Παράδοσης: Σεπτέμβριος 2024

Copyright ©

Ευχαριστίες

Αρχικά, θέλω να ευχαριστήσω περισσότερο απ' όλους τους γονείς μου, που μου δίνουν πάντα δύναμη και με έκαναν τον άνθρωπο που είμαι σήμερα. Χωρίς την εμπιστοσύνη τους και την αγάπη τόσο η προσωπική όσο και η ακαδημαϊκή μου πορεία θα γέμιζε κενά. Θέλω, ακόμα, να ευχαριστήσω τον καθηγητή μου Δουλεγέρη Χρήστο, που διέκρινε σε εμένα τις ικανότητες και προοπτικές που διαθέτω και συνέβαλε καθοριστικά στην εκπόνηση αυτής πτυχιακής εργασίας. Τέλος, ένα μεγάλο ευχαριστώ σε όλους όσους πίστεψαν σε εμένα και μου έδωσαν δύναμη να συνεχίσω.

Περίληψη

Τα σχέδια για την πρόληψη και τον μετριασμό των τρωτών σημείων στα δίκτυα υπολογιστών είναι γνωστά ως πλαίσια κυβερνοασφάλειας. Ένα «πλαίσιο κυβερνοασφάλειας» είναι μια συλλογή διεθνών προτύπων και βέλτιστωνπρακτικών. Με τη βοήθεια του πλαισίου κυβερνοασφάλειας, οι οργανισμοί μπορούν να μειώσουν την ευπάθειά τους σε επιθέσεις στον κυβερνοχώρο και να βελτιώσουν την ισχύ της άμυνάς τους. Το θέμα της διπλωματικής μου εργασίας είναι η εφαρμογή του πλαισίου κυβερνοασφάλειας NIST στο πλαίσιο της ναυτιλιακής βιομηχανίας, εστιάζοντας στη σημασία της κυβερνοασφάλειας όσον αφορά τις επιχειρησιακές τεχνολογίες και τις τεχνολογίες πληροφοριών της ναυτιλίας. Δεδομένου ότι ο κλάδος έχει εξαρτηθεί σε μεγάλο βαθμό από τα διασυνδεδεμένα συστήματα για τη ναυσιπλοΐα, την επικοινωνία και την εφοδιαστική, η έρευνα αυτή θα ρίξει φως στις προκλήσεις της κυβερνοασφάλειας που αντιμετωπίζουν οι ναυτιλιακές εταιρείες και θα αναδείξει τη ζήτηση για πλαίσια όπως το NIST CSF για την προστασία από τις απειλές στον κυβερνοχώρο. Η μελέτη θα δώσει αρχικά μια ιστορική επισκόπηση του τρόπου με τον οποίο αναπτύχθηκε το NIST και της αποστολής του, θέτοντας έτσι θεμελιώδη ρόλο στη θέσπιση προτύπων στην κυβερνοασφάλεια. Στη συνέχεια, θα εμβαθύνει σε λεπτομέρειες σχετικά με το CSF του NIST και θα διερευνήσει τις λεπτομέρειες των συστατικών στοιχείων, συμπεριλαμβανομένων των στοιχείων Identify, PrOTect, Detect, Respond και Recover, στις ναυτικές επιχειρήσεις. Οι ενότητες θα είναι σημαντικές για την αξιολόγηση των πρακτικών διαχείρισης κινδύνου, των τρωτών σημείων στα ναυτιλιακά συστήματα OT -για παράδειγμα, τα συστήματα ελέγχου πρόωσης και πλοήγησης μεταξύ άλλων- και των στοιχείων IT, όπως τα δίκτυα επικοινωνιών. Η παρούσα πτυχιακή θέτει το πλαίσιο NIST σε μια συγκριτική προοπτική σε σχέση με άλλα πρωτόκολλα κυβερνοασφάλειας, τονίζοντας την προσαρμοστικότητα του NIST σε διάφορες οργανωτικές δομές τόσο σε επίπεδο μεγάλων ναυτιλιακών επιχειρήσεων όσο και σε επίπεδο μικρότερων φορέων. Μελέτες περιπτώσεων και στατιστικές αναλύσεις τεκμηριώνουν περαιτέρω το γεγονός ότι το πλαίσιο κυβερνοασφάλειας του NIST μπορεί να χρησιμοποιηθεί για τον εντοπισμό, τη διαχείριση και την ανάπτυξη στρατηγικών αντιμετώπισης περιστατικών με φόντο τον ναυτιλιακό τομέα. Χρησιμεύει για την παροχή συστάσεων σχετικά με την εφαρμογή ελέγχων κυβερνοασφάλειας για τους ναυτιλιακούς οργανισμούς σύμφωνα με τις κατευθυντήριες γραμμές που ορίζει το NIST, αναπτύσσοντας ανθεκτικότητα από τις επιπτώσεις που επιφέρουν οι κυβερνοεπιθέσεις στη ζωή και τη συνεχή λειτουργία των ναυτιλιακών συστημάτων. Στη συνέχεια, παρουσιάζεται μια εφαρμοσμένη ανάλυση με τη χρήση δεδομένων από μια πραγματική ναυτιλιακή εταιρεία για να καταδειχθούν οι πρακτικές εφαρμογές διαχείρισης κινδύνων, ο σχεδιασμός έκτακτης ανάγκης και να γίνει η σύγκριση με άλλα πλαίσια. Το κεφάλαιο αυτό καταδεικνύει πώς το πλαίσιο κυβερνοασφάλειας ενισχύει την ανθεκτικότητα ενός οργανισμού έναντι των απειλών στον κυβερνοχώρο, προσδίδοντας στη μελέτη ένα επίπεδο πρακτικής αυθεντικότητας.
Στο τέλος, συνοψίζονται τα ευρήματα μου και παρέχω συμπεράσματα σχετικά με την αποτελεσματικότητα του πλαισίου στη ναυτιλιακή βιομηχανία, ενισχύοντας τη σημασία των δομημένων πρακτικών κυβερνοασφάλειας για τη διασφάλιση της επιχειρησιακής ασφάλειας και συμμόρφωσης

Λέξεις Κλειδιά: Κυβερνοασφάλεια, Πλαίσιο Κυβερνοασφάλειας, CSF, το πλαίσιο κυβερνοασφάλειας NIST, Ναυτιλιακή βιομηχανία, Διαχείριση κινδύνων, Επιχειρησιακή τεχνολογία, Τεχνολογία πληροφοριών

Abstract

Plans for preventing and mitigating Vulnerabilities in computer networks are known as Cybersecurity frameworks. A "cybersecurity framework» is a collection of international standards and best practices. With the assistance of the Cybersecurity Framework, organizations can reduce their vulnerability to cyber-attacks and improve the strength of their defenses. The topic of my thesis is to apply the NIST Cybersecurity Framework within the marine time industry, focusing on the importance of Cybersecurity concerning Marine time operational technologies and information technologies. Given that the industry has become very dependent on interconnected systems for navigation, communication, and logistics, such research will shed light on the challenges of Cybersecurity facing marine time companies and highlight the demand for such frameworks as the NIST CSF to protect against cyber threats. The study will first give a historical overview of how NIST was developed and ITs mission, thus setting a foundational role in setting standards in Cybersecurity. Then, IT will delve deep into details regarding the NIST CSF and explore the details of the components, including Identify, Protect, Detect, Respond, and Recover, in marine time operations. Sections will be important in the assessment of risk management practices, Vulnerabilities in marine time OT systems-for instance, propulsion controls and navigation controls amongst Other-and IT components like communications networks. This thesis puts the NIST framework into a comparative perspective in relation to other Cybersecurity Protocols, stressing the adaptability of NIST to various organizational structures at both the level of large marine time enterprises and the smaller operators. Case studies and statistical analyses further establish the fact that the NIST CSF can be used to identify, manage, and develop incident response strategies against the background of the marine time sector. IT serves to provide recommendations on implementing Cybersecurity controls for marine time organizations in line with the guidelines laid down by NIST, developing resilience from the impacts brought about by cyberattacks on life and continuous operations of marine time systems. Furthermore, an applied analysis is then presented using data from a real shipping company to demonstrate practical applications of risk management, contingency planning and comparison with other contexts. This chapter demonstrates how the cyberSecurity framework enhances an organization’s resilience against cyber threats, adding a level of practical authenticity to the study. In the end, I summarize my findings and provide conclusions on the effectiveness of the framework in the marine time industry, reinforcing the importance of structured Cybersecurity practices in ensuring operational Security and compliance

Key Words: Cyber Security, Cyber Security Framework, CSF, NIST CyberSecurity Framework, Marinetime Industry, Risk Management, Operational Technology, Information Technology

Πίνακας Περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Εισαγωγή

Σε αυτήν την Ενότητα γίνεται μια αναδρομή στον χρόνο για την πορεία και την εξέλιξη του NIST. Στην παρούσα πτυχιακή θα αναλυθεί το πλαίσιο κυβερνοασφάλειας του NIST. Η ναυτιλία είναι ένας κλάδος ανερχόμενος και άκρως σημαντικό στον βιοπορισμό των ανθρώπων. Παράλληλα όμως, είναι ένας κλάδος ο οποίος συνεχίζει να εξελίσσεται και τα συστήματα που χρησιμοποιεί δεν συμβαδίζουν με αυτά του βιομηχανικού τομέα. Ως συνέπεια αυτού, η κίνηση του δικτύου και ο διαμοιρασμός πληροφοριών από και προς ένα εμπορικό πλοίο, μπορεί να είναι ευάλωτα και με ιδιαίτερο ενδιαφέρον προς τους κακόβουλους χρήστες. Οι κίνδυνοι που παραμονεύουν διαφέρουν και τα μέτρα που πρέπει να ληφθούν πρέπει να είναι άμεσα και καθοριστικά. Οι εταιρείες των πλοίων δεν μπορούν πλέον να αρκεστούν στην προστασία του παρόχου και οφείλουν να λάβουν πιο σοβαρά τα ζητήματα της κυβερνοασφάλειας καθώς πλέον οι επιθέσεις ανέρχονται σε μεγάλο βαθμό με τα παραδείγματα να ποικίλουν, όπως θα αναφερθούν κάποια στη συνέχεια των κεφαλαίων. Η ναυτιλία αποτελεί αναπόσπαστο κομμάτι των μεταφορών πρώτων υλών, αγαθών ή ακόμη και καυσίμων και δεν θα μπορούσε να αναιρεθεί η λειτουργικότητα της. Ωστόσο, για την ομαλή διένεξη των παραπάνω, θα πρέπει να εξασφαλιστεί η ασφάλεια του δικτύου στον τομέα της ναυτιλίας και των επικοινωνιών Η παρούσα πτυχιακή εξετάζει την εφαρμογή του Πλαισίου Κυβερνοασφάλειας (CSF) του NIST στον ναυτιλιακό τομέα, εστιάζοντας στον τρόπο με τον οποίο αντιμετωπίζει τους κινδύνους κυβερνοασφάλειας που σχετίζονται τόσο με τα επιχειρησιακά συστήματα όσο και με τα συστήματα τεχνολογίας πληροφοριών.

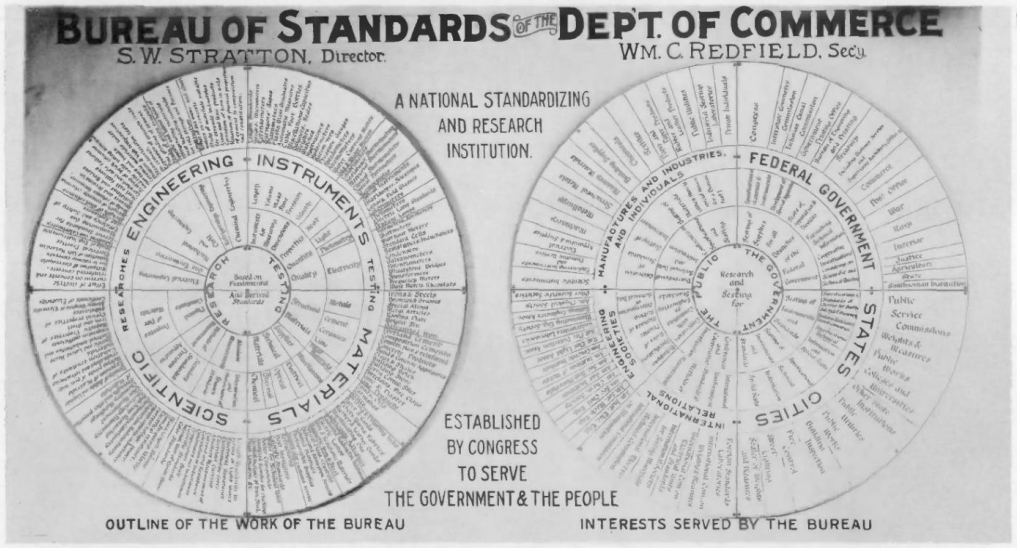
1. Τι είναι το NIST

1.1 Ιστορική Αναδρομή του NIST

1.1.1 Σημαντικές εξελίξεις

Τα Άρθρα της Συνομοσπονδίας ήταν μια συμφωνία μεταξύ των 13 πολιτειών των Ηνωμένων Πολιτειών, πρώην Δεκατριών Αποικιών, που χρησίμευε ως το πρώτο πλαίσιο διακυβέρνησης του έθνους[1]. Επικυρώθηκε από τις αποικίες το 1781, υπό τον όρο: Οι Ηνωμένες Πολιτείες στο Κογκρέσο που συγκεντρώθηκαν θα έχουν το μοναδικό και αποκλειστικό δικαίωμα και την εξουσία να ρυθμίζουν το κράμα και την αξία του νομίσματος που κόβεται από τη δική τους αρχή ή από αυτή των αντίστοιχων πολιτειών—καθορίζοντας τα πρότυπα βαρών και μέτρων σε όλες τις Ηνωμένες Πολιτείες. Το άρθρο 1, τμήμα 8, του Συντάγματος των Ηνωμένων Πολιτειών, που επικυρώθηκε το 1789, παραχώρησε αυτές τις εξουσίες στο νέο Κογκρέσο: «Το Κογκρέσο θα έχει την εξουσία... Να κερδίζει χρήματα, να ρυθμίζει την αξία τους και ξένων νομισμάτων, και καθορίστε το πρότυπο των βαρών και των μέτρων». Έπειτα από αλλαγές που επήλθαν πάνω στα πρότυπα μέτρησης, Βαρών και αξίας-δημιουργίας νομισμάτων από μελλοντικούς Προέδρους των Ηνωμένων Πολιτειών Αμερικής κατάφερε η κυβέρνηση των Ηνωμένων Πολιτειών το 1838 και υιοθέτησε ένα ενιαίο σύνολο προτύπων. Από το 1830 έως το 1901, ο ρόλος της επίβλεψης των βαρών και των μέτρων ασκούνταν από το Γραφείο Τυποποιημένων Βαρών και Μετρήσεων, το οποίο ήταν μέρος της Έρευνας της Ακτής - μετονομάστηκε σε Έρευνα Ακτών των Ηνωμένων Πολιτειών το 1836 και Έρευνα Ακτών και Γεωδαιτικών Ηνωμένων Πολιτειών το 1878—στο Υπουργείο Οικονομικών των Ηνωμένων Πολιτειών.

Το Εθνικό Γραφείο Προτύπων, που ναυλώθηκε από το Κογκρέσο των ΗΠΑ στις 3 Μαρτίου 1901, ως απάντηση σε ένα νομοσχέδιο που προτάθηκε από τον βουλευτή James H. Southard (R, Ohio), ιδρύθηκε με την εντολή να παρέχει τυπικά βάρη και μέτρα και να λειτουργεί ως το εθνικό φυσικό εργαστήριο για τις Ηνωμένες Πολιτείες. Ο Southard είχε προηγουμένως χορηγήσει ένα νομοσχέδιο για τη μετρική μετατροπή των Ηνωμένων Πολιτειών. [2]



Εικόνα 1. Διάγραμμα δραστηριοτήτων NBS, 1915 [2]

Το Προεδρείο ανέλαβε τη φύλαξη των αντιγράφων των ράβδων κιλών και μετρητών που αποτελούσαν τα πρότυπα για τα μέτρα των ΗΠΑ και δημιούργησε ένα πρόγραμμα για την παροχή υπηρεσιών μετρολογίας σε επιστημονικούς και εμπορικούς χρήστες των Ηνωμένων Πολιτειών. Εκτός από τα βάρη και τα μέτρα, το Γραφείο ανέπτυξε όργανα για ηλεκτρικές μονάδες και για μέτρηση φωτός. Το 1905 συγκλήθηκε μια συνάντηση που θα ήταν η πρώτη «Εθνική Διάσκεψη για τα Βάρη και τα Μέτρα».

Εκείνη την εποχή, οι Ηνωμένες Πολιτείες είχαν ελάχιστα, έως καθόλου, έγκυρα εθνικά πρότυπα για οποιεσδήποτε ποσότητες ή προϊόντα. Αυτό που είχε ήταν ένα συνονθύλευμα τοπικά και περιφερειακά εφαρμοσμένων προτύπων, συχνά αυθαίρετων, που αποτελούσαν πηγή σύγχυσης στο εμπόριο. Ήταν δύσκολο για τους Αμερικανούς να διεξάγουν δίκαιες συναλλαγές ή να ταιριάζουν σωστά τα εξαρτήματα μεταξύ τους. Τα υλικά κατασκευής ήταν ανομοιόμορφης ποιότητας και τα οικιακά προϊόντα ήταν αναξιόπιστα. Λίγοι Αμερικανοί εργάστηκαν ως επιστήμονες, επειδή οι περισσότερες επιστημονικές εργασίες βασίστηκαν στο εξωτερικό. Ωστόσο, οι Ηνωμένες Πολιτείες έγιναν παγκόσμια δύναμη και η ανάγκη για καθιερωμένα εργαστήρια προτύπων, ένας οργανισμός υπεύθυνος για τη ρύθμιση των προτύπων βαρών και μέτρων στις Ηνωμένες Πολιτείες συζητήθηκε για πολλά χρόνια από επιστήμονες και μηχανικούς. Η αναπτυσσόμενη ηλεκτρική βιομηχανία χρειαζόταν όργανα μέτρησης και συχνά συμμετείχε σε δικαστικές διαφορές λόγω της έλλειψης προτύπων. Τα αμερικανικά όργανα έπρεπε να σταλούν στο εξωτερικό για βαθμονόμηση. Το έθνος είχε ήδη γραφείο σταθμών και μέτρων. Οι πρώτες προσπάθειες για την παροχή ακριβών (αν και μη νόμιμων) προτύπων βαρών και μέτρων έγιναν τη δεκαετία του 1830 από τον Ferdinand Rudolph Hassler, έναν Ελβετό μηχανικό και μετρολόγο που μετανάστευσε στις Ηνωμένες Πολιτείες και έγινε ο πρώτος επιθεωρητής βαρών και μέτρων. Αλλά το γραφείο είχε λίγους υπαλλήλους και σε κάποιους δεν άρεσε η ιδέα της ομοσπονδιακής κυβέρνησης να επιβάλλει πρότυπα ή οτιδήποτε άλλο στη βιομηχανία.

THE EVENING STAR, MONDAY, MARCH 11, 1901

CORRECT MEASURES

Function of the New Bureau of Standards.

LABORATORY TO BE ERECTED

Prof. Stratton, the Director, Details Need of Establishment.

A HANDICAP REMOVED

A new bureau of the government, authorized by the last Congress, will be established in this city in the near future and will give employment to a number of persons. It is to be known as the national bureau of standards and is to be under the control of the Treasury Department. A separate building for a laboratory, to cost not to exceed $250,000, is to be erected on a site to be purchased at a cost of $25,000.

Mr. Samuel W. Stratton of Chicago has been appointed by the President to be chief of the bureau at an annual salary of $5,000. Prof. Stratton is to have the following assistants, to be appointed by the Secretary of the Treasury: One physicist, at an annual salary of $3,500; one chemist, at $3,500; two assistant physicists or chemists, each at an annual salary of $2,200; one laboratory assistant, at $1,800; one laboratory assistant, at $1,200; one secretary, at $2,000; one clerk, at $1,200; one messenger, at $720; one en-

Director Stratton.

Εικόνα 2. Bureau of Standards, που αργότερα άλλαξε σε NIST, η ίδρυση περιγράφηκε στην έκδοση του The Evening Star στις 11 Μαρτίου 1901 [2].

Το NIST αρχικά ήταν μέρος του Υπουργείου Οικονομικών, στη συνέχεια μεταφέρθηκε στο Υπουργείο Εμπορίου και Εργασίας, αργότερα χωρίστηκε σε δύο μονάδες. Το Ινστιτούτο πήγε με το Υπουργείο Εμπορίου, όπου παραμένει σήμερα. Ο Samuel W. Stratton, καθηγητής φυσικής στο Πανεπιστήμιο του Σικάγο, έγινε ο πρώτος διευθυντής, θέση που κράτησε για 21 χρόνια. [3] Το αρχικό προσωπικό ήταν 12. Μετά από αρκετά χρόνια σε προσωρινούς χώρους, το NIST μετακόμισε σε μια τοποθεσία στη λεωφόρο Κονέκτικατ στην περιοχή της Κολούμπια, λίγα μίλια από τον Λευκό Οίκο. Τα επιστημονικά και τεχνολογικά προγράμματα ξεκίνησαν από το μηδέν. Μετά τη βελτίωση των προτύπων ηλεκτρικής μέτρησης, το NIST ανέπτυξε γρήγορα καλύτερα πρότυπα μήκους και μάζας και νέα πρότυπα θερμοκρασίας, φωτός και χρόνου. Το Ινστιτούτο καθιέρωσε επίσης πρότυπα ασφάλειας στο εμπόριο και τη βιομηχανία και την απόδοση μεταξύ των δημόσιων επιχειρήσεων κοινής ωφέλειας, και προετοίμασε και διατήρησε εκατοντάδες τυπικά δείγματα υλικών που βοήθησαν στην εισαγωγή ποιοτικού ελέγχου στη βιομηχανία των ΗΠΑ.

-Η ανάπτυξη της πρώτης ψηφιακής υπολογιστικής μηχανής ENIAC (Electronic Numerical Integrator and Computer) υποστηρίχθηκε από το NBS.

-Συμμετοχή στην ανάπτυξη ατομικών προτύπων μέτρησης, ειδικά του ατομικού ρολογιού.

-Στη δεκαετία του 1960 και του 1970, το NBS συνέχισε να αναπτύσσει νέα εθνικά πρότυπα, ειδικά σε τομείς όπως τα ηλεκτρονικά, η τηλεπικοινωνία και η μικροηλεκτρονική. Παράλληλα, άρχισε να επεκτείνεται στη διαχείριση και ασφάλεια πληροφοριών καθώς η τεχνολογία άρχισε να παίζει μεγαλύτερο ρόλο στην καθημερινή ζωή και τις βιομηχανίες.

-Το 1988, το όνομα άλλαξε από National Bureau of Standards σε National Instituteof Standards and Technology (NIST) για να αντικατοπτρίζει τις αλλαγές στην αποστολή του οργανισμού, που πλέον επικεντρωνόταν σε νέες τεχνολογίες και στις ανάγκες της ψηφιακής εποχής [5].

-NIST και Οικονομία Πληροφορίας (1988-Σήμερα): Με τη μετονομασία του, το NIST εισήλθε στη σύγχρονη εποχή, παίζοντας καθοριστικό ρόλο στην ανάπτυξη και ασφάλεια τεχνολογιών όπως οι υπολογιστές, οι επικοινωνίες, και το διαδίκτυο.

-Κατά τη διάρκεια της δεκαετίας του 1990 και 2000, το NIST ενσωμάτωσε τις πιο πρόσφατες εξελίξεις της πληροφορικής στην αποστολή του. Έγινε γνωστό για την ανάπτυξη προτύπων στον τομέα της κυβερνοασφάλειας, με κορυφαίο επίτευγμα το NIST CyberSecurity Framework (CSF) το 2014, το οποίο χρησιμοποιείται από ιδιωτικές και δημόσιες επιχειρήσεις παγκοσμίως για την προστασία τους από κυβερνοαπειλές.

1.1.2 Προγράμματα και Πρωτοβουλίες

Το NIST υλοποιεί διάφορα ερευνητικά προγράμματα και πρωτοβουλίες που στοχεύουν στη βελτίωση της τεχνολογίας και των προτύπων. Μερικά από τα πιο σημαντικά είναι τα παρακάτω.

Baldrige Performance Excellence Program: Ένα εθνικό πρόγραμμα που προωθεί την επιχειρησιακή αριστεία στις ΗΠΑ και βοηθά τους οργανισμούς να βελτιώσουν την ποιότητα και τις διαδικασίες τους.
Smart Grid Program: Στοχεύει στην ανάπτυξη προτύπων και τεχνολογιών για τον εκσυγχρονισμό του ενεργειακού δικτύου των ΗΠΑ, προκειμένου να γίνει πιο ανθεκτικό και αποδοτικό. Έτσι το NIST επηρεάζει σε μεγάλο βαθμό των τομέα των έξυπνων δικτύων και ενέργειας.

Quantum Science: Το NIST βρίσκεται στην αιχμή της κβαντικής έρευνας, συμβάλλοντας στην ανάπτυξη κβαντικών υπολογιστικών συστημάτων και κρυπτογραφίας δίνοντας κατευθυντήριες γραμμές και στον τομέα της κβαντικής τεχνολογίας.

Advanced Manufacturing: Μέσα από πρωτοβουλίες όπως το Manufacturing USA, το NIST συνεργάζεται με τη βιομηχανία και τον ακαδημαϊκό χώρο για την ανάπτυξη προηγμένων κατασκευαστικών τεχνολογιών ώστε να βοηθήσει την εξέλιξη του τομέα: Βιομηχανική Ανάπτυξη και Προηγμένες Κατασκευές καθώς και την Ανθεκτικότητα Υποδομών και Κατασκευών

NIST CyberSecurity Framework (CSF): Το πλαίσιο αυτό με το οποίο θα ασχοληθούμε περαιτέρω στην συνέχεια της ερευνητικής αυτής εργασίας είναι ένα από τα πλέον γνωστά προγράμματα του NIST. Παρέχει ένα πλαίσιο διαχείρισης κυβερνοασφάλειας που χρησιμοποιείται από κυβερνητικούς οργανισμούς και ιδιωτικές εταιρείες παγκοσμίως[4].
Σημαντικές κατευθυντήριες γραμμές όπως οι FIPS (Federal Information Processing Standards) και η σειρά NIST SP 800 βοηθούν στον καθορισμό κρυπτογραφικών και τεχνολογικών προτύπων ασφαλείας. Το Zero Trust Architectureκαι η ασφάλεια για τις υποδομές του Διαδικτύου των Πραγμάτων (IOT) είναι επίσης περιοχές κλειδιά όπου το NIST έχει επιρροή.

1.1.3 Επιρροή στην Καθημερινή Ζωή και την Παγκόσμια Κοινωνία

Η συμβολή του NIST επεκτείνεται πέρα από την επιστήμη και την τεχνολογία, επηρεάζοντας την καθημερινή ζωή των πολιτών και την παγκόσμια κοινωνία. Οι ακριβείς μετρήσεις και τα πρότυπα που αναπτύσσει το NIST διασφαλίζουν την ποιότητα προϊόντων, τη σωστή λειτουργία υποδομών, την ακρίβεια των συσκευών που χρησιμοποιούμε, και την ασφάλεια των δεδομένων μας. Επίσης, η συνεισφορά του στην κυβερνοασφάλεια προστατεύει την ιδιωτικότητα και τις πληροφορίες των χρηστών σε παγκόσμιο επίπεδο.

Η διεθνής συνεργασία με άλλους οργανισμούς τυποποίησης και μετρολογίας βοηθά στη διασφάλιση της συμβατότητας των προτύπων και την προώθηση της καινοτομίας σε παγκόσμια κλίμακα.

1.2 Τα στοιχεία του «NIST»

Το NIST (National Institute of Standards and Technology) παρέχει πλήθος προτύπων, πλαισίων και οδηγιών για διαφορετικούς τομείς. Αυτά τα πρότυπα καλύπτουν διάφορους τομείς της τεχνολογίας και της ασφάλειας πληροφοριών, προσφέροντας ένα πλήρες σύστημα διαχείρισης και βελτίωσης της ασφάλειας για επιχειρήσεις και οργανισμούς. Παρακάτω θα αναφέρω τα πια σημαντικά πλαίσια και πρότυπα του NIST καθώς και κάποια βασικά στοιχεία τους.

1.2.1 NIST Special Publication (SP) 800 Series

Η σειρά NIST SP 800 αποτελεί μια συλλογή εγγράφων που εστιάζουν στην ασφάλεια πληροφοριών και τις οδηγίες διαχείρισης. Είναι από τις πιο γνωστές δημοσιεύσεις του NIST και χρησιμοποιούνται ευρέως στην κυβερνοασφάλεια. Υπάρχουν πάνω από 200 ειδικές εκδόσεις στη σειρά NIST SP 800, αλλά ο αριθμός αυτός αυξομειώνεται καθώς προστίθενται νέες εκδόσεις και ενημερώνονται ή αποσύρονται παλαιότερες. Παρακάτω είναι τα κύρια έγγραφα της σειράς.

-NIST SP 800-39: «Διαχείριση του κινδύνου ασφάλειας πληροφοριών: Οργάνωση, αποστολή και άποψη του συστήματος πληροφοριών». Η δημοσίευση αυτή παρέχει οδηγίες για την καθιέρωση ενός ολοκληρωμένου, σε επίπεδο οργανισμού, προγράμματος αφιερωμένου στη διαχείριση του κινδύνου ασφάλειας πληροφοριών. Το πρόγραμμα έχει σχεδιαστεί για να αντιμετωπίζει τους κινδύνους που σχετίζονται με τις οργανωτικές λειτουργίες, συμπεριλαμβανομένης της αποστολής, των επιχειρήσεων, της εικόνας και της φήμης, καθώς και τους κινδύνους για τα περιουσιακά στοιχεία του οργανισμού, τα άτομα, άλλες οντότητες και το Έθνος που προκύπτουν από τη λειτουργία και τη χρήση των ομοσπονδιακών συστημάτων πληροφοριών. Η καθοδήγηση σχετικά με τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών είναι συμπληρωματική και μπορεί να ενσωματωθεί σε μια ευρύτερη πρωτοβουλία διαχείρισης επιχειρηματικών κινδύνων (ERM). Ο σκόπιμος σχεδιασμός της είναι σκόπιμα περιεκτικός, εστιάζοντας στους κινδύνους ασφάλειας πληροφοριών που προκύπτουν κυρίως από τη λειτουργία και τη χρήση των τεχνολογιών πληροφοριών.

-NIST SP 800-53: «Έλεγχοι ασφάλειας και απορρήτου για πληροφοριακά συστήματα και οργανισμούς». Το NIST SP 800-53 δημοσιεύθηκε για πρώτη φορά το 2005 και έχει υποστεί αρκετές αναθεωρήσεις ως απάντηση στο εξελισσόμενο τοπίο. Παρέχεται ένας κατάλογος ελέγχων ασφάλειας και προστασίας της ιδιωτικής ζωής σχεδιασμένος για ομοσπονδιακά συστήματα πληροφοριών, εξαιρουμένων εκείνων που αφορούν την εθνική ασφάλεια. Αυτοί οι

έλεγχοι είναι απαραίτητοι για τους ομοσπονδιακούς οργανισμούς, επιτρέποντας την ανάπτυξη και εφαρμογή μιας προσέγγισης με βάση τον κίνδυνο για την αποτελεσματική διαχείριση των κινδύνων ασφάλειας πληροφοριών. Μπορεί να ανταποκριθεί στις ευρείες απαιτήσεις ασφάλειας που επιβάλλονται στα πληροφοριακά συστήματα και τους οργανισμούς. Οι έλεγχοι αυτοί έχουν σχεδιαστεί ώστε να είναι συνεπείς και συμπληρωματικοί με άλλα καθιερωμένα πρότυπα ασφάλειας πληροφοριών. Η αναθεώρηση 5, που κυκλοφόρησε τον Σεπτέμβριο του 2020, εισήγαγε ουσιαστικές αλλαγές, συμπεριλαμβανομένης της αφαίρεσης του όρου «ομοσπονδιακός», επεκτείνοντας την εφαρμογή των εν λόγω κανονισμών σε όλους τους οργανισμούς. Αυτοί οι έλεγχοι μπορούν να αντιμετωπίσουν ποικίλες απαιτήσεις ασφάλειας για συστήματα πληροφοριών και οργανισμούς, ενώ παράλληλα ευθυγραμμίζονται με τα καθιερωμένα πρότυπα ασφάλειας πληροφοριών. Μπορείτε να μάθετε περισσότερα εδώ σχετικά με τον τρόπο χρήσης τους.

-NIST SP 800-37: «Οδηγός για την εφαρμογή του πλαισίου διαχείρισης κινδύνων στα ομοσπονδιακά συστήματα πληροφοριών». Αυτό το πλαίσιο προσφέρει ένα μεθοδικό αλλά προσαρμόσιμο πλαίσιο για την εποπτεία του κινδύνου ασφάλειας πληροφοριών σε επίπεδο οργανισμού, αποστολής/επιχειρησιακής διαδικασίας και πληροφοριακού συστήματος. Ο κύριος στόχος του είναι να προσφέρει ένα πλαίσιο διαχείρισης κινδύνων που επιτρέπει στους οργανισμούς να αξιολογούν και να διαχειρίζονται αποτελεσματικά τους κινδύνους που σχετίζονται με την ασφάλεια των δεδομένων τους και τους κινδύνους προστασίας της ιδιωτικής ζωής. Για τις ομάδες μας, το NIST SP 800-37 παρέχει κατευθυντήριες γραμμές για την επιλογή των κατάλληλων ελέγχων ασφαλείας από το NIST SP 800-53 με βάση τα αναγνωρισμένα επίπεδα κινδύνου και τις απαιτήσεις ασφαλείας του οργανισμού.

-NIST SP 800-30: «Οδηγός για τη διενέργεια εκτιμήσεων κινδύνου». Η έκδοση αυτή είναι ζωτικής σημασίας για τους οργανισμούς που επιθυμούν να κατανοήσουν και να διαχειριστούν τους κινδύνους που σχετίζονται με τα πληροφοριακά τους συστήματα και τα δεδομένα. Χρησιμοποιείται ευρέως από ομοσπονδιακές υπηρεσίες και άλλους οργανισμούς για την αξιολόγηση και τη διαχείριση των κινδύνων που σχετίζονται με τα πληροφοριακά τους συστήματα. Με βάση τις έννοιες που παρουσιάζονται στην Ειδική Έκδοση 800-27 του NIST, το NIST SP 800-30 παρέχει μια δομημένη προσέγγιση για την αξιολόγηση των κινδύνων. Η δημοσίευση αυτή προσφέρει μια συστηματική προσέγγιση αξιολόγησης κινδύνων, η οποία περιλαμβάνει τον εντοπισμό απειλών, τρωτών σημείων και πιθανών επιπτώσεων στα συστήματα πληροφοριών. Επιπλέον, παρέχει κατευθύνσεις για την ιεράρχηση των κινδύνων και την επιλογή κατάλληλων στρατηγικών μετριασμού των κινδύνων.

-NIST SP 800-146: «Σύνοψη και συστάσεις για το υπολογιστικό νέφος». Το έγγραφο απευθύνεται σε ένα φάσμα υπευθύνων λήψης αποφάσεων στον τομέα της τεχνολογίας πληροφοριών, συμπεριλαμβανομένων των επικεφαλής αξιωματικών πληροφοριών, των προγραμματιστών συστημάτων πληροφοριών, των διαχειριστών συστημάτων και δικτύων, των υπευθύνων ασφάλειας συστημάτων πληροφοριών και των ιδιοκτητών συστημάτων. Απλοποιεί την έννοια των συστημάτων νέφους και προσφέρει συστάσεις προσαρμοσμένες σε αυτούς τους κρίσιμους ενδιαφερόμενους φορείς σε απλή γλώσσα. Βοηθά τους οργανισμούς που επιθυμούν να κατανοήσουν και να εφαρμόσουν το υπολογιστικό νέφος μέσω μιας ολοκληρωμένης επισκόπησης του υπολογιστικού νέφους, συμπεριλαμβανομένων των πλεονεκτημάτων του, των ανοικτών ζητημάτων και της διαχείρισης των συναφών κινδύνων. Συγκεκριμένα, εμβαθύνει στις μεθόδους ανάπτυξης των συστημάτων υπολογιστικού νέφους, στη σειρά των διαθέσιμων υπηρεσιών, στους οικονομικούς παράγοντες που πρέπει να ληφθούν υπόψη, στα τεχνικά χαρακτηριστικά, όπως η απόδοση και η αξιοπιστία, στους τυποποιημένους όρους παροχής υπηρεσιών και στις ανησυχίες για την ασφάλεια.

-NIST SP 800-60: «Οδηγός για την αντιστοίχιση τύπων πληροφοριών και πληροφοριακών συστημάτων σε κατηγορίες ασφαλείας». Ένας κρίσιμος πόρος για οργανισμούς που επιθυμούν να κατηγοριοποιήσουν τις πληροφορίες και τα πληροφοριακά τους συστήματα σύμφωνα με τις απαιτήσεις ασφαλείας τους. Παρέχει ολοκληρωμένες κατευθυντήριες γραμμές για την κατανόηση αυτών των απαιτήσεων και τη διαχείριση των σχετικών κινδύνων. Χρησιμοποιούμε το NIST SP 800-60 για να βοηθήσουμε τους οργανισμούς στην κατηγοριοποίηση των επιπέδων επιπτώσεων που σχετίζονται με τις πληροφορίες και τα πληροφοριακά συστήματα, ευθυγραμμιζόμενοι με τις απαιτήσεις του Federal Information Security Management Act (FISMA).

-NIST SP 800-137: Συνεχής παρακολούθηση της ασφάλειας πληροφοριών (ISCM) Το NIST SP 800-137 καθοδηγεί τη συνεχή παρακολούθηση της ασφάλειας πληροφοριών (ISCM) για ομοσπονδιακά συστήματα και οργανισμούς πληροφοριών. (Παρεμπιπτόντως, το ISCM είναι σημαντικό επειδή λειτουργεί ως εργαλείο διαχείρισης κινδύνων και υποστήριξης αποφάσεων σε κάθε επίπεδο ενός οργανισμού). Το NIST SP 800-137 έχει σχεδιαστεί για την αντιμετώπιση των κινδύνων που σχετίζονται με τις οργανωτικές λειτουργίες. Αυτό περιλαμβάνει την αποστολή, τις λειτουργίες, την εικόνα και τη φήμη. Αλλά και τους κινδύνους για τα περιουσιακά στοιχεία του οργανισμού, τα άτομα, τις άλλες οντότητες και το έθνος που απορρέουν από τη λειτουργία και τη χρήση των ομοσπονδιακών συστημάτων πληροφοριών. Γιατί είναι πολύτιμο; Από πού πρέπει να ξεκινήσουμε; Ανώτερη και αμερόληπτη ασφάλεια στον κυβερνοχώρο. Μακροπρόθεσμη ασφάλεια στον κυβερνοχώρο και διαχείριση κινδύνων. Νωρίτερη ανίχνευση των ευπαθειών. Προληπτική ανταπόκριση σε περιστατικά. Αυξημένη ορατότητα και βιώσιμες βέλτιστες πρακτικές στο πλαίσιο του προγράμματος κυβερνοασφάλειας του οργανισμού σας. Επαναλαμβανόμενα αποτελέσματα σε όλες τις αλυσίδες εφοδιασμού και τους καταλόγους προμηθευτών. Γεφύρωση του χάσματος μεταξύ τεχνικών και οικονομικών ηγετών. Το καλύτερο από όλα είναι ότι μπορεί να προσαρμοστεί στις ανάγκες του οργανισμού σας.

-NIST SP 800-207: Αρχιτεκτονική μηδενικής εμπιστοσύνης. Η ZTA είναι μια στρατηγική προσέγγιση για την ασφάλεια στον κυβερνοχώρο. Βασίζεται σε ένα κομψό πρωτόκολλο: μην εμπιστεύεστε κανέναν χρήστη ή εφαρμογή εξ ορισμού την οποία θα αναλύσουμε και περαιτέρω αργότερα. Αυτός ο απλός κανόνας εφαρμόζεται επανειλημμένα, επικυρώνοντας κάθε βήμα μιας ψηφιακής αλληλεπίδρασης. Το NIST SP 800-207 παρέχει στις επιχειρήσεις έναν οδικό χάρτη υψηλού επιπέδου για τη μετάβαση και την εφαρμογή μιας προσέγγισης ZTA. Δίνει προτεραιότητα στην προστασία των πόρων έναντι των τμημάτων του δικτύου, επειδή οι επιχειρήσεις, σε αντίθεση με πολλές ομοσπονδιακές υπηρεσίες, έχουν πολυάριθμους απομακρυσμένους χρήστες και περιουσιακά στοιχεία που βασίζονται στο cloud και εκτείνονται πέρα από τα όρια του δικτύου τους. Η ZTA είναι ήδη παρούσα στις τρέχουσες ομοσπονδιακές πολιτικές και προγράμματα κυβερνοασφάλειας. Ωστόσο, το NIST SP 800- 207 εξακολουθεί να είναι χρήσιμο για τους διαχειριστές κυβερνοασφάλειας και τους διαχειριστές δικτύων των οργανισμών, επειδή περιλαμβάνει μια ανάλυση κενών των τομέων στους οποίους απαιτείται περισσότερη έρευνα και τυποποίηση για να βοηθήσει τους οργανισμούς στην ανάπτυξη και εφαρμογή στρατηγικών ZTA. Η ZTA δεν προορίζεται να είναι μια απλή ανάπτυξη, αλλά ξεκινώντας με μια σταθερή κατανόηση της επιχείρησης και των δεδομένων του οργανισμού θα οδηγήσει σε μια ισχυρή προσέγγιση της μηδενικής εμπιστοσύνης.

1.2.2 NIST Privacy Framework

Πρόκειται για ένα πλαίσιο που στοχεύει στην προστασία της ιδιωτικότητας, παρέχοντας στους οργανισμούς οδηγίες για την αντιμετώπιση κινδύνων σχετικά με την προστασία δεδομένων

προσωπικού χαρακτήρα. Είναι παρόμοιο με το CyberSecurity Framework, αλλά εστιάζει περισσότερο στην προστασία της ιδιωτικότητας.

1.2.3 NIST Risk Management Framework (RMF)

Το πλαίσιο αυτό παρέχει οδηγίες για τη διαχείριση κινδύνων ασφαλείας για πληροφοριακά συστήματα. Εστιάζει στην ενσωμάτωση της ασφάλειας κατά τη διαδικασία ανάπτυξης και διαχείρισης πληροφοριακών συστημάτων, προσφέροντας μια δομημένη προσέγγιση για την ανάλυση και τον περιορισμό των κινδύνων.

1.2.4 NIST Risk Cryptographic Standards

Το NIST παρέχει μια σειρά από πρότυπα για την κρυπτογράφηση, συμπεριλαμβανομένων των αλγορίθμων και των πρωτοκόλλων που χρησιμοποιούνται για την ασφάλεια πληροφοριών. Τα κύρια πρότυπα βρίσκονται παρακάτω.

-AES (Advanced Encryption Standard): Ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού.
-SHA (Secure Hash Algorithm): Χρησιμοποιείται για την παραγωγή κατακερματισμένων τιμών (hashes).
-RSA και ECC (Elliptic Curve Cryptography): Αλγόριθμοι ασύμμετρης κρυπτογράφησης για ασφαλή ανταλλαγή κλειδιών.

1.2.5 NIST National Initiative for Cybersecurity Education (NICE) Framework

Το Πλαίσιο NICE για την ασφάλεια στον κυβερνοχώρο είναι ένας ολοκληρωμένος πόρος που αναπτύχθηκε από το NIST για τον καθορισμό και την κατηγοριοποίηση των τομέων ικανοτήτων και των ρόλων εργασίας στον κυβερνοχώρο.

Καθιερώνει ένα κοινό λεξιλόγιο που περιγράφει την εργασία και τους εργαζόμενους στην κυβερνοασφάλεια σε όλους τους τομείς, παρέχοντας ένα τυποποιημένο λεξιλόγιο για την περιγραφή λειτουργιών και απαιτήσεων. Το πλαίσιο περιλαμβάνει επτά κατηγορίες ρόλων εργασίας με 52 συγκεκριμένους ρόλους εργασίας, πάνω από 2.200 δηλώσεις καθηκόντων, γνώσεων και δεξιοτήτων (TKS) και έντεκα τομείς ικανοτήτων. Χρησιμεύει ως ένας εθνικά εστιασμένος πόρος για τους εργοδότες για την ανάπτυξη του εργατικού δυναμικού τους στον τομέα της κυβερνοασφάλειας, υποστηρίζοντας τις προσπάθειες αξιολόγησης, σχεδιασμού, πρόσληψης και ανάπτυξης του εργατικού δυναμικού, ενώ παρέχει έναν ολοκληρωμένο οδηγό για όσους εισέρχονται ή εξελίσσονται στον τομέα της κυβερνοασφάλειας. Το Πλαίσιο NICE επικαιροποιείται συνεχώς με βάση τη δέσμευση μεταξύ της κυβέρνησης, του ιδιωτικού τομέα και του ακαδημαϊκού χώρου, διασφαλίζοντας τη συνάφεια του με τις εξελισσόμενες ανάγκες της κυβερνοασφάλειας. Ο αρθρωτός σχεδιασμός του επιτρέπει την ευέλικτη εφαρμογή του σε διάφορες οργανωτικές δομές, καθιστώντας το πολύτιμο τόσο για τον δημόσιο και τον ιδιωτικό τομέα, όσο και για ακαδημαϊκά ιδρύματα. Το πλαίσιο υποστηρίζει την ευθυγράμμιση της εκπαίδευσης και της κατάρτισης, διευκολύνει τα μονοπάτια ανάπτυξης σταδιοδρομίας και επιτρέπει στους οργανισμούς να αξιολογούν τις ικανότητες του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας, συμβάλλοντας τελικά στην ανάπτυξη ενός εξειδικευμένου και αποτελεσματικού εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας σε εθνικό επίπεδο [8].

1.2.6 NIST SP 1800 Series (Practice Guides for Cybersecurity)

Αυτή η σειρά περιέχει οδηγούς βέλτιστων πρακτικών για την κυβερνοασφάλεια και την εφαρμογή ασφαλών συστημάτων σε επιχειρήσεις. Τα έγγραφα αυτά παρέχουν πρακτικές λύσεις σε τεχνικά ζητήματα ασφάλειας.

1.2.7 NIST Federal Information Processing Standards (FIPS)

Τα FIPS είναι πρότυπα που χρησιμοποιούνται σε ομοσπονδιακά πληροφοριακά συστήματα για την προστασία δεδομένων. Είναι υποχρεωτικά για την κυβέρνηση των ΗΠΑ αλλά χρησιμοποιούνται ευρέως και από άλλους οργανισμούς. Τα κύρια FIPS βρίσκονται παρακάτω.

FIPS 140-2: Αφορά την ασφάλεια σε συσκευές κρυπτογράφησης. FIPS 199: Κατηγοριοποίηση συστημάτων πληροφορικής με βάση το επίπεδο ευαισθησίας τους. FIPS 200: Απαιτήσεις για την ασφάλεια των πληροφοριακών συστημάτων ομοσπονδιακών οργανισμών.

1.2.8 NIST Internet of Things (IOT) Cybersecurity Framework

Παρέχει οδηγίες και πρακτικές για την ασφάλεια των συσκευών IOT, οι οποίες αποτελούν σημαντικό κομμάτι της σύγχρονης τεχνολογίας. Το πλαίσιο καλύπτει τα ρίσκα που σχετίζονται με τα IOT και πώς αυτά μπορούν να περιοριστούν.

1.2.9 NIST Zero Trust Architecture (ZTA)

Η Zero Trust Architecture(ZTA) είναι ένα σύστημα ασφαλείας που βασίζεται στην αρχή ότι δεν πρέπει να εμπιστευόμαστε καμία υποδομή ή χρήστη, ακόμα και αν έχουν εντυπωσιάσει πρότυπα έγκρισης. Αυτό το σύστημα λειτουργεί υποθέτοντας ότι κάθε συνδεδεμένος χρήστης ή υποδομή είναι πιθανό να είναι απειλητική.

Η ZTA ανατρέπει την παραδοσιακή μορφή ασφαλείας, η οποία συνήθως βασίζεται στην εντύπωση έγκρισης και τα προφίλ χρηστών. Αντ' αυτού, η ZTA προτείνει μια πιο προσεκτική προσέγγιση, όπου κάθε αίτηση πρέπει να ελεγχθεί και να εγκριθεί. Αυτή η αρχιτεκτονική προτείνει μικρές, αυτόνομες ζώνες ασφαλείας που δεν εμπιστεύονται καμία υποδομή ή χρήστη εκτός από αυτές που έχουν ειδικά εγκριθεί. Η ZTA προτείνει επίσης μια συνεχόμενη διαδικασία ασφαλείας, όπου κάθε αίτηση πρέπει να ελεγχθεί και να εγκριθεί, ανεξάρτητα από το πού προέρχεται ή ποια είναι η προσέγγιση του χρήστη. Αυτό επιτυγχάνεται μέσω της διαχωρισμένων υποδομών για να περιοριστεί η κίνδυνος διαρροής πληροφορικής. Η ZTA απαιτεί συνεχείς επανεξετάσεις και αναθεωρήσεις των ασφαλών διαδικασιών για να εξασφαλιστεί ότι παραμένουν αποτελεσματικές ενάντια σε νέες απειλές. Επιπλέον, η ZTA απαιτεί επαγγελματική εκπαίδευση και συνεχόμενη εκπαίδευση για τους υπεύθυνους ασφαλείας και τους χρήστες για να γίνεται κατανοητή η αρχιτεκτονική και οι διαδικασίες της. Τέλος, η ZTA προτείνει τη συνεργασία μεταξύ διαφόρων τμημάτων της εταιρείας και των εξωτερικών συνεργατών για να διασφαλιστεί η αποτελεσματικότητα της αρχιτεκτονικής [9].

1.2.10 NIST Digital Identity Guidelines

Οι οδηγοί ασφάλειας ψηφιοποιημένου περιεχομένου της NIST είναι ένα σύμπλεγμα τεσσάρων τόμων που προσφέρει καθολική καθοδήγηση για την διαχείριση και την ασφάλεια στην ψηφιοποίηση.

Το σύμπλεγμα αυτό, γνωστό ως SP 800-63 Revision 4 και τις συμπληρωματικές του εκδόσεις SPs 800-63A, 800-63B και 800-63C, έχει ενημερωθεί για να αντιμετωπίσει τις σύγχρονες απαιτήσεις ασφαλείας και πρόσβασης. Οι οδηγοί αυτά προτείνουν μια ενδιαφέρουσα προσέγγισή στην διαχείριση των κινδύνων, την αποτροπή της απάτης και την εξασφάλιση της ευρείας και ισότιμης πρόσβασης στα ψηφιοποιημένα υπηρεσίες. Το σύμπλεγμα αυτό προτείνει επίσης καθοδηγήσεις για την χρήση σύγχρονων ψηφιοποιημένων τρόπων αποτύπωσης της ταυτότητας, όπως οι ψηφιοποιημένες κλειδιά και οι ψηφιοποιημένες τσάντες, καθώς και παραδοσιακούς φυσικών τρόπους αποτύπωσης της ταυτότητας. Οι οδηγοί αυτά επίσης προτείνουν λεπτομερείς καθοδηγήσεις για την χρήση βιομετρικών μέσων αποτύπωσης της ταυτότητας, καθώς και για την αντιμετώπιση εξαιρέσεων και προβλημάτων που μπορεί να παρουσιάσουν οι χρήστες. Το NIST ζητά δημόσιες υποψήφιες για το νέο σύμπλεγμα οδηγών μέχρι τον Οκτώβριο του 2024, προκειμένου να διασφαλίσει ότι οι οδηγοί αυτά αντιστοιχούν στις σύγχρονες ανάγκες της κοινωνίας και των οργανισμών [10].

1.2.11 NIST Cloud Computing Security Framework

Το Πλαίσιο ασφάλειας υπολογιστικού νέφους του NIST, το οποίο περιγράφεται λεπτομερώς στην ειδική έκδοση 500-292 του NIST, προσφέρει μια δομημένη προσέγγιση για τη διαχείριση ασφαλών περιβαλλόντων νέφους. Ορίζει πέντε βασικούς ρόλους στο οικοσύστημα του νέφους: Ο καθένας με συγκεκριμένες αρμοδιότητες για την ενίσχυση της σαφήνειας και της συνεργασίας στο πλαίσιο των υποδομών νέφους. Οι πέντε βασικές αρχιτεκτονικές συνιστώσες που περιλαμβάνει το πλαίσιο είναι οι παρακάτω. Κατανάλωση υπηρεσιών, εσωτερική και εξωτερική συνδεσιμότητα,φορητότητα παρόχων, λειτουργία κέντρου δεδομένων και διαχείριση νέφους

Αυτά τα στοιχεία διέπουν τις αλληλεπιδράσεις μεταξύ των ενδιαφερομένων μερών, δίνοντας έμφαση στην ασφάλεια σε όλες τις πτυχές των λειτουργιών του νέφους. Το πλαίσιο παρέχει καθοδήγηση σχετικά με την αυθεντικοποίηση, την εξουσιοδότηση και τον έλεγχο για την υποστήριξη της ασφαλούς πρόσβασης και του χειρισμού δεδομένων. Στα βασικά σημεία αναφοράς περιλαμβάνονται ο ορισμός βασικών όρων και εννοιών του νέφους, η αποσαφήνιση των ρόλων του οικοσυστήματος, η αντιμετώπιση των ζητημάτων ασφάλειας σε κάθε επίπεδο και η προσφορά κατευθυντήριων γραμμών διαχείρισης κινδύνου. Οι τακτικές ενημερώσεις του πλαισίου βοηθούν τους οργανισμούς να παραμένουν ευθυγραμμισμένοι με τις τελευταίες προκλήσεις και τεχνολογίες, υποστηρίζοντας την ασφαλή υιοθέτηση του cloud και τον μετριασμό των κινδύνων [11].

1.2.12 Σύγκριση μεταξύ του Πλαισίου Κυβερνοασφάλειας (CSF) του NIST και του NIST SP 800-53

Και τα δύο έχουν αναπτυχθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Και τα δύο παρέχουν καθοδήγηση σχετικά με τον τρόπο προστασίας των πληροφοριακών συστημάτων και των δεδομένων που περιέχουν. Και τα δύο παρέχουν μια προσέγγιση της ασφάλειας με βάση τον κίνδυνο. -Και τα δύο παρέχουν ένα ολοκληρωμένο σύνολο ελέγχων ασφαλείας και καθοδήγησης. Και τα δύο παρέχουν μια δομημένη προσέγγιση για την εφαρμογή της ασφάλειας. Και τα δύο παρέχουν μια κοινή γλώσσα για τη συζήτηση των απαιτήσεων ασφάλειας. Και τα δύο είναι σχεδιασμένα ώστε να προσαρμόζονται στις συγκεκριμένες ανάγκες ενός οργανισμού. Και τα δύο παρέχουν καθοδήγηση σχετικά με τον τρόπο αξιολόγησης της αποτελεσματικότητας των ελέγχων ασφαλείας. Και τα δύο παρέχουν ένα πλαίσιο για τη συνεχή βελτίωση της ασφάλειας. Και τα δύο παρέχουν ένα πλαίσιο για τη συμμόρφωση με τους σχετικούς κανονισμούς και πρότυπα.

Οι βασικές διαφορές μεταξύ του NIST CyberSecurity Framework (CSF) και του NIST SP 800-

53 είναι οι παρακάτω:

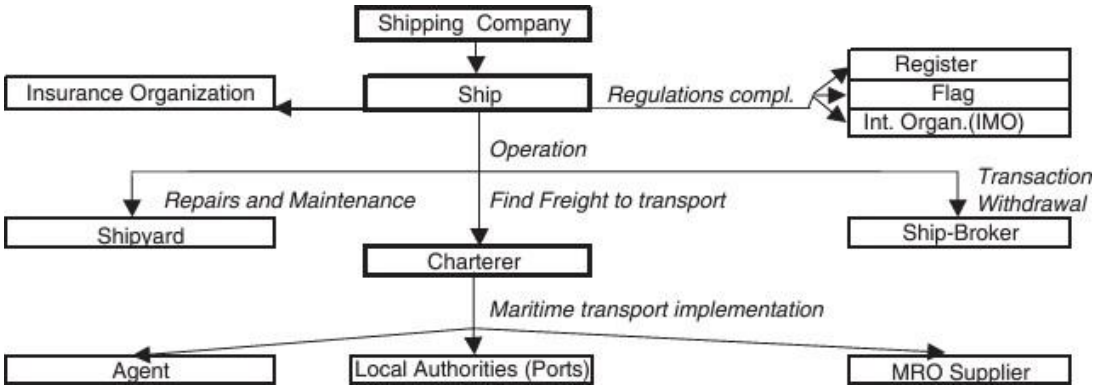
-Το NIST CyberSecurity Framework (CSF) είναι ένα εθελοντικό πλαίσιο που έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να διαχειριστούν τους κινδύνους κυβερνοασφάλειας, ενώ το NIST SP 800-53 είναι ένα σύνολο ελέγχων ασφάλειας και προστασίας της ιδιωτικής ζωής που εφαρμόζεται σε όλα τα ομοσπονδιακά συστήματα πληροφοριών.

-Το NIST CSF είναι ένα πλαίσιο υψηλού επιπέδου που επικεντρώνεται στη διαχείριση κινδύνων, ενώ το NIST SP 800-53 είναι ένα λεπτομερές σύνολο ελέγχων ασφαλείας. Επίσης το NIST CSF παρέχει ένα ολοκληρωμένο σύνολο βέλτιστων πρακτικών που πρέπει να ακολουθήσουν οι οργανισμοί, ενώ το NIST SP 800-53 παρέχει συγκεκριμένους ελέγχους ασφαλείας που πρέπει να εφαρμοστούν.

-Το NIST CSF είναι ένα πλαίσιο, ενώ το NIST SP 800-53 είναι ένα σύνολο προτύπων. Το NIST CSF έχει σχεδιαστεί για οργανισμούς όλων των μεγεθών, ενώ το NIST SP 800-53 έχει σχεδιαστεί για ομοσπονδιακές υπηρεσίες [12].

1.3 Υποδομές και Τεχνολογίες στην Ναυτιλία

Η ναυτιλιακή βιομηχανία έχει προφανώς επηρεαστεί από την εμφάνιση των νέων τεχνολογιών πληροφοριών και επικοινωνιών (ΙΤΕ). Η υιοθέτηση και η χρήση των ΙΤΕ αναγνωρίζεται όλο και περισσότερο ως το βέλτιστο μέσο για την ανταλλαγή πληροφοριών μεταξύ φορτωτών και μεταφορέων σε όλη την αλυσίδα εφοδιασμού. Τα οφέλη από τη χρήση των νέων ΙΤΕ σε ολόκληρη την αλυσίδα αξίας της ναυτιλίας περιλαμβάνουν ταχύτερη πρόσβαση σε πληροφορίες, βελτιωμένη επικοινωνία με πελάτες και επιχειρηματικούς εταίρους, καλύτερη εξυπηρέτηση πελατών, μείωση του κόστους, υψηλότερη παραγωγικότητα και ποιότητα υπηρεσιών.



Εικόνα 3. Παρουσιάζεται ένα μοντέλο υψηλού επιπέδου των ναυτιλιακών φορέων (ενδιαφερομένων μερών) και των πιθανών ηλεκτρονικών αλληλεπιδράσεων και λειτουργιών τους (το μοντέλο αναφέρεται ειδικότερα στην εμπορευματική ναυτιλία). [16]

Οι σύγχρονες ΙΤΕ έχουν γίνει κομβικό σημείο για τις ναυτιλιακές εταιρείες στην προσπάθειά τους να αποκτήσουν ανταγωνιστικό πλεονέκτημα έναντι των αντιπάλων τους, συνεργαζόμενες στενά με συνδεδεμένους εταίρους στις δραστηριότητες της αλυσίδας αξίας που είναι προσανατολισμένες στο δίκτυο. Σήμερα, οι εγκαταστάσεις των δικτύων επικοινωνίας στις επιχειρήσεις, που διασυνδέουν τους εξωτερικούς συμμετέχοντες στην αλυσίδα αξίας και τα εσωτερικά τμήματα, επιτρέπουν στις επιχειρήσεις να συντονίζουν τις πληροφοριακές, εικονικές και φυσικές αλυσίδες αξίας τους με σκοπό τη δημιουργία προστιθέμενης αξίας για τους πελάτες τους, τους συνεργάτες τους και μάλιστα για εσωτερική βελτιωμένη οργανωτική άνοδο[16]. Στη ναυτιλία, η ενοποίηση των Τεχνολογιών Πληροφορικής (ΙΤ) και των Τεχνολογιών Λειτουργίας (ΤΛ) δημιουργεί νέες ευκαιρίες για την αποδοτική διοίκηση και παρακολούθηση των πληροφοριακών συστημάτων και των φυσικών δραστηριοτήτων του στόλου και των εγκαταστάσεων. Μέσω της συνεργασίας μεταξύ ΙΤ και ΟΤ, οι ναυτιλιακές εταιρείες έχουν τη δυνατότητα να συγκεντρώνουν, να αναλύουν και να αξιοποιούν δεδομένα σε πραγματικό χρόνο, επιτυγχάνοντας έτσι βελτίωση της επιχειρησιακής αποδοτικότητας, ενίσχυση της ασφάλειας και καλύτερη αντιμετώπιση των αναγκών πελατών και συνεργατών. Αυτή η ενσωμάτωσή βοηθά στον συντονισμό και την ολοκλήρωση των αλυσίδων αξίας στην επιδίωξη της προστιθέμενης αξίας και του ανταγωνιστικού πλεονεκτήματος. Κατά την εξέταση της κυβερνό-ασφάλειας ενός πλοίου,

είναι απαραίτητο να γίνει η διάκριση μεταξύ των Τεχνολογιών Πληροφορικής (IT: Information Systems) και των Τεχνολογιών Λειτουργίας (OT: Operation Systems) που συμμετέχουν σε επιχειρησιακές λειτουργίες του πλοίου.

1.3.1 Τεχνολογία Πληροφοριών

Κάθε εξοπλισμός ή διασυνδεδεμένο σύστημα ή υποσύστημα εξοπλισμού που χρησιμοποιείται στην αυτόματη απόκτηση, αποθήκευση, χειρισμό, διαχείριση, μετακίνηση, έλεγχο, εμφάνιση, μεταγωγή, ανταλλαγή, μετάδοση ή λήψη δεδομένων ή πληροφοριών.

1.3.2 Λειτουργική Τεχνολογία

Σύστημα πληροφοριών που χρησιμοποιείται για τον έλεγχο βιομηχανικών διαδικασιών, όπως η κατασκευή, ο χειρισμός προϊόντων, η παραγωγή και η διανομή. Τα βιομηχανικά συστήματα ελέγχου περιλαμβάνουν συστήματα εποπτικού ελέγχου και συλλογής δεδομένων (SCADA) που χρησιμοποιούνται για τον έλεγχο γεωγραφικά διασκορπισμένων περιουσιακών στοιχείων, καθώς και κατανεμημένα συστήματα ελέγχου (DCS) και μικρότερα συστήματα ελέγχου που χρησιμοποιούν προγραμματιζόμενους λογικούς ελεγκτές για τον έλεγχο τοπικών διεργασιών.

1.3.3 Διαφορά μεταξύ συστημάτων IT & OT

Τα συστήματα OT εμπλέκονται στην πραγματική λειτουργία των συστημάτων (π.χ. έλεγχος κύριας μηχανής), ενώ τα συστήματα IT ελέγχουν τη ροή δεδομένων. Η IT καλύπτει το φάσμα των τεχνολογιών για την επεξεργασία πληροφοριών, συμπεριλαμβανομένων του λογισμικού, του υλικού και των τεχνολογιών επικοινωνίας. Πιθανότατα η σημαντικότερη διαφορά μεταξύ της κυβερνοασφάλειας του IT και του OT είναι το περιβάλλον στο οποίο λειτουργούν και το οποίο προστατεύουν. Η κυβερνοασφάλεια OT προστατεύει βιομηχανικά περιβάλλοντα, τα οποία συνήθως περιλαμβάνουν μηχανήματα, PLC και επικοινωνία μέσω βιομηχανικών πρωτοκόλλων. Τα συστήματα OT δεν λειτουργούν σε κανονικά λειτουργικά συστήματα, συχνά δεν διαθέτουν παραδοσιακά εργαλεία ασφαλείας και συνήθως προγραμματίζονται διαφορετικά από τους συμβατικούς υπολογιστές.
Αντίθετα, η κυβερνοασφάλεια IT προστατεύει κοινές συσκευές, όπως επιτραπέζιους και φορητούς υπολογιστές, πληκτρολόγια, εκτυπωτές και smartphones. Ασφαλίζει καθημερινά περιβάλλοντα όπως το cloud και τους διακομιστές χρησιμοποιώντας τυπικές λύσεις όπως antivirus και firewalls, καθώς και δημοφιλή πρωτόκολλα επικοινωνίας όπως το Hypertext Transfer Protocol (HTTP), το Remote Desktop Protocol (RDP) και το Secure Shell (SSH).

CIA vs. CAIC :
Ένας από τους καλύτερους τρόπους για να διακρίνετε τη διαφορά μεταξύ της ασφάλειας IT και της ασφάλειας OT είναι η τριάδα της CIA. Η τριάδα CIA είναι ένα μοντέλο που έχει σχεδιαστεί για να καθοδηγεί τις πολιτικές για την ασφάλεια των πληροφοριών σε έναν οργανισμό. Με σειρά προτεραιότητας, η CIA σημαίνει εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

-Η Πληροφοριακή Τεχνολογία (IT) CIA : Εμπιστευτικότητα Ακεραιότητα Διαθεσιμότητα

-Η Λειτουργική Τεχνολογία (OT) CAIC : Έλεγχος Διαθεσιμότητα Ακεραιότητα Εμπιστευτικότητα

Πίνακας 1. Ανάλυση διαφορών μεταξύ IT καI OT συστημάτων.[16]

Κατηγορίες	IT	OT
Απαιτήσεις επιδόσεων	μη πραγματικό χρόνο -η απόκριση πρέπει να είναι συνεπής -λιγότερο κρίσιμη αλληλεπίδραση έκτακτης ανάγκης Ο αυστηρά περιορισμένος έλεγχος πρόσβασης μπορεί να εφαρμοστεί στο βαθμό που απαιτείται για την ασφάλεια	σε πραγματικό χρόνο η ανταπόκριση είναι κρίσιμη για το χρόνο η ανταπόκριση στον άνθρωπο και σε κάθε άλλη αλληλεπίδραση έκτακτης ανάγκης είναι κρίσιμη η πρόσβαση στο OT θα πρέπει να ελέγχεται αυστηρά, αλλά δεν θα πρέπει να παρεμποδίζει ή να παρεμβαίνει στην αλληλεπίδραση ανθρώπου-μηχανής
Απαιτήσεις διαθεσιμότητας (αξιοπιστίας)	απαντήσεις όπως η επανεκκίνηση είναι αποδεκτές οι ελλείψεις διαθεσιμότητας μπορεί να είναι ανεκτές, ανάλογα με τις λειτουργικές απαιτήσεις του συστήματος	αντιδράσεις όπως η επανεκκίνηση μπορεί να μην είναι αποδεκτές λόγω επιχειρησιακών απαιτήσεων οι απαιτήσεις διαθεσιμότητας μπορεί να απαιτούν εφεδρικά συστήματα
Απαιτήσεις διαχείρισης κινδύνων	διαχείριση δεδομένων η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι υψίστης σημασίας η ανοχή σε σφάλματα μπορεί να είναι λιγότερο σημαντική. Οι επιπτώσεις των κινδύνων μπορεί να προκαλέσουν καθυστέρηση: του εκτελωνισμού του πλοίου, της έναρξης της φόρτωσης/εκφόρτωσης και των εμπορικών συναλλαγών. και επιχειρηματικές δραστηριότητες	έλεγχος του φυσικού κόσμου η ασφάλεια είναι υψίστης σημασίας, ακολουθούμενη από την προστασία της διαδικασίας η ανοχή σε σφάλματα είναι απαραίτητη, ακόμη και ο στιγμιαίος χρόνος διακοπής λειτουργίας μπορεί να μην είναι αποδεκτός οι επιπτώσεις του κινδύνου είναι η μη συμμόρφωση με τις κανονιστικές διατάξεις, καθώς και η βλάβη του προσωπικού επί του σκάφους, του περιβάλλοντος, του εξοπλισμού ή/και του φορτίου
Λειτουργία του συστήματος	Τα συστήματα έχουν σχεδιαστεί για χρήση με τα κοινώς γνωστά λειτουργικά συστήματα οι αναβαθμίσεις είναι απλές με τη διαθεσιμότητα εργαλείων αυτοματοποιημένης ανάπτυξης	διαφορετικά και ενδεχομένως ιδιόκτητα λειτουργικά συστήματα, συχνά χωρίς ενσωματωμένεςδυνατότητες ασφαλείας οι αλλαγές στο λογισμικό πρέπει να γίνονται προσεκτικά, συνήθως από τους προμηθευτές λογισμικού, λόγω των εξειδικευμένων αλγορίθμων ελέγχου και της πιθανής εμπλοκής τροποποιημένου υλικού και λογισμικού
Περιορισμοί πόρων	τα συστήματα προσδιορίζονται με επαρκείς πόρους για την υποστήριξη της προσθήκης εφαρμογών τρίτων, όπως λύσεις ασφαλείας	τα συστήματα έχουν σχεδιαστεί για την υποστήριξη της προβλεπόμενης επιχειρησιακής διαδικασίας και ενδέχεται να μην διαθέτουν αρκετή μνήμη και υπολογιστική πόρους για να υποστηρίξουν την προσθήκη δυνατοτήτων ασφαλείας

1.3.4 Η Ψηφιοποίηση του Πλοίου

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. Αντίστοιχα, ο νηογνώμονας Lloyd's Register (LR) στις σχετικές οδηγίες αναφέρει ότι τα δια- συνδεδεμένα συστήματα του πλοίου, μετατρέπουν το πλοίο σε ένα σύνολο διασυνδεδεμένων συστημάτων – «Ένα σύστημα από συστήματα». Τέτοια πλοία μπορούν να περιγράφουν με έναν νέο όρο, "cyber-enabled". Κάποιες βασικές τεχνολογίες πληροφορικής (IT) που χρησιμοποιούνται συνήθως στα πλοία της ναυτιλιακής βιομηχανίας είναι οι παρακάτω:

-Το λογισμικό ERP: Ενσωματώνει διάφορες επιχειρηματικές διαδικασίες, όπως απογραφή, προμήθειες και μισθοδοσία, παρέχοντας κεντρική πρόσβαση σε δεδομένα για τις λειτουργίες του πλοίου και της ξηράς.

-Συστήματα διαχείρισης πληρώματος: Λογισμικό που χρησιμοποιείται για τη διαχείριση του προγραμματισμού του πληρώματος, της εκπαίδευσης, της πιστοποίησης, της μισθοδοσίας και των πληροφοριών υγείας, διασφαλίζοντας τη συμμόρφωση με τις κανονιστικές διατάξεις και την ευημερία του πληρώματος.

-Πλατφόρμες Internet of Things (IOT): Χρησιμοποιούνται για τη συλλογή δεδομένων από αισθητήρες επί του σκάφους και τη μετάδοσή τους σε συστήματα στη στεριά για ανάλυση. Η IT γενικότερα διαχειρίζεται τη ροή και την αποθήκευση των δεδομένων ξηράς.

Η ναυτιλιακή βιομηχανία έχει γίνει μάρτυρας μιας αύξησης των κυβερνοεπιθέσεων, καθώς κακόβουλοι φορείς προσπαθούν να εκμεταλλευτούν τα τρωτά σημεία των συστημάτων επιχειρησιακής τεχνολογίας (OT) των πλοίων. Τα συστήματα OT περιλαμβάνουν κρίσιμες λειτουργίες όπως η επικοινωνία, η πρόωση, η διαχείριση ενέργειας, η πλοήγηση και η διαχείριση φορτίου. Καθώς τα πλοία συνδέονται ολοένα και περισσότερο στο Διαδίκτυο για τη βελτίωση της επιχειρησιακής απόδοσης και της επικοινωνίας, αυτά τα συστήματα OT γίνονται πιο ευάλωτα σε κυβερνοεπιθέσεις που μπορούν να διαταράξουν τις λειτουργίες του πλοίου. Παρακάτω θα επικεντρωθούμε στα τρωτά σημεία που σχετίζονται με τα συστήματα επικοινωνίας, τα συστήματα ελέγχου μηχανών πρόωσης και ισχύος, τα συστήματα πλοήγησης και τα συστήματα διαχείρισης φορτίου, καθώς αποτελούν άμεσο και σημαντικό κίνδυνο για τις λειτουργίες των πλοίων, καθώς και για την ασφάλεια τόσο του πληρώματος όσο και του φορτίου.

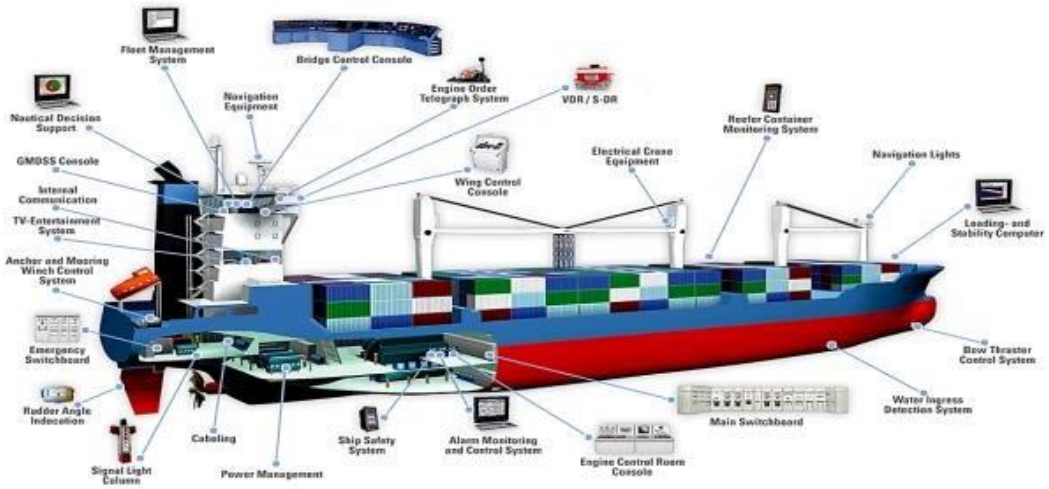
1.3.5 Συστήματα Επικοινωνίας

Η επικοινωνία μεταξύ πλοίων και μεταξύ πλοίων και ξηράς είναι κρίσιμη για διαδικασίες όπως η ειδοποίηση, η αναφορά και η αποστολή ή λήψη πληροφοριών για την ασφάλεια στη θάλασσα. Συνεπώς, η εγκατάσταση ενός ασφαλούς και αξιόπιστου συστήματος επικοινωνίας στο πλοίο είναι απαραίτητη. Οι σύγχρονες τεχνολογίες επικοινωνίας που είναι διαθέσιμες σήμερα έχουν αποδειχθεί πολύτιμες για ναυτικούς και λιμενικές αρχές, επιτρέποντάς τους να παραμένουν συνδεδεμένοι ανεξαρτήτως τοποθεσίας. Πολλές λειτουργίες, όπως αναφορές

καιρού, ενημερώσεις χαρτών, πρόσβαση σε email, αποστολή και λήψη ειδοποιήσεων κινδύνου και αναφορά θέσης, καθίστανται δυνατές μέσω δορυφορικών συστημάτων επικοινωνίας. Τα υποσυστήματα που περιλαμβάνονται στα συστήματα επικοινωνίας είναι το Δορυφορικό Σύστημα Επικοινωνίας (SATCOM), το Ολοκληρωμένο Σύστημα Επικοινωνίας (ICS), η φωνή μέσω δορυφόρου (Voice Over Internet Protocol - VOIP) και το ασύρματο τοπικό δίκτυο (WLAN).

- Σύστημα δορυφορικών επικοινωνιών (SATCOM) :

Τα πλοία χρειάζονται αξιόπιστη σύνδεση στο Διαδίκτυο για την εκτέλεση βασικών λειτουργιών και για να μπορεί το πλήρωμα να επικοινωνεί με τις οικογένειές του κατά τη διάρκεια της υπεράκτιας παραμονής τους. Οι τεχνολογίες SATCOM το καθιστούν εφικτό. Το δορυφορικό Διαδίκτυο είναι ένας τύπος ασύρματης σύνδεσης όπου τα σήματα μεταδίδονται και λαμβάνονται μεταξύ επίγειων σταθμών και δορυφόρων που βρίσκονται σε τροχιά γύρω από τη Γη. Ένας VSAT (Very Small Aperture Terminal) είναι ένας επίγειος σταθμός που χρησιμοποιείται για την παροχή δεδομένων σε πραγματικό χρόνο σχετικά με τη θέση άλλων πλοίων, βέλτιστα σχέδια δρομολόγησης και ακριβείς ναυτικούς χάρτες και γενικότερα για την μετάδοση-λήψη δεδομένων, φωνής και βίντεο μέσω δορυφορικού δικτύου επικοινωνιών. Ο VSAT περιλαμβάνει δύο κύρια μέρη: τον πομποδέκτη, που εγκαθίσταται εξωτερικά, και μια τερματική συσκευή που συνδέεται στον υπολογιστή του χρήστη για τη μετάδοση δεδομένων. Όλες οι συνδέσεις ρυθμίζονται και ελέγχονται μέσω της διαδικτυακής διεπαφής διαχείρισης VSAT [17].



Εικόνα 4. Ολοκληρωμένο σύστημα επικοινωνίας (ICS). [18]

Οι εμπειρογνώμονες του Volpe εντόπισαν εκατοντάδες ICS που είναι εγκατεστημένα σε φορτηγά πλοία σύμφωνα με την εικόνα 5, καθώς και σε όλη την υποδομή που υποστηρίζει τη λειτουργία των πλοίων και τη ναυσιπλοΐα, καθώς και τη φόρτωση, την εκφόρτωση και τη μετακίνηση.

-Τα εμπορικά πλοία βασίζονται σε εκατοντάδες ICS για τη διαχείριση της πρόωσης, την υποστήριξη πλοήγηση και τις επικοινωνίες, παρέχουν πυροπροστασία, λειτουργούν

συστήματα ασφαλείας και διαχειρίζονται φόρτωση και εκφόρτωση φορτίου.

-Τα ICS βρίσκονται επίσης στα σκάφη υποστήριξης, όπως τα πλοηγικά σκάφη, τα ρυμουλκά, τα πυροσβεστικά σκάφη και τα σκάφη αντιμετώπισης πετρελαιοκηλίδων, τα οποία εξασφαλίζουν την ασφαλή μετακίνηση των πλοίων και του φορτίου τους κατά την είσοδο και την έξοδο από το λιμάνι και τα οποία παρακολουθούν την ασφάλειά τους κατά την αγκυροβόλησή τους σε τερματικούς σταθμούς επιβατών και φορτίων.

-Πολλά συστήματα πλοήγησης, βοηθήματα πλοήγησης και συστήματα διαχείρισης της κυκλοφορίας των πλοίων που χρησιμοποιούνται από την Ακτοφυλακή των ΗΠΑ (USCG) για την ασφαλή καθοδήγηση των πλοίων στις πλωτές οδούς έχουν ενσωματωμένο ICS.

–Τα ICS συχνά ελέγχουν τα μηχανικά συστήματα που λειτουργούν τις κλειδαριές και τα φράγματα. Επίσης βρίσκονται στους γερανούς εμπορευματοκιβωτίων δίπλα στην αποβάθρα, στα φορτηγά οχήματα και στα αυτόνομα οχήματα που φορτώνουν, εκφορτώνουν και μεταφέρουν εμπορευματοκιβώτια σε ένα σύγχρονο λιμάνι [18].

•Φωνή μέσω πρωτοκόλλου Διαδικτύου (VOIP)
Τα τηλέφωνα VOIP επιτρέπουν στο πλήρωμα να πραγματοποιεί και να δέχεται τηλεφωνικές κλήσεις μέσω του Διαδικτύου. Πλοήγηση σε απομονωμένες και απομακρυσμένες περιοχές απαιτεί μια γραμμή ζωής επικοινωνίας που μπορεί να παρέχει 24ωρη συνδεσιμότητα με τα λιμάνια και τα γραφεία, ιδίως σε δύσκολες περιβαλλοντικές συνθήκες. Ένα γρήγορο, αξιόπιστο, οικονομικά αποδοτικό και ασφαλές σύστημα επικοινωνίας όπως τα τηλέφωνα VOIP βοηθά στην παροχή σαφών οδηγιών που σχετίζονται με το ταξίδι και την ασφάλεια πληροφορίες για το πλήρωμα. Το πρωτόκολλο έναρξης συνόδου είναι το πρωτόκολλο για τον έλεγχο των πολυμέσων επικοινωνιών πολυμέσων, όπως συνεδρίες κλήσεων φωνής και βίντεο μέσω του πρωτοκόλλου διαδικτύου. [19]

•Ασύρματο τοπικό δίκτυο (WLAN)
Ένα WLAN είναι μια εγκατάσταση ασύρματου δικτύου όπου πολλές συσκευές συνδέονται για να σχηματίσουν μια τοπική περιοχή δίκτυο. Οι δρομολογητές μπορούν να συνδεθούν στο μόντεμ VSAT και να ρυθμιστούν ώστε να χρησιμοποιούνται ως σημεία πρόσβασης Wi- Fi για τη σύνδεση συσκευών, δημιουργώντας ένα WLAN. Μπορεί να υπάρχουν διάφορα σημεία πρόσβασης στο πλοίο για διάφορες επιχειρησιακούς σκοπούς και για προσωπική χρήση του πληρώματος, επομένως πρέπει να είναι ασφαλή. Εκτός από το τρωτά σημεία σε ένα σημείο πρόσβασης, εάν αυτό τοποθετηθεί σε μια θέση όπου μπορεί να υπάρξει φυσική πρόσβαση, αυτά μπορούν εύκολα να παραβιαστούν. Ως εκ τούτου, είναι ζωτικής σημασίας η διασφάλιση των σημείων πρόσβασης. [20]

•Συστήματα πρόωσης, μηχανημάτων και ελέγχου Ισχύος
Τα συστήματα αυτά περιλαμβάνουν διάφορες κρίσιμες λειτουργίες που απαιτούν συνεχή έλεγχο και παρακολούθηση, όπως το σύστημα καυσίμου, τη διαχείριση κινητήρων και τα συστήματα συναγερμών. Η επικοινωνία μεταξύ των συστημάτων OT και IT γίνεται μέσω σειριακών πρωτοκόλλων (όπως το NMEA για το OT) και δικτύων Ethernet/IP για το IT. Σε πολλές περιπτώσεις, τα συστήματα OT συνδέονται με τα IT για υπηρεσίες συντήρησης και παρακολούθησης, γεγονός που δημιουργεί μια διασύνδεση που μπορεί να αποτελεί επιφάνεια επίθεσης για χάκερς. Η απουσία κρυπτογράφησης και αυθεντικοποίησης στα πρωτόκολλα OT διευκολύνει τους εισβολείς να εκμεταλλευτούν τα τρωτά σημεία μέσω του δικτύου και να εισέλθουν σε κρίσιμα συστήματα, προκαλώντας πιθανές δυσλειτουργίες.

Ειδικότερα, κοινά μέσα, όπως οι θύρες USB και ηλεκτρονικό ψάρεμα emails, αυξάνουν τον κίνδυνο πρόσβασης κακόβουλων ατόμων στο δίκτυο του πλοίου [21].

•Σύστημα ρυθμιστή κινητήρα
Ο κινητήρας του πλοίου χρησιμοποιείται για την πρόωση του πλοίου και την παραγωγή ενέργειας επί του πλοίου. Το σύστημα του κινητήρα χρησιμοποιείται για τον έλεγχο της μέσης ταχύτητας του κινητήρα υπό μεταβαλλόμενες καταστάσεις φορτίου [22]. Υπάρχουν διάφοροι τύποι κινητήρα συστημάτων, για παράδειγμα, σε έναν κινητήρα διπλού καυσίμου, οι δύο κύριοι ελεγκτές περιλαμβάνουν τη μονάδα ελέγχου κτυπήματος και τον ελεγκτή διπλού καυσίμου. Η μονάδα ελέγχου κτυπήματος είναι υπεύθυνη για τη ρύθμιση των ιδιοτήτων καυσίμου/αέρα, ενώ ο ελεγκτής διπλού καυσίμου είναι υπεύθυνος για τον έλεγχο της ταχύτητας του κινητήρα. Δίκτυο σειριακής επικοινωνίας (π.χ. δίκτυο NMEA/CAN) χρησιμοποιείται ως τρόπος επικοινωνίας με τα υπόλοιπα μηχανήματα του πλοίου. [29]. Ορισμένες από τις παραμέτρους που πρέπει να λαμβάνονται υπόψη στη λειτουργία του κινητήρα ενός πλοίου περιλαμβάνουν την ποσότητα του καυσίμου που εγχέεται, η πίεση, η θερμοκρασία καύσης, η θερμοκρασία του κινητήρα και η κατάσταση εκκίνησης/διακοπής λειτουργίας του κινητήρα [25].

- Σύστημα καυσίμου πετρελαίου

Το σύστημα μαζούτ είναι ζωτικής σημασίας για την πρόωση και την παραγωγή ενέργειας του πλοίου [26]. Οι ναυτικοί κινητήρες μετατρέπουν τη θερμότητα που παράγεται από την καύση του μαζούτ σε μηχανική ενέργεια μέσω της διαδικασίας καύσης. Καύσιμο στάθμη της δεξαμενής, η θερμοκρασία και το ιξώδες είναι μερικές από τις βασικές παραμέτρους που πρέπει να λαμβάνονται υπόψη σε ένα σύστημα μαζούτ [25].

- Σύστημα παρακολούθησης και ελέγχου συναγερμών

Το σύστημα παρακολούθησης και ελέγχου συναγερμών βοηθά στην παρακολούθηση και τον έλεγχο όλων των συναγερμών που εφαρμόζονται στο πλοίο μέσω μιας κονσόλας πολλαπλών λειτουργιών ή ενός υπολογιστή [27]. Συνδέει τους συναγερμούς που σχετίζονται με όλα τα συστήματα του πλοίου και εκπέμπει οπτικά ή ηχητικά σήματα σε περίπτωση έκτακτης ανάγκης ή βλάβης του συστήματος. [23]. Δεδομένου ότι τα συστήματα του πλοίου είναι ευάλωτα σε αστοχίες/δυσλειτουργίες και σε διάφορους ανθρώπινους παράγοντες, ο το σύστημα συναγερμού διαδραματίζει ζωτικό ρόλο στην ειδοποίηση του πληρώματος κατά τη διάρκεια βλαβών του συστήματος και έκτακτων περιστατικών.

- Σύστημα διαχείρισης Ισχύος (PMS)

Το σύστημα διαχείρισης ισχύος είναι υπεύθυνο για την παροχή αδιάλειπτης παροχής ισχύος σε όλες τις συστήματα του σκάφους. Το PMS αυτοματοποιεί λειτουργίες όπως η εκκίνηση/διακοπή των γεννητριών, η τάση και η έλεγχος της τάσης και της συχνότητας και έλεγχος του φορτίου. Τα πλοία λειτουργούν με διάφορες ηλεκτρονικές συσκευές και το φορτίο, όπως όπως τα δοχεία καυσίμων και τα κλιματιζόμενα εμπορευματοκιβώτια πρέπει να μεταφέρονται ελέγχοντας ορισμένες ιδιότητες όπως η θερμοκρασία, η πίεση κ.λπ. [29], επομένως η διακοπή της παροχής ηλεκτρικής ενέργειας θα επηρεάσει τις λειτουργίες των πλοίων. Το παράμετροι που πρέπει να λαμβάνονται υπόψη σε ένα PMS περιλαμβάνουν την κατάσταση της γεννήτριας (εκκίνηση/διακοπή), την τάση, τη συχνότητα, τη γεννήτρια φορτίο γεννήτριας, κ.λπ. [31]. Όλες αυτές οι παράμετροι μπορούν να παρακολουθούνται και να ελέγχονται μέσω της διαχείρισης ισχύος συστήματος.

- Γεννήτρια έκτακτης ανάγκης καl μπαταρίες

Μια γεννήτρια έκτακτης ανάγκης παρέχει εφεδρική ισχύ σε κρίσιμες συσκευές του πλοίου κατά τη διάρκεια της λειτουργίας της κύριας γεννήτριας ή κατά τη διάρκεια διακοπής ρεύματος. Τόσο οι μπαταρίες όσο και η γεννήτρια έκτακτης ανάγκης μπορούν να χρησιμοποιηθούν σε περίπτωση έκτακτης ανάγκης. Η γεννήτρια μπορεί να ελέγχεται μέσω της κονσόλας του συστήματος διαχείρισης ισχύος, όπου η τάση και οι συχνότητα παρακολουθείται. Κατά τη διάρκεια της απώλειας της κύριας παροχής ρεύματος, όταν το ηλεκτρικό ρελέ ανιχνεύσει χαμηλή τάση ή συχνότητα, θα ενεργοποιήσει αυτόματα τη γεννήτρια έκτακτης ανάγκης [28]. Τα πλοία και τα εμπορευματοκιβώτια φορτίου απαιτούν σταθερή παροχή ενέργειας καθ' όλη τη διάρκεια του ταξιδιού τους. Reefer εμπορευματοκιβώτια που μεταφέρουν ευαίσθητα στη θερμοκρασία εμπορεύματα (όπως φάρμακα και ευπαθή τρόφιμα) είναι ιδιαίτερα ιδιαίτερα ευάλωτα σε διαταραχές της παροχής ηλεκτρικής ενέργειας [29].

1.3.6 Συστήματα Πλοήγησης

Τα σκάφη είναι εξοπλισμένα με πολλά προηγμένα συστήματα εξοπλισμού πλοήγησης που παρέχουν ακριβή πλοήγηση δεδομένα. Τα συστήματα πλοήγησης μπορεί να ελέγχονται εξ ολοκλήρου από το σύστημα ή να βρίσκονται αλλού, με το σκάφος να ελέγχεται μέσω ραδιοφώνου ή άλλων σημάτων. Ο προσδιορισμός της σωστής θέσης, της ταχύτητας και της πορείας του σκάφους είναι απαραίτητη για να διασφαλιστεί ότι το σκάφος φτάνει στον προορισμό του με ασφάλεια και εντός του χρονοδιαγράμματος. Τα συστήματα πλοήγησης περιλαμβάνουν τα ακόλουθα υποσυστήματα: ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών, σύστημα ραδιοεπικοινωνίας. σύστημα αυτόματης αναγνώρισης, παγκόσμιο σύστημα εντοπισμού θέσης, δυναμικό σύστημα εντοπισμού θέσης. σύστημα, παγκόσμιο σύστημα ασφάλειας ναυτικής ανάγκης, καταγραφές δεδομένων ταξιδιού και ολοκληρωμένο σύστημα πλοήγησης.

- Ηλεκτρονικό σύστημα απεικόνισης χάρτη και πληροφοριών (ECDIS) :

Το ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών (ECDIS) είναι ένα ηλεκτρονικό σύστημα ναυτικών χαρτών για τον εντοπισμό θέσεων και την απόκτηση κατευθύνσεων για το ταξίδι του πλοίου. Το ECDIS εντοπίζει με ακρίβεια τα ναυτιλιακά με τη βοήθεια του παγκόσμιου συστήματος εντοπισμού θέσης (GPS). Εμφανίζει επίσης πληροφορίες ραντάρ, τις καιρικές συνθήκες, τις συνθήκες πάγου, την ταχύτητα, τη θέση και την προγραμματισμένη διαδρομή του πλοίου. Το ECDIS είναι ένας υπολογιστής σταθμός εργασίας εγκατεστημένος στη γέφυρα του πλοίου, ο οποίος συνήθως εκτελείται σε λειτουργικά συστήματα όπως Windows ή Linux. Οι διεπαφές που συνδέονται στο ECDIS περιλαμβάνουν το ραντάρ του πλοίου, το αυτόματο AIS, αισθητήρας θέσης, αισθητήρας ταχύτητας και αισθητήρας πορείας. Αυτές οι διεπαφές συχνά συνδέονται στο τοπικό δίκτυο (LAN) του πλοίου μέσω NMEA (συνδυασμένο ηλεκτρικό και δεδομένων για την επικοινωνία μεταξύ ναυτικών ηλεκτρονικών συσκευών), το οποίο με τη σειρά του διαθέτει μια πύλη στο Διαδίκτυο. Με βάση τις προδιαγραφές του παρόχου υπηρεσιών και τις εγκαταστάσεις επικοινωνίας επί του σκάφους, οι ενημερώσεις των ηλεκτρονικών ναυτικών χαρτών (ENC) πραγματοποιούνται μέσω θυρών USB, διανομής δεδομένων μέσων (π.χ. DVD), συνημμένο ηλεκτρονικό ταχυδρομείο (SATCOM) και λήψη από το διαδίκτυο. Όλα αυτά είναι δυνατά επιφάνειες επίθεσης που μπορούν να χρησιμοποιήσουν οι επιτιθέμενοι για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο ECDIS [29].

- Ραδιοανίχνευση και εμβέλεια (RADAR) :

Το σύστημα RADAR διαδραματίζει σημαντικό ρόλο στην ασφαλή πλοήγηση ενός πλοίου. Αποτελεί υποχρεωτικό εξοπλισμό για τη ναυσιπλοΐα, που χρησιμοποιείται για τον εντοπισμό,

την παρακολούθηση, τον εντοπισμό θέσης των πλοίων και για την ασφαλή πλοήγηση ενός πλοίου από ένα σημείο σε άλλο. Για την αποφυγή συγκρούσεων, τα πλοία βασίζονται σε συστήματα ραντάρ συχνοτήτων S-band και X-band, τα οποία μπορούν να εντοπίζουν στόχους και να εμφανίζουν πληροφορίες στην οθόνη, όπως η απόσταση του πλοίου από τη στεριά, πλωτά αντικείμενα, εμπόδια και άλλα σκάφη στην περιοχή. Οι διεπαφές που συνδέονται με το RADAR περιλαμβάνουν τοπικός διακόπτης ethernet και πρωτόκολλα ethernet, τα οποία μπορεί να λειτουργούν ως επιφάνειες επίθεσης για τους επιτιθέμενους για να αποκτήσουν πρόσβαση στα συστήματα του πλοίου [30].

- Αυτόματο σύστημα αναγνώρισης (AIS) :

Το AIS έχει σχεδιαστεί κυρίως για να επιτρέπει στα πλοία να βλέπουν και να γίνονται αντιληπτά από τη θαλάσσια κυκλοφορία στην περιοχή τους. Βοηθά στην αναγνώριση των πλοίων και των σημάτων ναυσιπλοΐας. Το AIS βοηθά στην απόκτηση συγκεκριμένων πληροφοριών των πλοίων σε ορισμένη περιοχή, όπως το όνομά τους, η ταχύτητα, η θέση, η κατεύθυνση, ο ρυθμός στροφής, ο προορισμός, και φυσικές παραμέτρους, όπως μήκος, πλάτος, χωρητικότητα, πλάτος και βύθισμα, σε γειτονικά πλοία και παράκτιες περιοχές. αρχές. Το AIS συνδέει έναν τυποποιημένο πομποδέκτη πολύ υψηλής συχνότητας (VHF) με ένα σύστημα εντοπισμού θέσης. σύστημα, όπως ένας δέκτης GPS, καθώς και με άλλους ηλεκτρονικούς αισθητήρες πλοήγησης, όπως η γυροπυξίδα. ή δείκτης ταχύτητας στροφής [31].

- ΠαγκόσμΙΟ σύστημα εντοπΙσμού θέσης (GPS) :

Το GPS είναι ένα κρίσιμο στοιχείο που βοηθά στον προσδιορισμό ακριβών γεωγραφικών θέσεων για την πλοήγηση. Ένα σύστημα GPS περιλαμβάνει τρία συστήματα: δορυφόρους, επίγειους σταθμούς και δέκτες. Το GPS πληροφορίες αναπαράγονται συχνά σε άλλο εξοπλισμό πλοήγησης στη γέφυρα, όπως τα ραντάρ, σύστημα αυτόματης αναγνώρισης, συστήματα ηλεκτρονικής πλοήγησης και συστήματα επικοινωνίας, για να βοηθήσουν στην την πλοήγηση. Το διαφορικό GPS (DGPS), μια βελτίωση του βασικού σήματος GPS, παρέχει πολύ υψηλότερη ακρίβεια και αυξημένη ασφάλεια στις περιοχές κάλυψής του για τις θαλάσσιες επιχειρήσεις [32].

- Δυναμικό σύστημα εντοπΙσμού θέσης (DPS) :

Ένα σύστημα δυναμικού εντοπισμού θέσης είναι ένα αυτοματοποιημένο σύστημα ελεγχόμενο από υπολογιστή που διατηρεί τη θέση ενός σκάφους θέση και την πορεία του πλοίου ελέγχοντας τις δικές του προπέλες και προωθητήρες. Οι αισθητήρες αναφοράς θέσης, σε εκτός από τους αισθητήρες ανέμου, τους αισθητήρες κίνησης και τις γυροπυξίδες, παρέχουν δεδομένα στον υπολογιστή σχετικά με το τη θέση του σκάφους, το μέγεθος και την κατεύθυνση των περιβαλλοντικών δυνάμεων που επηρεάζουν τη θέση του. Ο κύριος λειτουργίες ενός συστήματος DP αποτελούνται από τα εξής: - Εκτίμηση της θέσης και της πορείας του σκάφους - Προσδιορισμός των σφαλμάτων θέσης και πορείας μεταξύ των σημείων ρύθμισης και των εκτιμήσεων. - Καθορισμός της διορθωτικής δράσης που πρέπει να εφαρμοστεί - Υπολογισμός της εντολής προς τους προωθητήρες [33].

- ΠαγκόσμΙΟ σύστημα ασφάλεΙας ναυτΙκής ανάγκης (GMDSS) :

Το Παγκόσμιο Σύστημα Ναυτικής Έκτακτης Ανάγκης και Ασφάλειας (GMDSS) είναι ένα πρότυπο για τη χρήση της επικοινωνίας πρωτοκόλλου, των διαδικασιών και του εξοπλισμού ασφαλείας που μπορεί να χρησιμοποιηθεί κατά τη στιγμή της κατάστασης κινδύνου από το πλοίο. Το GMDSS στέλνει σήμα κινδύνου μέσω δορυφορικού ή ράδιο-εξοπλισμού επικοινωνίας. Χρησιμοποιείται ως μέσο για τη μετάδοση και τη λήψη πληροφοριών για τη θαλάσσια ασφάλεια, καθώς και ως ένα γενικό 18 κανάλι επικοινωνίας. INMARSAT,

NAVTEX, ραδιοφάρος ένδειξης θέσης έκτακτης ανάγκης (EPIRB), ο εξοπλισμός εντοπισμού έρευνας και διάσωσης και η ψηφιακή επιλεκτική κλήση είναι τα διάφορα συστατικά στοιχεία του GMDSS [34].

- Καταγραφέας δεδομένων ταξιδιού (VDR) :

Το Voyage Data Recorder (VDR) είναι ένας εξοπλισμός που λειτουργεί παρόμοια με το «μαύρο κουτί» ενός αεροσκάφους και είναι υπεύθυνος για τη συλλογή και τη διατήρηση όλων των σχετικών πληροφοριών για ένα πλοίο. Αυτό το σύστημα καταγράφει διάφορα δεδομένα, όπως η ταχύτητα, η κατεύθυνση, η θέση, η κατάσταση των συστημάτων του πλοίου, οι πληροφορίες σχετικά με τη μηχανή, τα καύσιμα κ.λπ., τα οποία θα είναι χρήσιμα κατά τη διάρκεια μιας έρευνας ατυχήματος για να εξεταστεί τι είχε συμβεί. συνέβη στο πλοίο και το πλήρωμα. Επιπλέον, το VDR περιλαμβάνει ένα σύστημα καταγραφής φωνής που μπορεί να αποθηκεύσει έως και 12 ώρες πληροφοριών [29].

- Ολοκληρωμένο σύστημα πλοήγησης (INS) :

Το ολοκληρωμένο σύστημα πλοήγησης (INS) εντείνει την επιχειρησιακή αποτελεσματικότητα και την ασφάλεια του πλοίου πλοήγησης με τον εξοπλισμό μιας πολυλειτουργικής οθόνης που βασίζεται στην ενσωμάτωση τουλάχιστον δύο πλοηγικών λειτουργιών. Πρόκειται για μια πλατφόρμα λογισμικού που περιλαμβάνει δεδομένα από τα συστήματα ECDIS και RADAR, με αισθητήρες για άλλες λειτουργίες πλοήγησης. Οι πιθανές επιφάνειες επίθεσης στο INS είναι το Server Message Block (SMB) και το πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας [35].

1.3.7 Συστήματα Διαχείρισης Φορτίου

Το σύστημα διαχείρισης φορτίου βοηθά στον αξιόπιστο έλεγχο και την παρακολούθηση του φορτίου. Οι λειτουργίες μπορούν να είναι αυτοματοποιηθούν ανάλογα με τον τύπο του πλοίου και του φορτίου. Η κατάσταση του φορτίου και τα σχετικά δεδομένα είναι συχνά διαθέσιμα και διαχειρίζονται μέσω του διαδικτύου, αυξάνοντας τις πιθανότητες κυβερνοεπιθέσεων. Τα υποσυστήματα που καλύπτονται στα συστήματα διαχείρισης φορτίου είναι η αίθουσα ελέγχου φορτίου και το σύστημα υδάτινου έρματος.

- Αίθουσα ελέγχου φορτίου (CCR)

Μια αίθουσα ελέγχου φορτίου (CCR) είναι ένας χώρος όπου ελέγχεται η φόρτωση και εκφόρτωση του φορτίου και παρακολουθείται από έναν υπεύθυνο (PIC). Ο σχεδιασμός και η διάταξη μιας αίθουσας ελέγχου φορτίου μπορεί να καθοριστεί με βάση τον σχεδιασμό ενός πλοίου, τις απαιτήσεις των πλοιοκτητών και τις δυνατότητες ενός συγκεκριμένου ναυπηγείου. Το CCR μπορεί να είναι ένα ξεχωριστό δωμάτιο ή τα όργανα ελέγχου μπορούν να τοποθετηθούν στη γέφυρα του πλοίου. Το PIC μπορεί να ελέγχει τη φόρτωση/εκφόρτωση του φορτίου, τις αντλίες απογύμνωσης, τον έλεγχο των θέσεων των βαλβίδων και των επιπέδων των υγρών στο φορτίο μέσω του εξοπλισμού που υπάρχει στο CCR [36].

- Σύστημα νερού έρματος (BWS)

Το σύστημα έρματος (BWS) είναι ένα ξεχωριστό διαμέρισμα εντός του πλοίου που αποθηκεύει νερό ως έρμα για να προσφέρει σταθερότητα στο πλοίο. Η χρήση νερού σε μια τέτοια δεξαμενή θα βοηθήσει στη ρύθμιση του βάρους του πλοίου σε μη φυσιολογικές συνθήκες. Η λειτουργία του συστήματος περιλαμβάνει επίσης την άντληση του νερού έρματος για προσωρινή μείωση του βυθίσματος του πλοίου όταν αυτό εισέρχεται σε ρηχά ύδατα [47] [29]. Το νερό έρματος 19 σύστημα διαχείρισης (BWMS) είναι ένας άλλος τύπος

συστήματος ελεγχόμενου από υπολογιστή για τη διαχείριση της επεξεργασίας νερού έρματος για την απομάκρυνση των θαλάσσιων οργανισμών και των στερεών υλικών.

1.4 Κίνδυνοι Κυβερνοασφάλειας

Οι επιχειρήσεις θα πρέπει να λαμβάνουν υπόψη τυχόν μοναδικά χαρακτηριστικά των πιθανών φορέων απειλών κατά τον εντοπισμό των απειλών. Ικανότητα, πιθανότητα και πρόθεση επίθεσης. Αυτό θα μπορούσε να περιλαμβάνει τη χρήση ενός εσωτερικού ή εξωτερικού ατόμου ως ακούσιου μεσάζοντα που εξαπλώνει ακούσια την απειλή, όπως μέσω ενός μολυσμένου USB stick. Αφού εντοπιστούν τα τρωτά σημεία, θα πρέπει να ληφθούν υπόψη οι απειλές προκειμένου να προσδιοριστεί η πιθανότητα ενός συμβάντος ή μιας επίθεσης. Η πιθανότητα του συμβάντος δημιουργεί τον παράγοντα κινδύνου εκτός από τον αντίκτυπο ενός συγκεκριμένου. Υπάρχει η πιθανότητα οργανισμοί και άτομα να απειλήσουν εκούσια ή ακούσια την ασφάλεια και την προστασία του πληρώματος, του περιβάλλοντος και του πλοίου. Κατά τη διενέργεια εκτιμήσεων κινδύνου, οι εταιρείες θα πρέπει να εξετάζουν κάθε τομέα της επιχείρησής τους για πιθανή έκθεση σε επιθέσεις στον κυβερνοχώρο. Η διαχείριση κινδύνου είναι πιο δύσκολη με τις απειλές στον κυβερνοχώρο από ό,τι με άλλους φορείς απειλών, επειδή το αποτέλεσμα αυτών των απειλών δεν είναι πάντα ορατό και πολλές εταιρείες αποφεύγουν να δημοσιοποιούν γεγονότα που σχετίζονται με απειλές στον κυβερνοχώρο ακριβώς για αυτό το λόγο. Όσον αφορά την ναυτιλία, τα πλοία εξαρτώνται σε μεγάλο βαθμό από τις ψηφιακές τεχνολογίες για την ενσωμάτωση των συστημάτων και την αυτοματοποίηση των λειτουργιών. Ενώ η αξιοποίηση των νέων τεχνολογιών για τις λειτουργίες των πλοίων προσφέρει σημαντικά οφέλη για το ναυτιλιακή βιομηχανία από άποψη αποδοτικότητας, οι κίνδυνοι μπορεί να εξακολουθούν να υφίστανται λόγω της έλλειψης ελέγχων ασφαλείας, της κακής σχεδιασμού και συντήρησης του συστήματος. Ο επιτιθέμενος μπορεί εύκολα να εκμεταλλευτεί τα τρωτά σημεία των συσκευών που συνδέονται με το ίντερνετ όπως το SATCOM για να διεισδύσει στο δίκτυο του πλοίου. Εάν τα συστήματα OT είναι συνδεδεμένα με Διαδίκτυο για επιχειρησιακούς σκοπούς και σκοπούς απομακρυσμένης εξυπηρέτησης, τότε η εν λόγω διασύνδεση θα βοηθήσει τον επιτιθέμενο να διεισδύσει και στο δίκτυο ΛΤ, ωστόσο αυτός ο τρόπος διείσδυσης απαιτεί άφθονες δεξιότητες. Αυτή η ενότητα εξετάζει τους κινδύνους στον κυβερνοχώρο που συνδέονται με καθένα από τα υποσυστήματα OT που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, Κεφάλαιο 3 της Ενότητας και παρέχει λεπτομερέστερη περιγραφή των κινδύνων στον κυβερνοχώρο στα συστήματα OT του πλοίου. Διευκρινίζεται ότι τα συστήματα IT και OT στο σύγχρονο τεχνολογικό τοπίο είναι εκτεθειμένα σε διαφορετικούς τύπους επιθέσεων, καθεμία από τις οποίες έχει μοναδικές επιπτώσεις και απαιτήσεις αντιμετώπισης. Τα συστήματα IT είναι πιο ευάλωτα σε επιθέσεις κακόβουλου λογισμικού και ransomware, σε απόπειρες ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής και σε παραβιάσεις δεδομένων, οι οποίες απειλούν κυρίως την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων, με αποτέλεσμα συχνά να προκαλείται ζημία στη φήμη των οργανισμών. Αντίθετα, τα συστήματα ΛΤ αντιμετωπίζουν μεγαλύτερους κινδύνους από επιθέσεις σε βιομηχανικά συστήματα ελέγχου (ICS), ευπάθειες σε παλαιά συστήματα, επιθέσεις άρνησης παροχής υπηρεσιών (DoS) και επιθέσεις σε μακροχρόνιες αλυσίδες εφοδιασμού. Αυτές οι επιθέσεις μπορούν να οδηγήσουν σε υλικές ζημιές σε περιουσιακά στοιχεία, διακοπή της λειτουργίας κρίσιμων υποδομών και δυνητικούς κινδύνους για την ασφάλεια των εργαζομένων[38]. Οι απαιτήσεις αντιμετώπισης διαφέρουν επίσης- τα συστήματα IT μπορούν γενικά να επανεκκινήσουν χωρίς σοβαρές λειτουργικές συνέπειες. Ωστόσο, τα συστήματα ΛΤ απαιτούν αυστηρό έλεγχο του χρόνου διακοπής

λειτουργίας και επανεκκίνησης λόγω των συνεχών λειτουργικών τους απαιτήσεων. Η εστίαση της ασφάλειας του καθενός διαφέρει επίσης: Η ασφάλεια IT δίνει έμφαση στην προστασία δεδομένων και εφαρμογών, στη διαχείριση ενημερώσεων λογισμικού και στον έλεγχο της πρόσβασης, ενώ η ασφάλεια OT δίνει προτεραιότητα στη σταθερότητα και την αξιοπιστία των βιομηχανικών διεργασιών με ισχυρούς ελέγχους πρόσβασης, συμπεριλαμβανομένων των μέτρων φυσικής ασφάλειας[39]. Τα χαρακτηριστικά του δικτύου διακρίνουν περαιτέρω το IT και το OT. Τα δίκτυα IT βασίζονται σε τυποποιημένα πρωτόκολλα και είναι σχεδιασμένα για συχνές ενημερώσεις. Τα δίκτυα OT, από την άλλη πλευρά, χρησιμοποιούν εξειδικευμένα βιομηχανικά πρωτόκολλα και είναι κατασκευασμένα για μεγάλους κύκλους ζωής, με τις αναβαθμίσεις να γίνονται σπάνια για τη διατήρηση της σταθερότητας των βιομηχανικών λειτουργιών. Για τους παραπάνω λόγους θα δοθεί έμφαση στις απειλές των OT συστημάτων στην ναυτιλία.

1.4.1 Κίνδυνοι στον Κυβερνοχώρο σε συστήματα επικοινωνίας

• Δορυφορικό σύστημα επικοινωνίας (SATCOM) & ολοκληρωμένο σύστημα επικοινωνίας (ICS)

- Ηλεκτρονικά μηνύματα ηλεκτρονικού «ψαρέματος»: Το εξουσιοδοτημένο προσωπικό του πληρώματος χρησιμοποιεί τον υπολογιστή στη γέφυρα του πλοίου για να έχει πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου για διάφορους σκοπούς, όπως, ενημερώσεις χαρτών, ενημερώσεις λογισμικού και λήψη ναυτιλιακών πληροφοριών από το κεντρικό τους γραφείο. Τα ηλεκτρονικά μηνύματα ηλεκτρονικού «ψαρέματος» στοχεύουν στην παράδοση κακόβουλου λογισμικού, όπως spyware, ransomware, ιούς, εξαπατώντας το θύμα να κάνει κλικ σε συνδέσμους ή να κατεβάσει μολυσμένα αρχεία. Η επίθεση αυτή μπορεί να οδηγήσει σε παραβίαση δεδομένων και μη διαθεσιμότητα συστημάτων. Τα ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος είναι ένας από τους συνήθεις τρόπους μέσω των οποίων οι επιτιθέμενοι μπορούν να εισέλθουν στο δίκτυο του πλοίου [40].

- Ξεπερασμένο λογισμικό VSAT: Συχνά, το λογισμικό VSAT δεν ενημερώνεται ή ενημερώνεται πολύ μετά την κυκλοφορία μιας ενημερωμένης επιδιόρθωσης. Οι ευπάθειες στις παλαιότερες εκδόσεις του λογισμικού συχνά δημοσιεύονται σε δημόσιους πόρους, τους οποίους οι επιτιθέμενοι στον κυβερνοχώρο μπορούν να χρησιμοποιήσουν για να εκμεταλλευτούν και να διαταράξουν τις λειτουργίες του πλοίου που εξαρτώνται από το SATCOM, καθώς και να διακόψουν την επικοινωνία μεταξύ πλοίου-ξηράς [41].

- Υποκλοπή: Η χρήση αδύναμων πρωτοκόλλων όπως το HTTP και το Telnet στη διεπαφή διαδικτυακής διαχείρισης VSAT μπορεί να επιτρέψει στον επιτιθέμενο να κρυφακούσει στο δίκτυο του σκάφους χρησιμοποιώντας εργαλεία υποκλοπής πακέτων και να υποκλέψει διαπιστευτήρια και ευαίσθητες πληροφορίες. Ο επιτιθέμενος είναι επίσης δυνατό να εισάγει ανεπιθύμητα δεδομένα στη διεπαφή ιστού ή να υποκλέψει ολόκληρη τη συνεδρία διαχείρισης [41] [42].

- Επίθεση cross-site scripting: Επιθέσεις κρυπτογράφησης μπορούν επίσης να εμφανιστούν σε μια κακοφτιαγμένη διεπαφή διαδικτυακής διαχείρισης VSAT. Οι επιτιθέμενοι μπορούν να ενημερωθούν για τις ευπάθειες σε διάφορες εκδόσεις VSAT από πηγές που δημοσιεύονται στο διαδίκτυο. Οι ελαττωματικές διαμορφώσεις καθαρισμού εισόδου μπορούν να επιτρέψουν στους χάκερ να εισάγουν αυθαίρετο κώδικα από την πλευρά του πελάτη. Λόγω αυτής της ευπάθειας, ένας επιτιθέμενος μπορεί να υποδυθεί έναν νόμιμο χρήστη και να στείλει κακόβουλους συνδέσμους, να τροποποιήσει τα διαπιστευτήρια, να καταγράψει τα

cookies και να καταλάβει τη σύνοδο [41] [42].

- Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο σκαφών: Η χρήση αδύναμων ή προεπιλεγμένων διαπιστευτηρίων ονόματος χρήστη και κωδικού πρόσβασης στη διεπαφή διαδικτυακής διαχείρισης VSAT μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στο δίκτυο σκάφους, μέσω της οποίας ένας εισβολέας μπορεί να αποκτήσει προνόμια όπως πρόσβαση διαχείρισης, πρόσβαση FTP και πρόσβαση στη γραμμή εντολών. Με αυτά τα προνόμια, ο εισβολέας μπορεί να προβάλει/επεξεργαστεί εμπιστευτικά αρχεία και να θέσει σε κίνδυνο άλλα συστήματα πλοίου στο δίκτυο. Τις περισσότερες φορές, οι προεπιλεγμένοι κωδικοί πρόσβασης δεν αλλάζουν ή οι κωδικοί πρόσβασης που έχουν οριστεί είναι πολύ αδύναμοι, π.χ. κοινοί κωδικοί πρόσβασης όπως 1234, abcd, οι οποίοι μπορούν εύκολα να σπάσουν με τη χρήση επιθέσεων ωμής βίας ή λεξικού [41] [43].

• Voice Over Internet Protocol (VOIP) [44]

- Επίθεση άρνησης υπηρεσίας (DoS): Αυτό θα εξαντλήσει το μέγιστο διαθέσιμο εύρος ζώνης και θα διαταράξει την κυκλοφορία των κλήσεων VOIP. Η επίθεση αυτή έχει ως αποτέλεσμα τη μη διαθεσιμότητα του δικτύου, η οποία με τη σειρά της προκαλεί έλλειψη επικοινωνίας στο εσωτερικό του πλοίου και μεταξύ πλοίου-ξηράς. Αποτελεί σοβαρή απειλή για το πλήρωμα και τις λειτουργίες του πλοίου, ιδίως εάν το δίκτυο δεν είναι διαθέσιμο κατά τη διάρκεια μιας έκτακτης ανάγκης.

- Υποκλοπή: Η χρήση ενός μη κρυπτογραφημένου δικτύου ή ενός ανεπαρκώς κρυπτογραφημένου δικτύου για κλήσεις VOIP μπορεί να οδηγήσει σε υποκλοπή, προκαλώντας παραβίαση της εμπιστευτικότητας και της ιδιωτικής ζωής. Οι χάκερς θα μπορούν να αποκτήσουν προσωπικές και εμπιστευτικές πληροφορίες με τη μη εξουσιοδοτημένη υποκλοπή μιας μη κρυπτογραφημένης κίνησης VOIP χρησιμοποιώντας εργαλεία εντοπισμού πακέτων όπως το Wireshark.

- Ηλετρονικό φωνητικό ψάρεμα: Το Ηλετρονικό φωνητικό ψάρεμα (Φωνητικό Ηλεκτρονικό ψάρεμα) είναι μια επίθεση κατά την οποία ένας επιτιθέμενος προσποιείται ότι είναι νόμιμη πηγή και εξαπατά το θύμα ώστε να παράσχει ευαίσθητες πληροφορίες. Αυτή η επίθεση πραγματοποιείται συνήθως με την παραποίηση της ταυτότητας καλούντο, για την οποία διατίθενται πολλά εργαλεία στο διαδίκτυο. Το κίνητρο μιας επίθεσης ηλεκτρονικό φωνητικό ψάρεμα θα ήταν να χειραγωγήσει το θύμα για να αποκτήσει ευαίσθητες πληροφορίες, όπως η τοποθεσία του πλοίου, τα στοιχεία του φορτίου, τα στοιχεία του πληρώματος κ.λπ..

• Ασύρματο τοπΙκό δίκτυο (WLAN) [45]

- Επίθεση άρνησης παροχής υπηρεσιών (DoS): Οι χάκερς μπορούν να εξαπολύσουν επίθεση DoS κατακλύζοντας το σημείο πρόσβασης/δρομολογητή με ψεύτικα αιτήματα σύνδεσης, προκαλώντας επιβράδυνση ή διακοπή του δικτύου, με αποτέλεσμα τη μη διαθεσιμότητα του διαδικτύου και των πόρων. Αυτά τα ψεύτικα αιτήματα προσπαθούν να εξαντλήσουν τη χωρητικότητα του εύρους ζώνης ενός σημείου πρόσβασης και να εμποδίσουν ένα νόμιμο αίτημα να φτάσει στο στόχο. Η επίθεση DoS προκαλεί μη διαθεσιμότητα του δικτύου και έλλειψη επικοινωνίας μεταξύ πλοίου και ξηράς, γεγονός που αποτελεί σοβαρή απειλή για το πλήρωμα και το σκάφος.
- Παραποίηση σημείου πρόσβασης: Καθώς τα πλοία έχουν μεγάλες περιοχές

λειτουργίας, πρέπει να τοποθετηθούν πολλά σημεία πρόσβασης σε διαφορετικές τοποθεσίες για γρήγορη και σταθερή πρόσβαση στο Διαδίκτυο. Εάν όμως το σημείο πρόσβασης τοποθετηθεί σε θέση όπου μπορεί να υπάρξει φυσική πρόσβαση, μπορεί να υπάρξει παραποίηση, καθώς χρειάζονται μόλις λίγα δευτερόλεπτα για να επανέλθει το σημείο πρόσβασης στις εργοστασιακές ρυθμίσεις.

- Υποκλοπή υποκλοπών/κατάχρηση συνεδρίας: Η κρυπτογράφηση του δικτύου του σκάφους είναι ζωτικής σημασίας, καθώς η έλλειψη ενός ασφαλούς προτύπου κρυπτογράφησης μπορεί να επιτρέψει στους χάκερ να υποκλέψουν το δίκτυο του σκάφους. Χρησιμοποιώντας εργαλεία υποκλοπής πακέτων, οι χάκερ μπορούν να κρυφακούσουν στο δίκτυο του σκάφους και να κλέψουν διαπιστευτήρια σύνδεσης και άλλες ευαίσθητες πληροφορίες. Αυτό μπορεί επίσης να οδηγήσει σε πειρατεία συνόδου, η οποία είναι η εκμετάλλευση μιας έγκυρης συνόδου υπολογιστή για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες ή υπηρεσίες σε ένα σύστημα υπολογιστή. Δεδομένου ότι το δίκτυο του σκάφους 22 χρησιμοποιείται για τις λειτουργίες του σκάφους και την προσωπική χρήση του πληρώματος, είναι ζωτικής σημασίας η κρυπτογράφηση του δικτύου με τη χρήση ενός ασφαλούς προτύπου κρυπτογράφησης.

1.4.2 Κίνδυνοι στον Κυβερνοχώρο σε συστήματα πρόωσης, μηχανών και ελέγχου ισχύος

- Σύστημα ρυθμιστή κινητήρα

- Επίθεση Man-in-the-middle (MITM): Ένας επιτιθέμενος μπορεί να εξαπολύσει επίθεση MITM αποκτώντας πρόσβαση στο δίκτυο του σκάφους και στη συνέχεια να αλλοιώσει τη σειριακή επικοινωνία μεταξύ των ελεγκτών του κινητήρα και άλλων συσκευών, διαταράσσοντας την απόδοση του κινητήρα. Ορισμένες από τις παραμέτρους που θα μπορούσαν να αλλοιωθούν περιλαμβάνουν την ποσότητα έγχυσης καυσίμου, την πίεση, τη θερμοκρασία καύσης, τη θερμοκρασία του κινητήρα και την κατάσταση εκκίνησης/διακοπής λειτουργίας του κινητήρα [23].
- Επίθεση κακόβουλου λογισμικού (Malware attack): Καθώς οι παράμετροι του κινητήρα παρακολουθούνται και ελέγχονται από έναν υπολογιστή ή μια κονσόλα πολλαπλών λειτουργιών, θα μπορούσε να εισαχθεί κακόβουλο λογισμικό μέσω θυρών USB στο εν λόγω σύστημα, το οποίο θα μπορούσε να προκαλέσει δυσλειτουργία του κινητήρα, με αποτέλεσμα έκρηξη ή σωματική βλάβη που θα επηρέαζε το πλήρωμα, το πλοίο και τα συστήματα επί του σκάφους [21].

- Σύστημα καυσίμων

- Επίθεση Man-in-the-middle (MITM): Αυτή η επίθεση συμβαίνει όταν ένας επιτιθέμενος εισβάλλει στο δίκτυο του σκάφους και χειρίζεται τα σειριακά δεδομένα που ανταλλάσσονται μεταξύ του συστήματος παρακολούθησης του κινητήρα και του καυσίμου και άλλων συσκευών στο σειριακό δίκτυο. Παράμετροι όπως η στάθμη καυσίμου, η θερμοκρασία και το ιξώδες, πρέπει να παρακολουθούνται για την ασφαλή λειτουργία. Για παράδειγμα, ο δείκτης στάθμης καυσίμου στο σύστημα παρακολούθησης καυσίμων μπορεί να παραποιηθεί ώστε να δείχνει λάθος στάθμη καυσίμου, γεγονός που μπορεί να οδηγήσει σε προβλήματα όπως υπερφόρτωση της δεξαμενής αποθήκευσης καυσίμων ή καθυστέρηση στην άφιξη στον προορισμό [23].
- Επίθεση κακόβουλου λογισμικού: Όταν εισάγεται κακόβουλο λογισμικό στο σύστημα παρακολούθησης καυσίμων (μέσω θύρας USB), μπορεί να εκτελεστεί κακόβουλος κώδικας ή εντολές στο σύστημα. Εξαιτίας αυτού, οι διαμορφώσεις των παραμέτρων καυσίμου θα

μπορούσαν να τροποποιηθούν, γεγονός που με τη σειρά του θα μπορούσε να προκαλέσει δυσλειτουργία του συστήματος, με αποτέλεσμα έκρηξη ή σωματική βλάβη που θα επηρέαζε το πλήρωμα και το πλοίο [21].

- Σύστημα παρακολούθησης καl ελέγχου συναγερμών

- Επίθεση Man-in-the-middle (MITM): Ένας εισβολέας μπορεί να εξαπολύσει επίθεση MITM, εισερχόμενος στο δίκτυο του πλοίου και τροποποιώντας τις εντολές που σχετίζονται με τους συναγερμούς που μεταδίδονται μεταξύ των συστημάτων επί του πλοίου. Ο επιτιθέμενος μπορεί είτε να καταστείλει έναν συναγερμό είτε να εγείρει ψεύτικους συναγερμούς, και εξαιτίας αυτού, το πλήρωμα μπορεί να μην γνωρίζει μια πιθανή βλάβη του συστήματος ή μια κατάσταση έκτακτης ανάγκης, θέτοντας σε κίνδυνο ζωές και φορτίο [23].
- Επίθεση κακόβουλου λογισμικού: Η διείσδυση κακόβουλου λογισμικού μέσω θυρών USB στο σύστημα παρακολούθησης και ελέγχου συναγερμών μπορεί να προκαλέσει κακή λειτουργία του, απειλώντας το ασφαλές ταξίδι του πλοίου και του πληρώματος [21].

- Σύστημα διαχείρισης Ισχύος (PMS)

- Επίθεση Man-in-the-middle (MITM): Αυτή η επίθεση μπορεί να συμβεί εάν ένας χάκερ εισέλθει στο δίκτυο του πλοίου και καταφέρει να αλλοιώσει τα σειριακά δεδομένα που εισέρχονται και εξέρχονται από το σύστημα διαχείρισης ισχύος. Οι παραπλανητικές τιμές τάσης και συχνότητας μπορεί να οδηγήσουν σε διακοπή της παροχής ρεύματος σε όλα τα συστήματα του πλοίου και τα εμπορευματοκιβώτια φορτίου, με αντίκτυπο στις λειτουργίες του πλοίου και στο φορτίο [23].
- Επίθεση κακόβουλου λογισμικού: Η διείσδυση κακόβουλου λογισμικού μέσω θυρών USB στο σύστημα διαχείρισης ισχύος ενδέχεται να παραπλανήσει τις λειτουργίες του, με αποτέλεσμα τη διακοπή της παροχής ισχύος στο πλοίο. Εξαιτίας αυτού, οι λειτουργίες του πλοίου θα διακοπούν και τα εμπορεύματα που βρίσκονται μέσα στα εμπορευματοκιβώτια φορτίου (π.χ. εμπορευματοκιβώτιο Reefer) ενδέχεται να υποστούν ζημιά [21].

- Γεννήτρια έκτακτης ανάγκης καl μπαταρίες

Η επίθεση Man-in-the-middle (MITM) και η επίθεση κακόβουλου λογισμικού στο σύστημα διαχείρισης ισχύος είναι οι δύο κύριοι κίνδυνοι στον κυβερνοχώρο που επηρεάζουν μια γεννήτρια έκτακτης ανάγκης. Οι επιθέσεις στον κυβερνοχώρο που προκαλούν αποτυχία του συστήματος διαχείρισης ισχύος μπορεί να διαταράξουν την αυτόματη εκκίνηση της γεννήτριας έκτακτης ανάγκης, καθώς οι έλεγχοι της γεννήτριας είναι παρόντες στο σύστημα διαχείρισης ισχύος [23]. Εάν ένας επιτιθέμενος παραβιάσει το σύστημα διαχείρισης ισχύος, η γεννήτρια έκτακτης ανάγκης ενδέχεται να μην μπορέσει να ξεκινήσει όταν υπάρχει διακοπή ρεύματος ή χαμηλή τάση, επηρεάζοντας έτσι τις λειτουργίες του πλοίου και το φορτίο του. Για παράδειγμα, τα εμπορευματοκιβώτια ψυγείων μεταφέρουν ευαίσθητα στη θερμοκρασία εμπορεύματα που απαιτούν σταθερή ηλεκτρική ενέργεια καθ' όλη τη διάρκεια του ταξιδιού.

1.4.3 Κίνδυνοι στον Κυβερνοχώρο σε συστήματα πλοήγησης

- Σύστημα απεικόνισης ηλεκτρονικού χάρτη καl πληροφοριών (ECDIS) [23]

- Επίθεση κακόβουλου λογισμικού: Το κακόβουλο λογισμικό μπορεί να εισέλθει στο σύστημα ECDIS όταν ένα μέλος του πληρώματος εισάγει σκόπιμα ή ακούσια μια μολυσμένη με κακόβουλο λογισμικό μονάδα USB στη θύρα USB του συστήματος, με αποτέλεσμα να διαταράσσεται η λειτουργία του ECDIS.
- Επίθεση άρνησης παροχής υπηρεσιών (DoS): Μια επίθεση DoS συμβαίνει όταν ένας επιτιθέμενος υπερφορτώνει το δίκτυο με κίνηση, η οποία θέτει εκτός λειτουργίας το ECDIS και αφήνει το σκάφος χωρίς μέσο ασφαλούς πλοήγησης. Ο επιτιθέμενος μπορεί επίσης να υποκλέψει ENCs (ηλεκτρονικούς χάρτες ναυσιπλοΐας) μέσω μη εξουσιοδοτημένης πρόσβασης στο δίκτυο του πλοίου μέσω του Διαδικτύου.
- Spoofing: Λόγω της έλλειψης κρυπτογράφησης και ελέγχου ταυτότητας, είναι δυνατή η παραποίηση των εισερχόμενων μηνυμάτων απλού κειμένου από το δίκτυο NMEA προς το ECIDS, για παράδειγμα, η αλλοίωση των πληροφοριών χάρτη που μπορεί να οδηγήσει σε σύγκρουση πλοίου.

• Εντοπισμός και εμβέλεια ραδιοσυχνοτήτων (RADAR)

– Εισβολή κακόβουλου λογισμικού: Ένας πιθανός τρόπος διείσδυσης κακόβουλου λογισμικού στο σύστημα RADAR είναι όταν ο καπετάνιος ανοίγει ένα φορτωμένο με ιούς ηλεκτρονικό ταχυδρομείο που περιέχει διάγραμμα για ενημέρωση. Καθώς το ραντάρ συνδέεται με το ECDIS μέσω πρωτοκόλλων Ethernet, όταν ο χάρτης ενημερώνεται στο ECDIS, ο ιός μεταφέρεται και εγκαθίσταται στο ECDIS και φτάνει στο ραντάρ μέσω του τοπικού διακόπτη ethernet. Η επίθεση αυτή αλλοιώνει την οθόνη του ραντάρ διαγράφοντας τους στόχους που εμφανίζονται στην οθόνη, τυφλώνοντας ουσιαστικά το πλοίο [46].
- Επίθεση Man-in-the-middle (MITM): Στην υπηρεσία SMB (Server Message Block) που εκτελείται στο ραντάρ, δεν απαιτείται υπογραφή και υπογραφές ασφαλείας. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει αυτές τις ευπάθειες στην υπηρεσία SMB για να εξαπολύσει επίθεση MITM και να εκτελέσει κώδικα χωρίς έλεγχο ταυτότητας [47].

• Σύστημα αυτόματης αναγνώρισης (AIS)

- Spoofing: Αν το λογισμικό AIS δεν διαθέτει ενσωματωμένη ασφάλεια ή έλεγχο ταυτότητας, μπορεί να γίνει επίθεση παραποίησης με την έναρξη ενός ψεύτικου επίγειου πύργου που εκπέμπει δεδομένα AIS.Για παράδειγμα, η μετάδοση στοιχείων ενός ανύπαρκτου πλοίου σε πορεία σύγκρουσης μπορεί να οδηγήσει σε συναγερμό CPA, ο οποίος μπορεί να αναγκάσει το πλοίο να παρεκκλίνει από την πορεία του και να συγκρουστεί πράγματι με εμπόδιο ή να προσαράξει [48].
- Επίθεση επανάληψης: Ένας επιτιθέμενος μπορεί να εξαπολύσει επίθεση επανάληψης εκτελώντας πλαστογραφημένες εντολές για να καθυστερήσει τον χρόνο μετάδοσης και να την ξαναστείλει ξανά και ξανά, με αποτέλεσμα μια επίθεση DoS.Αυτό μπορεί να έχει ως αποτέλεσμα την απενεργοποίηση της οθόνης AIS.

- Επίθεση μεταπήδησης συχνότητας: Οι λιμενικές αρχές παρέχουν συγκεκριμένες οδηγίες στον αναμεταδότη AIS του πλοίου να λειτουργεί σε μια συγκεκριμένη συχνότητα. Ένας επιτιθέμενος μπορεί να είναι σε θέση να παραποιήσει μια τέτοια εντολή για να αλλάξει τη συχνότητα. Εξαιτίας αυτής της επίθεσης άλματος συχνότητας, το πλοίο δεν θα είναι σε θέση να εκπέμψει ή να λάβει επικοινωνίες στη συχνότητα, επομένως τα στοιχεία του πλοίου ενδέχεται να μην είναι ορατά στην οθόνη AIS άλλων πλοίων [49].

- Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS)

- GPS Spoofing: Ένας επιτιθέμενος μπορεί να ξεκινήσει μια επίθεση GPS Spoofing στέλνοντας ψεύτικα σήματα GPS που μεταμφιέζονται σε πραγματικά σήματα. Αυτό θα παραπλανήσει τον δέκτη και θα τον κάνει να πιστέψει ότι η θέση του είναι ακριβής, ενώ στην πραγματικότητα είναι λανθασμένη, όπως έχει παραποιηθεί από τον επιτιθέμενο. Αυτή η επίθεση μπορεί να παραπλανήσει τα πλοία να πλοηγηθούν λανθασμένα και μπορεί επίσης να οδηγήσει σε συγκρούσεις πλοίου με πλοίο και πλοίου με στεριά [50].
- Παρεμπόδιση GPS: Ο επιτιθέμενος μπορεί να προκαλέσει παρεμβολές στα σήματα του παγκόσμιου δορυφορικού συστήματος πλοήγησης (GNSS).Το σήμα παρεμβολής θα είναι σημαντικά μεγαλύτερο από το σήμα GPS, εμποδίζοντας έτσι τη λήψη GPS. Αυτό θα προκαλέσει την εμφάνιση λανθασμένων θέσεων από το GPS και την παρουσίαση παραπλανητικών πληροφοριών στο AIS και στο ECDIS [51].

- Δυναμικό σύστημα εντοπισμού θέσης (DPS) [52]

- Επίθεση άρνησης παροχής υπηρεσιών (DoS): Ένας επιτιθέμενος μπορεί να προκαλέσει καταιγίδα δικτύου στο δέκτη του παγκόσμιου δορυφορικού συστήματος πλοήγησης (GNSS) και να εξαπολύσει επίθεση DoS. Αυτό θα προκαλέσει μη διαθεσιμότητα του συστήματος DP καθώς λαμβάνει σήματα (πληροφορίες θέσης) από τον δέκτη GNSS. Αυτό μπορεί να συμβεί όταν το λογισμικό του συστήματος DP είναι ανεπαρκές ή δεν έχει ενημερωθεί.
- Spoofing: Το Spoofing περιλαμβάνει τη μετάδοση ψευδών σημάτων στο δέκτη GNSS, παρόμοια με το GPS Spoofing, με αποτέλεσμα την εμφάνιση λανθασμένων πληροφοριών θέσης στην οθόνη του DPS.Αυτό θα οδηγήσει το πλοίο να αλλάξει την πορεία του λόγω των παραπλανητικών πληροφοριών στην οθόνη DPS.
- Επίθεση από πίσω πόρτα: Ο επιτιθέμενος μπορεί να εκτελέσει επίθεση backdoor για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα DP εγκαθιστώντας κακόβουλο λογισμικό που μπορεί να ξεπεράσει την κανονική πιστοποίηση ταυτότητας για πρόσβαση στο σύστημα. Αυτό θα έχει ως αποτέλεσμα ο επιτιθέμενος να πάρει τον έλεγχο του συστήματος και να παραπλανήσει τις λειτουργίες.

- Παγκόσμιο Σύστημα Ασφάλειας Ναυτικού ΚΙΝδύνου (GMDSS)

- Spoofing: Το GMDSS είναι ευάλωτο σε επιθέσεις στον κυβερνοχώρο. Ο επιτιθέμενος μπορεί να παραποιήσει τις εντολές κινδύνου και να παραδώσει ψευδείς πληροφορίες, προκαλώντας έτσι σύγχυση και καθυστέρηση στις επιχειρήσεις κινδύνου.
- Υποκλοπή: Ένας επιτιθέμενος μπορεί να υποκλέψει τα μηνύματα κινδύνου με υποκλοπή των σημάτων, με αποτέλεσμα την απώλεια της εμπιστευτικότητας [53].
- Επίθεση άρνησης παροχής υπηρεσιών (DoS): Εάν μια μολυσμένη από κακόβουλο λογισμικό εφαρμογή υπάρχει στο σύστημα και εκτελείται, τότε μπορεί να ξεκινήσει μια επίθεση DoS, με αποτέλεσμα να διακόπτεται η επικοινωνία μεταξύ των πλοίων και του πλοίου-ξηράς. Τα προβλήματα με τη μετάδοση και τη λήψη μηνυμάτων μπορεί να οδηγήσουν σε απώλεια ζωών κατά τη διάρκεια μιας κατάστασης κινδύνου [54].

- Voyage Data Recorder (VDR) [23]

- Επίθεση κακόβουλου λογισμικού: Μέσω του οποίου ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο VDR και να τα αλλοιώσει, να τα κλέψει ή να τα καταστρέψει.
- Απομακρυσμένη εκτέλεση κώδικα: Λόγω των τρωτών σημείων στις υπηρεσίες που εκτελούνται στο VDR, οι επιτιθέμενοι μπορούν να εκτελέσουν κώδικα με δικαιώματα διαχειριστή (root), έχοντας κατά συνέπεια απεριόριστη πρόσβαση εντός του λειτουργικού συστήματος. Αυτά τα προνόμια μπορούν επίσης να επιτρέψουν σε έναν εισβολέα να αλλοιώσει τις ενδείξεις ταχύτητας, θέσης, πορείας και να διαγράψει συνομιλίες από τη γέφυρα, να διαγράψει εικόνες ραντάρ κ.λπ.

• Ολοκληρωμένο σύστημα πλοήγησης (INS) [35]

- Επίθεση Man-in-the-middle (MITM): Λόγω του χαμηλού επιπέδου κρυπτογράφησης που χρησιμοποιείται στο διακομιστή πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (τερματική υπηρεσία) που εκτελείται στο INS, ένας εισβολέας μπορεί να πραγματοποιήσει επίθεση MITM και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα.
- Απομακρυσμένη εκτέλεση κώδικα: Εάν στο INS εκτελούνται παλαιότερες εκδόσεις της υπηρεσίας SMB (πιθανώς η έκδοση 1.0), ενδέχεται να εκτελεστεί απομακρυσμένη εκτέλεση κώδικα. Ένας απομακρυσμένος επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την ευπάθεια εκτελώντας κακόβουλο κώδικα χωρίς έλεγχο ταυτότητας, ο οποίος επιτρέπει την πρόσβαση στο σύστημα, όπου ο επιτιθέμενος μπορεί να εκτελέσει εντολές μέσω root και επίσης να αλλοιώσει ευαίσθητες πληροφορίες.

1.4.4 Κίνδυνοι στον Κυβερνοχώρο σε συστήματα διαχείρησης φορτίου

• Cargo Control Room (CCR) [47]

- Ransomware: Ως εκ τούτου, μηνύματα ηλεκτρονικού ταχυδρομείου ηλεκτρονικό ψάρεμα που έχουν δημιουργηθεί με κακόβουλο λογισμικό, όπως ransomware, μπορεί να σταλούν στον υπεύθυνο του δωματίου ελέγχου φορτίου. Εάν αποκτήσει πρόσβαση σε έναν κακόβουλο σύνδεσμο ή εάν κατεβάσει και εγκαταστήσει ένα κακόβουλο αρχείο, τότε το ransomware θα εξαπλωθεί και θα μολύνει το σύστημα παρακολούθησης φορτίου και άλλες συσκευές στο δίκτυο του πλοίου. Ως εκ τούτου, όλες οι συσκευές θα κρυπτογραφηθούν και δεν θα είναι δυνατή η πρόσβαση σε αυτές, εκτός εάν καταβληθούν λύτρα. Αυτό με τη σειρά του θα προκαλέσει οικονομικές απώλειες και θα διαταράξει τη λειτουργία του πλοίου και του φορτίου.
- Επίθεση με κακόβουλο λογισμικό: Το κακόβουλο λογισμικό μπορεί να εισχωρήσει στο σύστημα παρακολούθησης φορτίου εκούσια ή ακούσια με τη σύνδεση μιας μολυσμένης συσκευής USB στη θύρα USB. Ως εκ τούτου, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στο σύστημα και να κλέψει ή να παραποιήσει πληροφορίες που σχετίζονται με το φορτίο, όπως τιμές, αριθμό παρακολούθησης φορτίου, τόπο και ημερομηνία παράδοσης κ.λπ. Για παράδειγμα, ο εισβολέας μπορεί να παραποιήσει τον τόπο παράδοσης σε λάθος προορισμό.

• Σύστημα νερού έρματος (BWS)

- Επίθεση κακόβουλου λογισμικού: Η παρακολούθηση και ο έλεγχος του συστήματος

νερού έρματος μπορεί να γίνει από τα συστήματα της γέφυρας του πλοίου ή το σύστημα του μηχανοστασίου. Εάν εισαχθεί κακόβουλο λογισμικό μέσω θυρών USB στα εν λόγω συστήματα, ο επιτιθέμενος μπορεί να στείλει ψευδείς εντολές σχετικά με την αύξηση ή τη μείωση της στάθμης του νερού στο διαμέρισμα έρματος, με αποτέλεσμα το πλοίο να χάσει τη σταθερότητά του και να βυθιστεί [37].

- Ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος: Συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου μολυσμένα με κακόβουλο λογισμικό μπορεί να αποσταλούν στο σύστημα μέσω του οποίου παρακολουθείται το διαμέρισμα νερού έρματος. Εάν το εν λόγω σύστημα έχει μολυνθεί με κακόβουλο λογισμικό, τότε ο επιτιθέμενος μπορεί να παραβιάσει το σύστημα και να επέμβει στη λειτουργία των αισθητήρων, των ενεργοποιητών κ.λπ. και να προκαλέσει βλάβη στους σωλήνες και σε άλλα μέρη του συστήματος έρματος [23]. Αυτό θα προκαλέσει επίσης τη βύθιση του σκάφους λόγω αστάθειας.

1.4.5 STRIDE: Παράδειγμα

Από την ανάλυση των επιφανειών επίθεσης και των κινδύνων στον κυβερνοχώρο σε συστήματα ΛΤ πλοίων, είναι ορατό ότι καλύπτονται όλα τα χαρακτηριστικά του μοντέλου απειλών STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege) [54]. Μερικά παραδείγματα είναι τα ακόλουθα:

-Spoofing: Ένας αντίπαλος θα μπορούσε να παραποιήσει σήματα από το δέκτη GPS για να παραδώσει παραπλανητικές πληροφορίες για την πλοήγηση του πλοίου, λόγω της έλλειψης μηχανισμών πιστοποίησης ταυτότητας στο GPS.

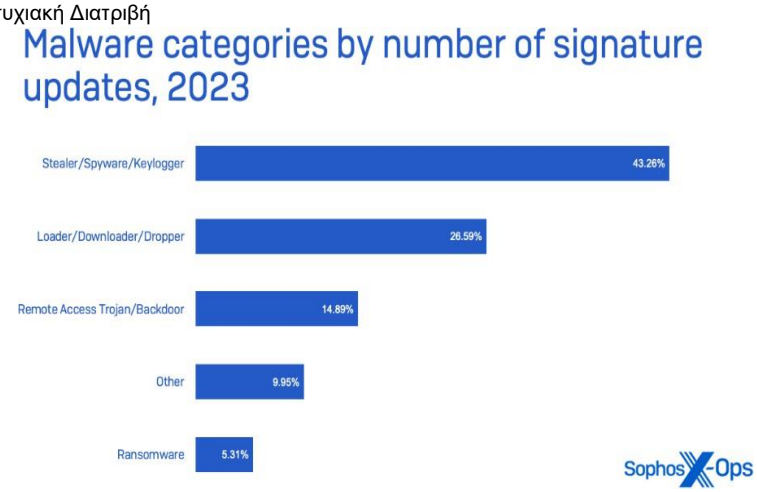
-Παραποίηση: Λόγω της έλλειψης κρυπτογράφησης και ελέγχου ταυτότητας στα πρωτόκολλα σειριακής επικοινωνίας, ο επιτιθέμενος μπορεί να αλλοιώσει την επικοινωνία που αναμεταδίδεται μεταξύ των συσκευών, με αποτέλεσμα την απώλεια της ακεραιότητας των δεδομένων και του ελέγχου του συστήματος.

-Ακύρωση: Ως εκ τούτου, ένας αντίπαλος μπορεί να πλαστογραφήσει τα μηνύματα AIS για να προκαλέσει σύγκρουση πλοίων. Τελικά, εάν το σύστημα δεν διαθέτει αρχεία καταγραφής για τον εντοπισμό του δράστη, τότε υπάρχει πιθανότητα απάρνησης.

-Αποκάλυψη πληροφορΙών: Η έλλειψη κρυπτογράφησης στη σύνδεση του πλοίου στο Διαδίκτυο μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών. Χρησιμοποιώντας εργαλεία υποκλοπής πακέτων, οι χάκερ μπορούν να κρυφακούσουν στο δίκτυο του πλοίου και να κλέψουν διαπιστευτήρια σύνδεσης και άλλες ευαίσθητες πληροφορίες.

-Άρνηση παροχής υπηρεσΙών: Ο επιτιθέμενος μπορεί να πραγματοποιήσει επίθεση άρνησης παροχής υπηρεσιών (DoS) στο δρομολογητή κατακλύζοντας το δρομολογητή με αιτήματα σύνδεσης, προκαλώντας επιβράδυνση ή διακοπή του δικτύου. Αυτό θα εμποδίσει τις νόμιμες συνδέσεις να αποκτήσουν πρόσβαση στους πόρους, με αποτέλεσμα να μην είναι διαθέσιμοι.

-Εξαίρεση προνομίων: Όταν χρησιμοποιούνται αδύναμα/προεπιλεγμένα διαπιστευτήρια ονόματος χρήστη και κωδικού πρόσβασης για τη σύνδεση στο περιβάλλον διαχείρισης VSAT web. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτές τις αδυναμίες και να αποκτήσει μη εξουσιοδοτημένη διοικητική πρόσβαση στο δίκτυο σκάφους. Με αυτό το προνόμιο, ο επιτιθέμενος θα είναι σε θέση να διαβάσει και να τροποποιήσει εμπιστευτικά αρχεία και να θέσει σε κίνδυνο άλλα συστήματα πλοίου στο δίκτυο.



Εικόνα 5. Ανιχνεύσεις κακόβουλου λογισμικού ανά τύπο για το 2023, όπως φαίνεται στα σύνολα δεδομένων των εργαστηρίων μας της Sophos X-ops. Εταιρία-ομάδας δράσης για την αντιμετώπιση προηγμένων απειλώ.

Στον ακόλουθο πίνακα παρατίθενται παραδείγματα απειλών, τα πιθανά κίνητρα και οι στόχοι εκείνων που επιτίθονται. Οι εν λόγω απειλητικοί παράγοντες θα έχουν διαφορετικούς βαθμούς δεξιοτήτων και πόρων για να απειλήσουν δυνητικά την ασφάλεια και την προστασία των πλοίων και την ικανότητα μιας εταιρείας να διεξάγει τις δραστηριότητές της [55].

Πίνακας 2. Παραδείγματα απειλών, πιθανά κίνητρα και στόχοι.[55]

Τυχαίοι Παράγοντες	Δεν υπάρχει κακόβουλο κίνητρο, αλλά καταλήγουν να προκαλούν ακούσια ζημιά από κακή τύχη.
Ακτιβιστές (συμπεριλαμβανομένων των δυσαρεστημένων εργαζομένων)	• εκδίκηση • διατάραξη της λειτουργίας • προσοχή των μέσων ενημέρωσης • ζημία φήμης
Εγκληματίες	• οικονομικό κέρδος • εμπορική κατασκοπεία • βιομηχανική κατασκοπεία
Ευκαιρίες	• η πρόκληση • κέρδος φήμης • οικονομικό κέρδος
• Κράτη • Κράτος που χρηματοδοτείται • οργανώσεις • Τρομοκράτες	• πολιτικό/ιδεολογικό κέρδος π.χ. (ανεξέλεγκτη) διατάραξη των οικονομιών και των κρίσιμων • εθνικές υποδομές • κατασκοπεία • οικονομικό-εμπορικό κέρδος

	• εμπορική-βιομηχανική κατασκοπεία

1.4.6 Στάδια Κυβερνοεπίθεσης

Η Microsoft αναφέρει ότι, κατά μέσο όρο, χρειάζονται 140 ημέρες για να αναγνωριστεί μια επίθεση (2018), χρόνος που έχει μειωθεί από τις 205 ημέρες του 2015. Παρόλα αυτά, συχνά οι παράνομες προσβάσεις παραμένουν αόρατες για χρόνια. Τα στάδια μιας επίθεσης περιλαμβάνουν:

-Παρακολούθηση/ΑναγνώρIση: Χρησιμοποιώντας δημόσιες πηγές, όπως τα κοινωνικά δίκτυα, οι επιτιθέμενοι συγκεντρώνουν πληροφορίες που μπορεί να αποκαλύπτουν αδυναμίες στα συστήματα της εταιρείας ή του πλοίου.

-Εγκατάσταση Κακόβουλου ΛογIσμIκού: Αυτό επιτυγχάνεται μέσω εταιρικών υπηρεσιών, παραπλανητικών email, μολυσμένων αφαιρούμενων μέσων ή ψευδών ιστοτόπων.

-Παραβίαση Συστήματος: Οι επιτιθέμενοι ενδέχεται να προχωρήσουν σε αλλαγές που επηρεάζουν τη λειτουργία του συστήματος, να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή ακόμα και να επιτύχουν πλήρη έλεγχο κάποιου συστήματος.

-Pivot: Μέσω του παραβιασμένου συστήματος, επιχειρούν επιθέσεις σε άλλα συστήματα εντός του δικτύου, παρακάμπτοντας πιθανές άμυνες όπως τα τείχη προστασίας.

Οι συνέπειες μίας επίθεσης εξαρτώνται από τα κίνητρα του επιτιθέμενου, ο οποίος μπορεί να αποσκοπεί σε:

- Πρόσβαση σε ευαίσθητα δεδομένα,
- Παραβίαση καταλόγων πληρώματος ή φορτίου,
- Προκαλώντας άρνηση εξυπηρέτησης (DoS),
- Ενεργοποίηση άλλων μορφών εγκλήματος, όπως κλοπές ή απάτες,
- Διατάραξη της λειτουργίας συστημάτων της εταιρίας ή του πλοίου.

Αυτά τα στάδια, τα κίνητρα και οι στόχοι καθιστούν τις επιθέσεις πολυεπίπεδες και δυσχεραίνουν τη διασφάλιση της κυβερνοασφάλειας [56].

1.5 Σύνοψη του Πρώτου Κεφαλαίου

Στην ενότητα 1 εξετάζω τις τεχνολογίες που είναι θεμελιώδεις για τη ναυτιλιακή βιομηχανία και τους κινδύνους κυβερνοασφάλειας που συνδέονται με την υιοθέτησή τους. Ενώ ο τομέας εφαρμόζει εξελιγμένα συστήματα IT και συστήματα OT, συμπεριλαμβανομένων των δικτύων επικοινωνίας, των βοηθημάτων πλοήγησης και των αυτοματοποιημένων συστημάτων ελέγχου, έχει πράγματι αποδειχθεί πολύ ευάλωτος από άποψη κυβερνοασφάλειας. Ενώ στην πραγματικότητα, οι δορυφορικές επικοινωνίες, η πρόωση και ο έλεγχος ισχύος και τα συστήματα πλοήγησης των ναυτιλιακών συστημάτων εξαρτώνται σχετικά από ψηφιακά δίκτυα που προάγουν την επιχειρησιακή αποτελεσματικότητα, εκθέτοντας τα πλοία και τις υποδομές σε απειλές στον κυβερνοχώρο -συμπεριλαμβανομένης της μη εξουσιοδοτημένης πρόσβασης, της παραβίασης δεδομένων και των πιθανών διαταραχών που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια και την αποτελεσματικότητα.
Αυτή η σύγκλιση στη ναυτιλία παρέχει μοναδικές προκλήσεις, επειδή τα συστήματα συνήθως δεν έχουν ολοκληρωμένη ασφάλεια σε σύγκριση με άλλες βιομηχανίες. Ως εκ τούτου, είναι καιρός να υπάρξουν δομημένοι μηχανισμοί κυβερνοασφάλειας στον τομέα της ναυτιλίας. Η προοπτική πλαισίων, όπως το NIST CyberSecurity Framework, παρέχει μια διέξοδο προς τα εμπρός, δεδομένου ότι αναλύει λεπτομερώς την οργάνωση πολιτικών για τον εντοπισμό, την προστασία, την ανίχνευση, την αντίδραση και την ανάκαμψη από συμβάντα κυβερνοασφάλειας. Στην επόμενη ενότητα, θα διαπιστώσουμε ότι υπάρχουν πρακτικοί τρόποι για αξιολόγηση, την πρόληψη ή τον χειρισμό μιας απειλής στον κυβερνοχώρο, καθώς και πολλές περιπτώσεις όπου οι άμυνες εταιριών-οργανισμών αποδείχτηκαν υποβαθμισμένες σε κυβερνοεπιθέσεις στο παρελθόν. Ωστόσο θα δούμε πως η υιοθέτηση πλαισίων όπως το NIST CSF μπορεί να αποτελέσει το κλειδί για την αντιμετώπιση των υφιστάμενων τρωτών σημείων και τη διασφάλιση της ανάπτυξης της κατάλληλης ανθεκτικότητας στον κυβερνοχώρο στη ναυτιλιακή βιομηχανία.

2. Τι είναι το NIST

2.1 Μετρίαση του κινδύνου

Τα μέτρα μετριασμού που παρέχονται στην παρούσα ενότητα αφορούν ειδικά τους κινδύνους στον κυβερνοχώρο που εντοπίστηκαν στα τέσσερα κύρια συστήματα OT του πλοίου, δηλαδή στα συστήματα επικοινωνίας, στα συστήματα πρόωσης, στα συστήματα ελέγχου μηχανών και ισχύος, στα συστήματα πλοήγησης και στα συστήματα διαχείρισης φορτίου. Τα εν λόγω μέτρα μετριασμού καλύπτουν τρεις κατηγορίες μέτρων, δηλαδή τεχνικά, διαδικαστικά και φυσικά μέτρα ασφαλείας. Μερικά από τα πολλά μέτρα περιλαμβάνουν τεχνικά μέτρα ασφαλείας, όπως τείχη προστασίας και εικονικά ιδιωτικά δίκτυα (VPN), διαχωρισμό της κίνησης OT και IT και εγκατάσταση αντι-κακόβουλου λογισμικού, φυσικά μέτρα ασφαλείας, συμπεριλαμβανομένων των καταλόγων ελέγχου πρόσβασης και της διασφάλισης ευαίσθητων συσκευών, και διαδικαστικά μέτρα που περιλαμβάνουν ενημερώσεις λειτουργικών συστημάτων και λογισμικού, μηχανισμούς επαναφοράς κωδικών πρόσβασης, ευαισθητοποίηση και εκπαίδευση του πληρώματος. Ως εκ τούτου, αυτοί οι έλεγχοι ασφαλείας συνιστώνται στους πλοιοκτήτες να τους επιβάλουν στα πλοία τους για να προστατευθούν από σημαντικές απειλές στον κυβερνοχώρο. Ο Πίνακας 3 παρέχει λεπτομερέστερη περιγραφή των μέτρων μετριασμού για τη διαχείριση των κινδύνων στον κυβερνοχώρο στα συστήματα OT των πλοίων.

2.1.1 Μέτρα μετριασμού για τα συστήματα επικοινωνίας

Πίνακας 3. SATCOM και ICS [44,45,57,58,59,60,61,62]

Δορυφορικό σύστημα επικοινωνίας (SATCOM) και ολοκληρωμένο σύστημα επικοινωνίας (ICS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Ηλεκτρονικό ψάρεμα μέσω ηλεκτρονικής αλληλογραφίας (Επίθεση κακόβουλου λογισμικού)	Στους υπολογιστές της επιχείρησης πρέπει να εγκατασταθεί λογισμικό προστασίας από ιούς. [57] - Τα αρχεία και τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνονται από μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να σαρώνονται με λογισμικό προστασίας από ιούς για να ελέγχονται για ιούς/κακόβουλο λογισμικό. - Πρέπει να δημιουργούνται τακτικά αντίγραφα ασφαλείας των δεδομένων και να αποθηκεύονται με ασφάλεια. - Το πλήρωμα πρέπει να ευαισθητοποιηθεί για τα ακόλουθα: - Δυνατότητα διάκρισης των ηλεκτρονικών μηνυμάτων ηλεκτρονικού ταχυδρομείου τύπου ηλεκτρονικό ψάρεμα από τα πραγματικά - Να γνωρίζουν ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστες πηγές πρέπει να εξετάζονται προσεκτικά και τα ύποπτα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου δεν πρέπει να ανοίγονται, ιδίως να μην ενεργοποιείται η λειτουργία μακροεντολών σε έγγραφα της Microsoft.

	- Να γνωρίζουν ότι δεν πρέπει να κάνουν κλικ σε ύποπτους συνδέσμους - Θα πρέπει να εφαρμοστεί η ασφάλεια του ηλεκτρονικού ταχυδρομείου
	- Για παράδειγμα, μπορεί να εφαρμοστεί το S/MIME (Secure Multipurpose Internet Mail Extension) για την κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου και τη διασφάλιση της αυθεντικότητας και της ακεραιότητας του ηλεκτρονικού ταχυδρομείου [58]
Ξεπερασμένο λογισμικό VSAT	- Η τελευταία έκδοση του λογισμικού πρέπει να είναι εγκατεστημένη στα τερματικά VSAT. - Οι ενημερώσεις λογισμικού πρέπει να ελέγχονται τακτικά για να διορθώνονται τα τρωτά σημεία. - Όλες οι ενημερώσεις πρέπει να καταγράφονται. Εάν πραγματοποιείται απομακρυσμένη υπηρεσία/συντήρηση ή ενημέρωση, η αυθεντικότητα της υπηρεσίας του προμηθευτή, της ενημέρωσης και της σύνδεσης απομακρυσμένης επιφάνειας εργασίας πρέπει να επαληθεύεται χειροκίνητα (π.χ. τηλεφωνική κλήση) πριν επιτραπεί η πρόσβαση για τη συγκεκριμένη απαίτηση. [59]
Υποκλοπές	Η διαδικτυακή διεπαφή διαχείρισης του τερματικού (VSAT) θα πρέπει να υποστηρίζει ασφαλή πρωτόκολλα όπως HTTPS, SSHv2.
Έγχυση κακόβουλου κώδικα	Η διαδικτυακή διεπαφή VSAT θα πρέπει να διαθέτει ενσωματωμένους μηχανισμούς ασφαλείας, όπως εξυγίανση εισόδου (κάθε ύποπτη είσοδος πρέπει να απορρίπτεται), κωδικοποίηση εξόδου, CSP (Content Security Policy) για την προστασία από επιθέσεις scripting [60].
Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο σκαφών: Διοικητική πρόσβαση, πρόσβαση FTP και πρόσβαση στη γραμμή εντολών	-Το τείχος προστασίας πρέπει να ρυθμιστεί ώστε να επιτρέπει μόνο τις πηγές ή τις διευθύνσεις IP που περιλαμβάνονται στη λευκή λίστα εντός ενός υποδικτύου. - Κατά την πρόσβαση στο Διαδίκτυο πρέπει να χρησιμοποιείται εικονικό ιδιωτικό δίκτυο. - Η διεύθυνση IP πρέπει να είναι ιδιωτική και να μην είναι διαθέσιμη σε κανένα δημόσιο τομέα (π.χ. Shodan). - Το λειτουργικό σύστημα, το antivirus, το τείχος προστασίας και άλλες εφαρμογές που χρησιμοποιούνται στον υπολογιστή της επιχείρησης (ο υπολογιστής που χρησιμοποιείται για την πρόσβαση στα μηνύματα ηλεκτρονικού ταχυδρομείου και η διεπαφή web του μόντεμ VSAT) πρέπει να ενημερώνονται/επιδιορθώνονται τακτικά.

	- Η πρόσβαση στον επαγγελματικό υπολογιστή θα πρέπει να περιορίζεται σε εξουσιοδοτημένο προσωπικό με διαχειριστική σύνδεση και ισχυρά διαπιστευτήρια. - Το προεπιλεγμένο όνομα χρήστη και ο κωδικός πρόσβασης στο μόντεμ VSAT πρέπει να αλλάξουν. Ο κωδικός πρόσβασης πρέπει να είναι ισχυρός,για παράδειγμα, συνιστάται κωδικός πρόσβασης με 8 χαρακτήρες και τουλάχιστον ένα κεφαλαίο γράμμα και έναν ειδικό χαρακτήρα. - Θα πρέπει να εφαρμόζονται μηχανισμοί επαναφοράς του κωδικού πρόσβασης- συνιστάται η αλλαγή του κωδικού πρόσβασης μία φορά ανά τρεις μήνες.
	- Μην καταγράφετε τους κωδικούς πρόσβασης σε σημειωματάρια ή αυτοκόλλητες σημειώσεις, για την αποθήκευση των κωδικών πρόσβασης μπορεί να χρησιμοποιηθεί μια ασφαλής εφαρμογή διαχείρισης κωδικών πρόσβασης ή ένα έγγραφο PDF/Word που προστατεύεται με κωδικό πρόσβασης. - Η πρόσβαση στον υπολογιστή της επιχείρησης πρέπει να μπλοκάρεται μετά από έναν αριθμό αποτυχημένων προσπαθειών σύνδεσης, π.χ. 5 προσπάθειες - Είναι καλό να υπάρχει έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) για την πρόσβαση στον υπολογιστή της επιχείρησης και στη διαδικτυακή διεπαφή VSAT. Το FTP πρέπει να είναι απενεργοποιημένο στη διεπαφή ιστού του μόντεμ VSAT

Φωνή μέσω πρωτοκόλλου Διαδικτύου (VOIP) | Μέτρα Περιορισμού [44],[61]	
Επίθεση άρνησης παροχής υπηρεσιών (DoS)	- Διαχωρίστε την κυκλοφορία δεδομένων και τη φωνητική κυκλοφορία , χρησιμοποιήστε ένα VLAN (Virtual Local Area Network)/Firewall αποκλειστικά για την κυκλοφορία VOIP. - Η ομάδα πληροφορικής πρέπει να παρακολουθεί συχνά το δίκτυο VOIP χρησιμοποιώντας συστήματα ανίχνευσης εισβολών.
Υποκλοπή	Η κυκλοφορία VOIP πρέπει να κρυπτογραφείται με ένα ασφαλές πρότυπο κρυπτογράφησης.
Ηλετρονικό φωνητικό ψάρεμα	Το πλήρωμα πρέπει να γνωρίζει ότι δεν πρέπει να παρέχει προσωπικά στοιχεία ή πληροφορίες σκάφους εάν λαμβάνει κλήσεις από άγνωστες πηγές.

Ασύρματο τοπικό δίκτυο (WLAN) | Μέτρα μετριασμού [45, 62]	
Επίθεση άρνησης παροχής υπηρεσιών (DoS)	- Το τείχος προστασίας πρέπει να έχει ρυθμιστεί ώστε να επιτρέπει τη σύνδεση μόνο για πηγές που περιλαμβάνονται στη λευκή λίστα. - Η ομάδα πληροφορικής πρέπει να παρακολουθεί συχνά το δίκτυο χρησιμοποιώντας συστήματα ανίχνευσης εισβολών.
Παραποίηση σημείου πρόσβασης	Οι δρομολογητές/σημεία πρόσβασης πρέπει να φυλάσσονται σε ασφαλές μέρος, όπως σε κλειδωμένο ντουλάπι.
Υποκλοπή / Session hijacking	Στα ασύρματα δίκτυα πρέπει να χρησιμοποιείται ένα ασφαλές πρότυπο κρυπτογράφησης. Ως ελάχιστο επίπεδο ασφάλειας πρέπει να χρησιμοποιείται το WEP (Wired Equivalent Privacy). Συνιστάται η χρήση ισχυρότερων προτύπων κρυπτογράφησης, όπως το WiFi PrOTected Access3..

2.1.2 Μέτρα μετριασμού για την πρόωση, τα μηχανήματα και τα συστήματα ελέγχου ισχύος

Πίνακας 4. Μέτρα Μετριασμού συστημάτων. [55,63,64]

Σύστημα καυσίμου πετρελαίου, σύστημα ρυθμιστή κινητήρα, σύστημα παρακολούθησης και ελέγχου συναγερμών, ισχύς, Σύστημα διαχείρισης, γεννήτριες και μπαταρίες έκτακτης ανάγκης	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού

Άνθρωπος στη μέση (ΑΣΜ- MITM:Man-In-The-Middle) επίθεση	-Το SATCOM πρέπει να είναι ασφαλές, όπως αναφέραμε στον Πίνακα 3. - Η απειλή ηλεκτρονικού ταχυδρομείου ηλεκτρονικό ψάρεμα πρέπει να μετριαστεί, όπως αναφέραμε προηγουμένως. - Λειτουργικό σύστημα, antivirus και άλλες εφαρμογές στον κινητήρα και στην παρακολούθηση καυσίμων συστήματος, του συστήματος παρακολούθησης και ελέγχου συναγερμών και της διαχείρισης ισχύος πρέπει να ενημερώνονται συχνά. - Η πρόσβαση του πληρώματος στα κρίσιμα συστήματα και στους υπολογιστές που ελέγχουν και παρακολουθούν τα μηχανήματα πρέπει να ρυθμίζονται. - Εάν γίνεται εξ αποστάσεως συντήρηση/συντήρηση σε οποιοδήποτε από τα συστήματα, η αυθεντικότητα της υπηρεσίας του προμηθευτή και η σύνδεση απομακρυσμένης επιφάνειας εργασίας πρέπει να επαληθεύεται χειροκίνητα (π.χ. τηλεφωνική κλήση) και στη συνέχεια να επιτρέπεται η πρόσβαση. - Το δίκτυο OT πρέπει να διαχωρίζεται από το δίκτυο IT με τείχος προστασίας/ΔΜΖ. [55, 63]. - Εάν χρησιμοποιείται μετατροπέας Serial-to-IP, πρέπει να υποστηρίζει κρυπτογράφηση, λογισμικό οι ενημερώσεις πρέπει να γίνονται τακτικά και τα διαπιστευτήρια πρέπει να είναι ισχυρά [64].
Επίθεση κακόβουλου λογισμικού (μέσω θυρών USB)	-Το λογισμικό Antivirus πρέπει να είναι εγκατεστημένο στον έλεγχο των μηχανημάτων και συστήματα παρακολούθησης. - Τα μέτρα φυσικής ασφάλειας πρέπει να εφαρμόζονται ως εξής: • Λίστα ελέγχου πρόσβασης για την είσοδο του πληρώματος στο δωμάτιο ελέγχου μηχανών ή σε οποιοδήποτε άλλο χώρο όπου υπάρχουν κρίσιμα μηχανήματα. • Ο κατάλογος ελέγχου πρόσβασης πρέπει να επανεξετάζεται και να ενημερώνεται τακτικά. - Θύρες USB στο σύστημα παρακολούθησης μηχανών και καυσίμων, παρακολούθησης συναγερμών και σύστημα ελέγχου και το σύστημα διαχείρισης ενέργειας πρέπει να ενεργοποιούνται μόνο σε διαχειριστή και να απενεργοποιούνται στις άλλες συνδέσεις χρηστών (εάν υπάρχουν) και στη σύνδεση του συστήματος πρέπει να έχουν ισχυρό όνομα χρήστη και κωδικό πρόσβασης. - Για τον αποκλεισμό των αχρησιμοποίητων θυρών μπορούν να χρησιμοποιηθούν αποκλειστές θυρών USB. - Για το πλήρωμα πρέπει να οριστούν ειδικά σημεία φόρτισης (θύρες).

	- Πρέπει να εγκατασταθεί σταθμός καθαρισμού USB - Ένας ξεχωριστός υπολογιστής με antivirus λογισμικό για τη σάρωση των μονάδων USB πριν από τη χρήση [55, 63].

2.1.3 Μέτρα μετριασμού για τα συστήματα πλοήγησης

Πίνακας 5. Μετριασμός στην πλοήγηση [65-75]

Ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών (ECDIS)		Ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών (ECDIS)
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού	
Επίθεση κακόβουλου λογισμικού (μέσω θυρών USB)	-Το λογισμικό Antivirus πρέπει να είναι εγκατεστημένο στο σύστημα ECDIS για να σαρώνει κάθε εξωτερικά μέσα πριν από τη σύνδεσή τους στο σύστημα. - Οι ενημερώσεις χαρτών ECDIS πρέπει να καταγράφονται. -Οι θύρες USB πρέπει να είναι απενεργοποιημένες και να ενεργοποιούνται μόνο από τον καπετάνιο του πλοίου όποτε υπάρχει ανάγκη χρήσης USB ή να ενεργοποιείται μόνο κατά τη σύνδεση του διαχειριστή και απενεργοποιημένη σε άλλες συνδέσεις χρηστών.	
	- Χρησιμοποιήστε αποκλειστές θυρών USB για να αποφύγετε τα περιττά plugins.	

Άρνηση παροχής υπηρεσιών (DoS) επίθεση	- Η εγκατάσταση τείχους προστασίας στο σύστημα ECDIS θα περιορίσει τις μη εξουσιοδοτημένες IP από την είσοδο στο δίκτυο του σκάφους [65]. - Οι ομάδες ασφαλείας πρέπει να παρακολουθούν συνεχώς τα δίκτυα για μη φυσιολογική δραστηριότητα. χρησιμοποιώντας συστήματα ανίχνευσης εισβολών
Απομίμηση	- Η κρυπτογράφηση σε όλο το δίκτυο NMEA διασφαλίζει την κρυπτογράφηση των δεδομένων πριν από τη διαμετακόμιση και πιστοποιούνται κατά την παραλαβή. Ένα ασφαλές Serial-to-IP μετατροπέας που υποστηρίζει κρυπτογράφηση και πιστοποίηση μπορεί να χρησιμοποιηθεί. - Καθώς οι μετατροπείς Serial-to-IP διαθέτουν διεπαφή web για διαμόρφωση, η προεπιλεγμένη πρέπει να αλλάξουν το όνομα χρήστη και ο κωδικός πρόσβασης. - Το λογισμικό της συσκευής μετατροπής πρέπει να ενημερώνεται συνεχώς.

Ράδιο-ανίχνευση και εμβέλεια (RADAR)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Εισβολή κακόβουλου λογισμικού	-Το λογισμικό Antivirus πρέπει να εγκατασταθεί στον υπολογιστή του αρχηγού, ο οποίος χρησιμοποιείται για τη λήψη ενημερώσεων χαρτών ECDIS. Αυτό θα αποτρέψει το κακόβουλο λογισμικό από να εξαπλωθεί στο RADAR μέσω του μεταγωγέα ethernet που συνδέεται με το ECDIS. - Εκπαιδεύστε το πλήρωμα στην αναγνώριση των ηλεκτρονικών μηνυμάτων ηλεκτρονικού «ψαρέματος».

Άνθρωπος στη μέση (ΑΣΜ-MITM:Man-In-The-Middle) επίθεση	-Επιβάλλοντας την υπογραφή (υπογραφές ασφαλείας) στο υποκείμενο λειτουργικό σύστημα της υπηρεσίας SMB, η επίθεση MITM μπορεί να μετριαστεί. Υπογραφή SMB τοποθετεί μια ψηφιακή υπογραφή σε κάθε μπλοκ μηνυμάτων διακομιστή, η οποία χρησιμοποιείται από τόσο οι πελάτες όσο και οι διακομιστές SMB για την αποτροπή επιθέσεων «man-in- the-middle» και εγγυάται ότι οι επικοινωνίες SMB δεν αλλοιώνονται [66]. - Η υπογραφή SMB είναι διαθέσιμη στα Microsoft Windows

	Server 2003, Microsoft Windows XP, Microsoft Windows 2000, Windows NT 4.0 και Windows 98 [67].
Σύστημα αυτόματης αναγνώρισης (AIS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Απομίμηση	-Τα μηνύματα AIS πρέπει να πιστοποιούνται. - Για να γίνει διάκριση μεταξύ πραγματικών και πλαστών σημάτων, πρέπει να υπάρχει ένας τρόπος να προσδιορίζεται άμεσα η θέση της μετάδοσης. Για παράδειγμα, χρησιμοποιώντας μια εφαρμογή γραφείου RFeye, οι μεταδόσεις μπορούν να εντοπιστούν γεωγραφικά με βάση τον χρόνο Διαφοράς άφιξης (TDoA). - Το λογισμικό RFeye εξάγει τα αποτελέσματα γεωεντοπισμού ως PoA (Power on Arrival) και θερμικούς χάρτες πιθανότητας TDOA και επικαλύπτει σε πραγματικό χρόνο AoA (γωνία άφιξης) σε διεπαφές χαρτών [68].

Επίθεση επανάληψης (Άρνηση παροχής υπηρεσιών)	Οι χρονοσφραγίδες πρέπει να παρακολουθούνται σε όλα τα μηνύματα AIS για να αποτρέπουν τους χάκερς από το να αποστέλλουν εκ νέου καταγεγραμμένα μηνύματα μετά από ένα ορισμένο χρονικό διάστημα, μειώνοντας έτσι τις πιθανότητες του επιτιθέμενου να υποκλέψει το μήνυμα και να το ξαναστείλει [69].
Συχνότητα επίθεση άλματος	-Η ακεραιότητα και η αυθεντικότητα των μηνυμάτων AIS πρέπει να διασφαλίζονται. - Το σχήμα PKI μπορεί να υιοθετηθεί στο πρωτόκολλο AIS για επικοινωνίες RF. - X.509, ένα γνωστό πρότυπο PKI όπου τα ψηφιακά πιστοποιητικά εκδίδονται από επίσημες εθνικές ναυτιλιακές αρχές, οι οποίες ενεργούν ως αρχές πιστοποίησης και διαμορφώνονται επίσης σε αναμεταδότες με άλλα αναγνωριστικά σταθμών (MMSI και διακριτικό κλήσης). Το X.509 πιστοποιεί τα μηνύματα που ανταλλάσσονται μεταξύ πλοίων και με τις λιμενικές αρχές [70].

Παγκόσμιο σύστημα εντοπισμού θέσης (GPS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Απομίμηση Συσκευών Πλοήγησης	Ο δέκτης GPS/GNSS θα πρέπει να ανιχνεύει το πλαστό σήμα από ένα μείγμα αυθεντικών και παραποιημένων σημάτων με τη χρήση τεχνικών κατά της παραποίησης, όπως η απόλυτη ισχύς παρακολούθηση, χωρική επεξεργασία [71].
Παρεμπόδιση Συσκευών Πλοήγησης	Η χρήση τεχνικής κατά των παρεμβολών, όπως η παρακολούθηση του φάσματος, επιτρέπει το GPS παρεμβολείς να ανιχνεύονται και να εντοπίζονται από κινητά συστήματα εντοπισμού κατεύθυνσης. Οι ακούσιες παρεμβολές μπορούν στη συνέχεια να προειδοποιηθούν και οι κακόβουλοι επιτιθέμενοι μπορούν να διώκονται [72].

Δυναμικό σύστημα εντοπισμού θέσης (DPS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Άρνηση παροχής υπηρεσιών (DoS) επίθεση	-Επιτρέποντας και απορρίπτοντας συγκεκριμένες IP: Επιτρέποντας μόνο νόμιμες διευθύνσεις IP ή αποκλεισμός αυτών που προέρχονται από γνωστούς επιτιθέμενους. Εγκατάσταση τείχους προστασίας στο DPS θα επιτρέπει μόνο γνωστές διευθύνσεις IP [65]. - Οι ομάδες ασφαλείας θα πρέπει να παρακολουθούν συνεχώς τα δίκτυα για μη φυσιολογική δραστηριότητα χρησιμοποιώντας συστήματα ανίχνευσης εισβολής. - Το λογισμικό του συστήματος ελέγχου DP πρέπει να ενημερώνεται.
Απομίμηση	Ο δέκτης GPS/GNSS θα πρέπει να ανιχνεύει το πλαστό σήμα από ένα μείγμα αυθεντικών και παραποιημένων σημάτων με τεχνικές κατά της παραποίησης, όπως η απόλυτη ισχύς παρακολούθηση, χωρική επεξεργασία [71].
Επίθεση από πίσω πόρτα	-Ένα προηγμένο antivirus μπορεί να ανιχνεύσει και να αποτρέψει κακόβουλο λογισμικό και κακόβουλες επιθέσεις. Πολλές κερκόπορτες
	εγκαθίστανται μέσω κακόβουλου λογισμικού, επομένως είναι απαραίτητο να εγκαταστήσετε ένα εργαλείο προστασίας από ιούς ικανό να ανιχνεύει τέτοιες απειλές [73].
Παγκόσμιο σύστημα ναυτικού κινδύνου και ασφάλειας (GMDSS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού

Απομίμηση	- Τα μηνύματα που ανταλλάσσονται μεταξύ των πλοίων και με τις λιμενικές αρχές πρέπει να είναι αυθεντικοποιημένα. - Το σχήμα PKI μπορεί να υιοθετηθεί στο GMDSS για να διασφαλιστεί η αυθεντικότητα των μηνυμάτων. που ανταλλάσσονται. Η εφαρμογή ασφάλειας ηλεκτρονικού ταχυδρομείου, όπως το S/MIME ή το DKIM, μπορεί επίσης να είναι χρήσιμη εάν οι εμπιστευτικές πληροφορίες διαβιβάζονται μέσω ηλεκτρονικού ταχυδρομείου [74].
Υποκλοπές	Το λογισμικό και τα εργαλεία που χρησιμοποιούνται στο σύστημα GMDSS πρέπει να επικαιροποιούνται για να αποφεύγονται να παρέχονται στους επιτιθέμενους ευκαιρίες εκμετάλλευσης των ευπαθειών και να κατεβάσουν κακόβουλο λογισμικό στο σύστημα μέσω του οποίου μπορούν να κρυφακούσουν.
Άρνηση παροχής υπηρεσιών (DoS) επίθεση	Η χρήση τείχους προστασίας στο σύστημα GMDSS θα αποτρέψει την επίθεση DoS επιτρέποντας μόνο γνωστές διευθύνσεις IP [65].
Καταγραφέας δεδομένων ταξιδιού (VDR)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
	-Πριν τοποθετήσετε οποιοδήποτε εξωτερικό μέσο στο σύστημα VDR, σαρώστε το μέσο για ιούς/κακόβουλο λογισμικό χρησιμοποιώντας λογισμικό προστασίας από ιούς.
Επίθεση κακόβουλου λογισμικού (μέσω θυρών USB)	- Οι θύρες USB πρέπει να απενεργοποιούνται και να ενεργοποιούνται μόνο από τον καπετάνιο του πλοίου. όποτε υπάρχει ανάγκη χρήσης USB ή να ενεργοποιούνται μόνο κατά τη σύνδεση του διαχειριστή και απενεργοποιημένος σε άλλες

	συνδέσεις χρηστών -Χρησιμοποιήστε αποκλειστές θυρών για να αποφύγετε τα περιττά πρόσθετα. Πρέπει να γίνεται τακτική δημιουργία αντιγράφων ασφαλείας δεδομένων (δεδομένα που καταγράφονται στο VDR) και να αποθηκεύονται με ασφάλεια.
Απομακρυσμένο κώδικα εκτέλεση	Τα περισσότερα σκάφη χρησιμοποιούν παλαιότερη έκδοση VDR (Furuno VR-3000 και VR5000). Οι ενημερωμένες εκδόσεις μπορούν να βοηθήσουν στην αποτροπή απομακρυσμένης εκτέλεσης κώδικα [75].
Ολοκληρωμένο σύστημα πλοήγησης (INS)	
Άνθρωπος στη μέση (ΑΣΜ-MITM:Man-In-The-Middle) επίθεση	Εξυπηρετητής πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (υπηρεσία τερματικού) που εκτελείται στην υποκείμενη λειτουργικό σύστημα (Windows) του INS είναι ευάλωτη σε μια man-in- the-middle λόγω του χαμηλού επιπέδου κρυπτογράφησης που χρησιμοποιείται. Η ευπάθεια μπορεί να χρησιμοποιηθεί από έναν απομακρυσμένο εισβολέα για να αποκτήσει πρόσβαση στο INS. Αυτή η επίθεση MITM μπορεί να αποτραπεί με την επιβολή ισχυρής κρυπτογραφίας.
Απομακρυσμένος κωδικός εκτέλεση	-Ενημερώστε το λειτουργικό σύστημα με μια ενημερωμένη έκδοση ασφαλείας που κυκλοφόρησε από το κατασκευαστή για την αποτροπή αυτής της επίθεσης. - Το SMB 3.1.1 - η τελευταία έκδοση του SMB των Windows - κυκλοφόρησε μαζί με server 2016 και τα Windows 10. Το SMB 3.1.1 περιλαμβάνει βελτιώσειςασφαλείας όπως η επιβολή ασφαλών συνδέσεων με νεότερους (SMB2 και μεταγενέστερους) πελάτες και ισχυρότερα πρωτόκολλα κρυπτογράφησης.

2.1.2 Μέτρα μετριασμού για τα συστήματα διαχείρησης φορτίου

Πίνακας 6. Μετριασμός σε συστήματα φορτίου. [65-75]

Αίθουσα ελέγχου φορτίου (CCR)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Ransomware (ηλεκτρονικό ψάρεμα μέσω ηλεκτρονικής αλληλογραφίας)	-Το λογισμικό Antivirus πρέπει να εγκατασταθεί στο σύστημα υπολογιστή ελέγχου φορτίου για να να προστατεύει το σύστημα από μηνύματα ηλεκτρονικού ταχυδρομείου που είναι φορτωμένα με ιούς. - Πρέπει να δημιουργούνται τακτικά αντίγραφα ασφαλείας των δεδομένων και να αποθηκεύονται με ασφάλεια. - Εκπαίδευση του πληρώματος για την αναγνώριση των ηλεκτρονικών μηνυμάτων ηλεκτρονικού «ψαρέματος». Το πλήρωμα δεν πρέπει να κάνει κλικ σε συνδέσμους από άγνωστες πηγές ή να αποκαλύπτει προσωπικά στοιχεία ή ευαίσθητα επιχειρησιακά στοιχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου.
Απομίμηση Επίθεση κακόβουλου λογισμικού (μέσω θυρών USB)	-Το λογισμικό Antivirus πρέπει να είναι εγκατεστημένο στο σύστημα του υπολογιστή για να σαρώνει κάθε μονάδες USB που συνδέονται στο σύστημα. - Οι θύρες USB πρέπει να είναι απενεργοποιημένες και να ενεργοποιούνται μόνο από τον καπετάνιο του πλοίου. όποτε υπάρχει ανάγκη χρήσης USB ή να ενεργοποιείται μόνο κατά τη σύνδεση του διαχειριστή και απενεργοποιημένη σε άλλες συνδέσεις χρηστών. Χρησιμοποιήστε αποκλειστές θυρών για να αποφύγετε τα περιττά πρόσθετα.
Σύστημα νερού έρματος (BWS)	
Κίνδυνοι στον κυβερνοχώρο	Μέτρα Περιορισμού
Απομίμηση επίθεση κακόβουλου λογισμικού (μέσω θυρών USB)	-Είναι ζωτικής σημασίας κάθε εξωτερικό μέσο να σαρώνεται για κακόβουλο λογισμικό σε μια αυτόνομο σύστημα πριν συνδεθεί σε οποιοδήποτε δίκτυο του πλοίου. Το λογισμικό προστασίας από ιούς βοηθά στη σάρωση οποιουδήποτε εξωτερικού μέσου για κακόβουλο λογισμικό πριν συνδεθούν στο σύστημα. -Οι θύρες USB πρέπει να είναι απενεργοποιημένες και να ενεργοποιούνται μόνο από τον καπετάνιο του πλοίου. όποτε υπάρχει ανάγκη χρήσης USB ή να ενεργοποιείται μόνο κατά τη

	σύνδεση του διαχειριστή και απενεργοποιημένη σε άλλες συνδέσεις χρηστών. -Χρησιμοποιήστε αποκλειστές θυρών για να αποφύγετε τα περιττά plugins.
Ηλεκτρονικά μηνύματα ηλεκτρονικό ψάρεμα	-Το λογισμικό Antivirus πρέπει να εγκατασταθεί στο σύστημα για την προστασία του συστήματος. από μηνύματα ηλεκτρονικού ταχυδρομείου ηλεκτρονικό ψάρεμα. - Πρέπει να δημιουργούνται τακτικά αντίγραφα ασφαλείας των δεδομένων και να αποθηκεύονται με ασφάλεια. - Εκπαίδευση του πληρώματος για τον εντοπισμό των ηλεκτρονικών μηνυμάτων ηλεκτρονικό ψάρεμα. - Το πλήρωμα δεν πρέπει να κάνει κλικ σε συνδέσμους από άγνωστες πηγές ή να αποκαλύπτει προσωπικά ή ευαίσθητα επιχειρησιακά στοιχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου.

2.2 Χαρακτηριστικά του «NIST CSF»

2.2.1 Ιστορικό: NIST CSF στο ναυτιλιακό πλαίσιο

Το CSF του NIST, το οποίο παρουσιάστηκε για πρώτη φορά το 2014 και ενημερώθηκε στην έκδοση 1.1 το 2018, χρησιμεύει ως κρίσιμος οδηγός για τους οργανισμούς για την ενίσχυση των μέτρων κυβερνοασφάλειας. Το εν λόγω πλαίσιο, βασισμένο σε μια συλλογική προσπάθεια με τη συμβολή της βιομηχανίας και της κυβέρνησης, προσφέρει ένα σύνολο προσαρμόσιμων προτύπων, κατευθυντήριων γραμμών και βέλτιστων πρακτικών που οργανώνονται σε πέντε βασικές λειτουργίες: Αναγνώρlση, προστασία, Ανίχνευση, Ανταπόκρlση καl Ανάκτηση. Οι λειτουργίες αυτές παρέχουν μια στρατηγική προσέγγιση για τη διαχείριση κινδύνων στον κυβερνοχώρο, επιτρέποντας την προσαρμογή στις μοναδικές ανάγκες των διαφόρων τομέων. Η ευελιξία του πλαισίου διευκολύνει την προσαρμογή για την κάλυψη διαφορετικών οργανωτικών αναγκών, ενισχύοντας τις δυνατότητές τους να προλαμβάνουν, να ανιχνεύουν και να ανταποκρίνονται στις απειλές στον κυβερνοχώρο. Ειδικότερα, την Ακτοφυλακή των Ηνωμένων Πολιτειών (USCG) έχει αναγνωρίσει την αξία του CSF, υποστηρίζοντας τη χρήση του εντός της ναυτιλιακής βιομηχανίας για την πλοήγηση σε κινδύνους σε βασικές επιχειρήσεις όπως η Marine time Bulk Liquids Transfer (MBLT), υπεράκτιες επιχειρήσεις και επιχειρήσεις επιβατηγών πλοίων.

Το NIST CSF v2.0, το οποίο θα κυκλοφορήσει το 2023, σηματοδοτεί μια σημαντική εξέλιξη στην προσέγγιση της διαχείρισης των κινδύνων κυβερνοασφάλειας σε διάφορους τομείς, συμπεριλαμβανομένης της ναυτιλιακής βιομηχανίας- αυτό το επικαιροποιημένο πλαίσιο επεκτείνεται πέρα από τις κρίσιμες υποδομές, προσφέροντας ένα καθολικό σύνολο κατευθυντήριων γραμμών που θα βοηθήσει οργανισμούς όλων των τύπων να μετριάσουν τους κινδύνους κυβερνοασφάλειας. Το CSF 2.0 εισάγει μια έκτη βασική λειτουργία, τη «διακυβέρνηση», παράλληλα με τις πέντε αρχικές (αναγνώριση, προστασία, ανίχνευση, αντίδραση και ανάκτηση). Η προσθήκη αυτή υπογραμμίζει τη σημασία της ενσωμάτωσης των πρακτικών κυβερνοασφάλειας με τη συνολική οργανωτική διακυβέρνηση, ώστε να διασφαλιστεί ότι η διαχείριση των κινδύνων στον κυβερνοχώρο ευθυγραμμίζεται με τους ευρύτερους επιχειρηματικούς στόχους. Η λειτουργία «Διοίκηση», υπάρχει ως μία ξεχωριστή κατηγορία, αναδεικνύοντας τον ουσιαστικό της ρόλο στη στρατηγική εποπτεία, όπως φαίνεται στην εικόνα 6.
Επιπλέον, το CSF 2.0 προσφέρει βελτιωμένους πόρους, συμπεριλαμβανομένων οδηγών γρήγορης εκκίνησης, προφίλ για καθοδήγηση συγκεκριμένων στόχων και ενημερωτικές αναφορές ή αντιστοιχίσεις για την πλοήγηση στους εκτεταμένους πόρους του NIST για την ασφάλεια στον κυβερνοχώρο. Αυτά τα εργαλεία είναι ανεκτίμητα για τους οργανισμούς, ιδίως στον τομέα της ναυτιλίας, καθώς μπορούν να βοηθήσουν στην πλοήγηση στις πολυπλοκότητες της διαχείρισης των απειλών στον κυβερνοχώρο. Με την υιοθέτηση του CSF 2.0, οι οντότητες μπορούν να εντοπίζουν καλύτερα τους πιθανούς κινδύνους, να ιεραρχούν τις δράσεις και να επικοινωνούν αποτελεσματικά τις ανησυχίες για την ασφάλεια στον κυβερνοχώρο, ενισχύοντας έτσι την άμυνά τους απέναντι στο εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο. [76]

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Εικόνα 6. Παράθεση των ονομάτων των βασικών λειτουργιών και κατηγοριών του CSF 2.0 και τα μοναδικά αλφαβητικά αναγνωριστικά. [76]

Οι βέλτιστες πρακτικές για την εφαρμογή της διαχείρισης κινδύνων στον κυβερνοχώρο, όπως εκτιμάται από το προσωρινές κατευθυντήριες γραμμές του IMO, είναι σημαντικές όταν συνδυάζονται με το NIST CSF [77]. Οι βέλτιστες πρακτικές τοποθετούν την ασφάλεια στον κυβερνοχώρο ως προτεραιότητα, μαζί με άλλους κινδύνους για την ασφάλεια, στο πλαίσιο του Διεθνή κώδικα διαχείρισης της ασφάλειας (ISM) [78]. Με την ενσωμάτωση των αρχών του το NIST CSF και την ενσωμάτωσή τους στις ειδικές για τον κλάδο κατευθυντήριες γραμμές του IMO, οι ναυτιλιακές και λιμενικές επιχειρήσεις έχουν τη δυνατότητα να σχεδιάζουν ισχυρές στρατηγικές κυβερνοασφάλειας που αντιμετωπίζουν τόσο τις γενικές όσο και τις ειδικές για τον κλάδο απειλές. Η έγκριση του το NIST CSF από τον IMO επικυρώνει περαιτέρω την αποτελεσματικότητα και την καταλληλόλητα του για τον ναυτιλιακό τομέα. Σε απάντηση στον αυξανόμενο κίνδυνο περιστατικών στον κυβερνοχώρο στη ναυτιλιακή βιομηχανία, ο International Association of Classification Societies (IACS) ενέκρινε δύο νέες ενοποιημένες απαιτήσεις, UR E26 και UR E27, για την ενίσχυση της ανθεκτικότητας των πλοίων στον κυβερνοχώρο [79]. Αυτές οι απαιτήσεις, οι οποίες ισχύουν για τα νέα πλοία που συνάπτονται από την 1η Ιανουαρίου 2024, επικεντρώνονται στην ενσωμάτωση μέτρων κυβερνοασφάλειας σε όλες τις φάσεις σχεδιασμού, κατασκευής και λειτουργίας ενός πλοίου. Το UR E26 ασχολείται με την ασφαλή ενσωμάτωση των επιχειρησιακών και πληροφοριακών τεχνολογιών, δίνοντας έμφαση στη συλλογική ανθεκτικότητα ενός πλοίου στον κυβερνοχώρο.

2.2.2 Ανάλυση του CSF 2.0

Θα ακολουθήσει μία λεπτομερής ανάλυση των βασικών λειτουργιών και κατηγοριών του CSF 2.0 και τα μοναδικά αλφαβητικά αναγνωριστικά του. [80]

ΔΙΑΚΥΒΕΡΝΗΣΗ (GV): Η στρατηγική, οι προσδοκίες και η πολιτική διαχείρισης κινδύνων κυβερνοασφάλειας του οργανισμού καθορίζονται, κοινοποιούνται και παρακολουθούνται –

• Οργανωτικό πλαίσιο (GV.OC): Οι συνθήκες - αποστολή, προσδοκίες των ενδιαφερομένων μερών, εξαρτήσεις και νομικές, κανονιστικές και συμβατικές απαιτήσεις - που περιβάλλουν τις αποφάσεις του οργανισμού για τη διαχείριση κινδύνων κυβερνοασφάλειας είναι κατανοητές.

-GV.OC-01: Η αποστολή του οργανισμού είναι κατανοητή και επηρεάζει τη διαχείριση κινδύνων κυβερνοασφάλειας
-GV.OC-02: Οι εσωτερικοί και εξωτερικοί ενδιαφερόμενοι φορείς είναι κατανοητοί και οι ανάγκες και οι προσδοκίες τους όσον αφορά τη διαχείριση κινδύνων κυβερνοασφάλειας είναι κατανοητές και λαμβάνονται υπόψη
-GV.OC-03: Οι νομικές, κανονιστικές και συμβατικές απαιτήσεις σχετικά με την ασφάλεια στον κυβερνοχώρο - συμπεριλαμβανομένων των υποχρεώσεων προστασίας της ιδιωτικής ζωής και των πολιτικών ελευθεριών - είναι κατανοητές και διαχειρίζονται
-GV.OC-04: Οι κρίσιμοι στόχοι, ικανότητες και υπηρεσίες από τις οποίες εξαρτώνται ή τις οποίες αναμένουν οι εξωτερικοί ενδιαφερόμενοι από τον οργανισμό είναι κατανοητοί και γνωστοποιούνται
-GV.OC-05: Τα αποτελέσματα, οι δυνατότητες και οι υπηρεσίες από τις οποίες εξαρτάται ο οργανισμός είναι κατανοητά και κοινοποιούνται

• Στρατηγική διαχείριση κινδύνων (GV.RM): Οι προτεραιότητες του οργανισμού, οι περιορισμοί, οι δηλώσεις ανοχής και διάθεσης ανάληψης κινδύνου και οι παραδοχές καθορίζονται, κοινοποιούνται και χρησιμοποιούνται για την υποστήριξη των αποφάσεων σχετικά με τους λειτουργικούς κινδύνους

-GV.RM-01: Οι στόχοι διαχείρισης κινδύνων καθορίζονται και συμφωνούνται από τα ενδιαφερόμενα μέρη του οργανισμού
-GV.RM-02: Καθορίζονται, κοινοποιούνται και διατηρούνται οι δηλώσεις διάθεσης και ανοχής κινδύνου
-GV.RM-03: Οι δραστηριότητες και τα αποτελέσματα της διαχείρισης κινδύνων κυβερνοασφάλειας περιλαμβάνονται στις διαδικασίες διαχείρισης επιχειρηματικών κινδύνων
-GV.RM-04: Καθορίζεται και κοινοποιείται η στρατηγική κατεύθυνση που περιγράφει τις κατάλληλες επιλογές αντιμετώπισης κινδύνων
-GV.RM-05: Δημιουργούνται γραμμές επικοινωνίας σε ολόκληρο τον οργανισμό για τους κινδύνους κυβερνοασφάλειας, συμπεριλαμβανομένων των κινδύνων από προμηθευτές και άλλα τρίτα μέρη
-GV.RM-06: Καθιερώνεται και κοινοποιείται τυποποιημένη μέθοδος για τον υπολογισμό, την τεκμηρίωση, την κατηγοριοποίηση και την ιεράρχηση των κινδύνων κυβερνοασφάλειας
-GV.RM-07: Οι στρατηγικές ευκαιρίες (δηλαδή οι θετικοί κίνδυνοι) χαρακτηρίζονται και περιλαμβάνονται στις οργανωτικές συζητήσεις για τους κινδύνους κυβερνοασφάλειας

- Ρόλοι, αρμοδιότητες και εξουσίες (GV.RR): Καθορίζονται και κοινοποιούνται οι ρόλοι, οι ευθύνες και οι εξουσίες της κυβερνοασφάλειας για την προώθηση της λογοδοσίας, της αξιολόγησης των επιδόσεων και της συνεχούς βελτίωσης

-GV.RR-01: Η ηγεσία του οργανισμού είναι υπεύθυνη και υπόλογη για τους κινδύνους κυβερνοασφάλειας και προάγει μια κουλτούρα που έχει επίγνωση των κινδύνων, ηθική και συνεχή βελτίωση
-GV.RR-02: Οι ρόλοι, οι ευθύνες και οι εξουσίες που σχετίζονται με τη διαχείριση των κινδύνων κυβερνοασφάλειας καθορίζονται, κοινοποιούνται, κατανοούνται και επιβάλλονται
-GV.RR-03: Διατίθενται επαρκείς πόροι ανάλογοι με τη στρατηγική, τους ρόλους, τις ευθύνες και τις πολιτικές διαχείρισης κινδύνων στον κυβερνοχώρο
-GV.RR-04: Η ασφάλεια στον κυβερνοχώρο περιλαμβάνεται στις πρακτικές ανθρώπινου δυναμικού

- Πολιτική (GV.PO): Η οργανωτική πολιτική κυβερνοασφάλειας καθιερώνεται, κοινοποιείται και επιβάλλεται.

-GV.PO-01: Η πολιτική για τη διαχείριση των κινδύνων κυβερνοασφάλειας θεσπίζεται με βάση το οργανωτικό πλαίσιο, τη στρατηγική κυβερνοασφάλειας και τις προτεραιότητες, κοινοποιείται και επιβάλλεται
-GV.PO-02: Η πολιτική για τη διαχείριση των κινδύνων κυβερνοασφάλειας επανεξετάζεται, επικαιροποιείται, κοινοποιείται και επιβάλλεται ώστε να αντικατοπτρίζει τις αλλαγές στις απαιτήσεις, τις απειλές, την τεχνολογία και την οργανωτική αποστολή.

- Εποπτεία (GV.OV): Τα αποτελέσματα των δραστηριοτήτων και των επιδόσεων διαχείρισης κινδύνων κυβερνοασφάλειας σε επίπεδο οργανισμού χρησιμοποιούνται για την ενημέρωση, τη βελτίωση και την προσαρμογή της στρατηγικής διαχείρισης κινδύνων

-GV.OV-01: Τα αποτελέσματα της στρατηγικής διαχείρισης κινδύνων κυβερνοασφάλειας επανεξετάζονται για την ενημέρωση και την προσαρμογή της στρατηγικής και της κατεύθυνσης
-GV.OV-02: Η στρατηγική διαχείρισης κινδύνων κυβερνοασφάλειας επανεξετάζεται και προσαρμόζεται ώστε να διασφαλίζεται η κάλυψη των οργανωτικών απαιτήσεων και κινδύνων
-GV.OV-03: Οι επιδόσεις της οργανωτικής διαχείρισης κινδύνων κυβερνοασφάλειας αξιολογούνται και επανεξετάζονται για τις αναγκαίες προσαρμογές

- Διαχείριση κινδύνων στην αλυσίδα εφοδιασμού στον κυβερνοχώρο (GV.SC): Οι διαδικασίες διαχείρισης κινδύνων της αλυσίδας εφοδιασμού στον κυβερνοχώρο προσδιορίζονται, θεσπίζονται, διαχειρίζονται, παρακολουθούνται και βελτιώνονται από τους οργανωτικούς φορείς

-GV.SC-01: Καθιερώνεται και συμφωνείται από τα οργανωτικά ενδιαφερόμενα μέρη ένα πρόγραμμα, μια στρατηγική, στόχοι, πολιτικές και διαδικασίες διαχείρισης κινδύνων της αλυσίδας εφοδιασμού κυβερνοασφάλειας
-GV.SC-02: Οι ρόλοι και οι ευθύνες για την ασφάλεια στον κυβερνοχώρο για τους προμηθευτές, τους πελάτες και τους εταίρους καθορίζονται, κοινοποιούνται και συντονίζονται εσωτερικά και εξωτερικά
-GV.SC-03: Η διαχείριση των κινδύνων της αλυσίδας εφοδιασμού στον κυβερνοχώρο ενσωματώνεται στις διαδικασίες διαχείρισης, αξιολόγησης και βελτίωσης των κινδύνων στον κυβερνοχώρο και στην επιχείρηση
-GV.SC-04: Οι προμηθευτές είναι γνωστοί και ιεραρχημένοι κατά κρισιμότητα
-GV.SC-05: Οι απαιτήσεις για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας στις αλυσίδες εφοδιασμού καθορίζονται, ιεραρχούνται και ενσωματώνονται στις συμβάσεις και σε άλλους τύπους συμφωνιών με προμηθευτές και άλλα σχετικά τρίτα μέρη
-GV.SC-06: Πραγματοποιείται σχεδιασμός και δέουσα επιμέλεια για τη μείωση των κινδύνων πριν από τη σύναψη επίσημων σχέσεων με προμηθευτές ή άλλα τρίτα μέρη
-GV.SC-07: Οι κίνδυνοι που δημιουργούνται από έναν προμηθευτή, τα προϊόντα και τις υπηρεσίες του και άλλα τρίτα μέρη κατανοούνται, καταγράφονται, ιεραρχούνται, αξιολογούνται, αντιμετωπίζονται και παρακολουθούνται κατά τη διάρκεια της σχέσης
-GV.SC-08: Οι σχετικοί προμηθευτές και άλλα τρίτα μέρη συμπεριλαμβάνονται στο σχεδιασμό, την αντιμετώπιση και τις δραστηριότητες αποκατάστασης περιστατικών
-GV.SC-09: Οι πρακτικές ασφάλειας της εφοδιαστικής αλυσίδας ενσωματώνονται στα προγράμματα κυβερνοασφάλειας και διαχείρισης επιχειρησιακών κινδύνων και η απόδοσή τους παρακολουθείται καθ' όλη τη διάρκεια του κύκλου ζωής των τεχνολογικών προϊόντων και υπηρεσιών
-GV.SC-10: Τα σχέδια διαχείρισης κινδύνων της εφοδιαστικής αλυσίδας κυβερνοασφάλειας περιλαμβάνουν διατάξεις για δραστηριότητες που λαμβάνουν χώρα μετά τη σύναψη συμφωνίας συνεργασίας ή παροχής υπηρεσιών

ΤΑΥΤΟΠΟΙΗΣΗ (ID): Κατανοούνται οι τρέχοντες κίνδυνοι κυβερνοασφάλειας του οργανισμού

• Διαχείριση περιουσιακών στοιχείων (ID.AM): Τα περιουσιακά στοιχεία (π.χ. δεδομένα, υλικό, λογισμικό, συστήματα, εγκαταστάσεις, υπηρεσίες, άνθρωποι) που επιτρέπουν στον οργανισμό να επιτύχει τους επιχειρηματικούς σκοπούς προσδιορίζονται και διαχειρίζονται σύμφωνα με τη σχετική σημασία τους για τους οργανωτικούς στόχους και τη στρατηγική κινδύνου του οργανισμού
-ID.AM-01: Διατηρούνται απογραφές του υλικού που διαχειρίζεται ο οργανισμός
-ID.AM-02: Διατηρούνται απογραφές του λογισμικού, των υπηρεσιών και των συστημάτων που διαχειρίζεται ο οργανισμός
-ID.AM-03: Διατηρούνται αναπαραστάσεις της εξουσιοδοτημένης δικτυακής επικοινωνίας του οργανισμού και των ροών δεδομένων εσωτερικού και εξωτερικού δικτύου
-ID.AM-04: Διατηρούνται απογραφές των υπηρεσιών που παρέχονται από προμηθευτές
-ID.AM-05: Τα περιουσιακά στοιχεία ιεραρχούνται με βάση την ταξινόμηση, την κρισιμότητα, τους πόρους και τον αντίκτυπο στην αποστολή
-ID.AM-07: Διατηρούνται απογραφές δεδομένων και αντίστοιχων μεταδεδομένων για καθορισμένους τύπους δεδομένων
-ID.AM-08: Διαχείριση συστημάτων, υλικού, λογισμικού, υπηρεσιών και δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους

• ΑξΙΟλόγηση κΙΝδύνου (ID.RA): Ο κίνδυνος κυβερνοασφάλειας για τον οργανισμό, τα περιουσιακά στοιχεία και τα άτομα είναι κατανοητός από τον οργανισμό
-ID.RA-01: Εντοπίζονται, επικυρώνονται και καταγράφονται τα τρωτά σημεία των περιουσιακών στοιχείων
-ID.RA-02: Οι πληροφορίες για τις απειλές στον κυβερνοχώρο λαμβάνονται από φόρουμ και πηγές ανταλλαγής πληροφοριών
-ID.RA-03: Εντοπίζονται και καταγράφονται οι εσωτερικές και εξωτερικές απειλές για τον οργανισμό
-ID.RA-04: Εντοπίζονται και καταγράφονται οι δυνητικές επιπτώσεις και πιθανότητες απειλών που εκμεταλλεύονται ευπάθειες
-ID.RA-05: Οι απειλές, τα τρωτά σημεία, οι πιθανότητες και οι επιπτώσεις χρησιμοποιούνται για την κατανόηση του εγγενούς κινδύνου και την ενημέρωση για την ιεράρχηση των προτεραιοτήτων αντιμετώπισης του κινδύνου
-ID.RA-06: Επιλέγονται, ιεραρχούνται, σχεδιάζονται, παρακολουθούνται και κοινοποιούνται οι απαντήσεις σε κινδύνους
-ID.RA-07: Οι αλλαγές και οι εξαιρέσεις διαχειρίζονται, αξιολογούνται ως προς τις επιπτώσεις σε κινδύνους, καταγράφονται και παρακολουθούνται
-ID.RA-08: Θεσπίζονται διαδικασίες για τη λήψη, ανάλυση και ανταπόκριση σε γνωστοποιήσεις ευπαθειών
-ID.RA-09: Η αυθεντικότητα και η ακεραιότητα του υλικού και του λογισμικού αξιολογούνται πριν από την απόκτηση και τη χρήση
-ID.RA-10: Οι κρίσιμοι προμηθευτές αξιολογούνται πριν από την απόκτηση

• Βελτίωση (ID.IM): Εντοπίζονται βελτιώσεις στις οργανωτικές διεργασίες, διαδικασίες και δραστηριότητες διαχείρισης κινδύνων κυβερνοασφάλειας σε όλες τις λειτουργίες του CSF.
-ID.IM-01: Οι βελτιώσεις εντοπίζονται από αξιολογήσεις
-ID.IM-02: Οι βελτιώσεις εντοπίζονται από δοκιμές και ασκήσεις ασφάλειας, συμπεριλαμβανομένων εκείνων που γίνονται σε συντονισμό με προμηθευτές και σχετικά τρίτα μέρη
-ID.IM-03: Βελτιώσεις εντοπίζονται από την εκτέλεση επιχειρησιακών διεργασιών, διαδικασιών και δραστηριοτήτων
-ID.IM-04: Καταρτίζονται, κοινοποιούνται, διατηρούνται και βελτιώνονται τα σχέδια αντιμετώπισης περιστατικών και άλλα σχέδια ασφάλειας στον κυβερνοχώρο που επηρεάζουν τις λειτουργίες.

ΠΡΟΣΤΑΣΙΑ (PR): Χρησιμοποιούνται διασφαλίσεις για τη διαχείριση των κινδύνων κυβερνοασφάλειας του οργανισμού

• Διαχείριση ταυτότητας, πιστοποίηση ταυτότητας και έλεγχος πρόσβασης (PR.AA): Η πρόσβαση στα φυσικά και λογικά περιουσιακά στοιχεία περιορίζεται σε εξουσιοδοτημένους χρήστες, υπηρεσίες και υλικό και διαχειρίζεται ανάλογα με τον εκτιμώμενο κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
-PR.AA-01: Οι ταυτότητες και τα διαπιστευτήρια για εξουσιοδοτημένους χρήστες, υπηρεσίες και υλικό διαχειρίζονται από τον οργανισμό
-PR.AA-02: Οι ταυτότητες αποδεικνύονται και συνδέονται με διαπιστευτήρια με βάση το πλαίσιο των αλληλεπιδράσεων

-PR.AA-03: Οι χρήστες, οι υπηρεσίες και το υλικό πιστοποιούνται
-PR.AA-04: Οι ισχυρισμοί ταυτότητας προστατεύονται, μεταφέρονται και επαληθεύονται.
-PR.AA-05: Τα δικαιώματα πρόσβασης, τα δικαιώματα και οι εξουσιοδοτήσεις ορίζονται σε μια πολιτική, διαχειρίζονται, επιβάλλονται και αναθεωρούνται και ενσωματώνουν τις αρχές των λιγότερων προνομίων και του διαχωρισμού των καθηκόντων
-PR.AA-06: Η φυσική πρόσβαση σε περιουσιακά στοιχεία διαχειρίζεται, παρακολουθείται και επιβάλλεται ανάλογα με τον κίνδυνο.

• Ενημέρωση καΙ κατάρτΙση (PR.AT): Το προσωπικό του οργανισμού είναι ενημερωμένο και εκπαιδευμένο σε θέματα κυβερνοασφάλειας, ώστε να μπορεί να εκτελεί τα καθήκοντά του που σχετίζονται με την κυβερνοασφάλεια

-PR.AT-01: Παρέχεται στο προσωπικό ευαισθητοποίηση και κατάρτιση ώστε να διαθέτει τις γνώσεις και τις δεξιότητες για την εκτέλεση γενικών καθηκόντων με γνώμονα τους κινδύνους κυβερνοασφάλειας
-PR.AT-02: Παρέχεται στα άτομα σε εξειδικευμένους ρόλους ευαισθητοποίηση και κατάρτιση ώστε να διαθέτουν τις γνώσεις και τις δεξιότητες για την εκτέλεση σχετικών καθηκόντων με γνώμονα τους κινδύνους κυβερνοασφάλειας

• ΑσφάλεΙα δεδομένων (PR.DS): Η διαχείριση των δεδομένων γίνεται σύμφωνα με τη στρατηγική κινδύνου του οργανισμού για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών
-PR.DS-01: Προστατεύονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων σε κατάσταση ηρεμίας
-PR.DS-02: Προστατεύονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων σε διακίνηση
-PR.DS-10: Προστατεύονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων σε χρήση
-PR.DS-11: Δημιουργούνται, προστατεύονται, διατηρούνται και ελέγχονται αντίγραφα ασφαλείας των δεδομένων

• ΑσφάλεΙα πλατφόρμας (PR.PS): Το υλικό, το λογισμικό (π.χ. υλικό λογισμικό, λειτουργικά συστήματα, εφαρμογές) και οι υπηρεσίες των φυσικών και εικονικών πλατφορμών διαχειρίζονται σύμφωνα με τη στρατηγική κινδύνου του οργανισμού για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους
-PR.PS-01: Καθιερώνονται και εφαρμόζονται πρακτικές διαχείρισης διαμόρφωσης
-PR.PS-02: Το λογισμικό συντηρείται, αντικαθίσταται και αφαιρείται ανάλογα με τον κίνδυνο
-PR.PS-03: Το υλικό συντηρείται, αντικαθίσταται και αφαιρείται ανάλογα με τον κίνδυνο
-PR.PS-04: Δημιουργούνται και διατίθενται αρχεία καταγραφής για συνεχή παρακολούθηση
-PR.PS-05: Αποτρέπεται η εγκατάσταση και η εκτέλεση μη εξουσιοδοτημένου λογισμικού
-PR.PS-06: Ενσωματώνονται ασφαλείς πρακτικές ανάπτυξης λογισμικού και η απόδοσή τους παρακολουθείται καθ' όλη τη διάρκεια του κύκλου ζωής της ανάπτυξης λογισμικού.

• ΑνθεκτΙκότητα τεχνολογΙκών υποδομών (PR.IR): Η διαχείριση των αρχιτεκτονικών ασφάλειας γίνεται με τη στρατηγική κινδύνου του οργανισμού για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των περιουσιακών στοιχείων και της οργανωτικής ανθεκτικότητας

-PR.IR-01: Τα δίκτυα και τα περιβάλλοντα προστατεύονται από μη εξουσιοδοτημένη λογική πρόσβαση και χρήση
-PR.IR-02: Τα τεχνολογικά περιουσιακά στοιχεία του οργανισμού προστατεύονται από περιβαλλοντικές απειλές
-PR.IR-03: Εφαρμόζονται μηχανισμοί για την επίτευξη των απαιτήσεων ανθεκτικότητας σε κανονικές και δυσμενείς καταστάσεις
-PR.IR-04: Διατηρείται επαρκής χωρητικότητα πόρων για τη διασφάλιση της διαθεσιμότητας
ΑΝΙΧΝΕΥΣΗ (DE): Εντοπίζονται και αναλύονται πιθανές επιθέσεις και παραβιάσεις της ασφάλειας στον κυβερνοχώρο.

- Συνεχής παρακολούθηση (DE.CM): Τα περιουσιακά στοιχεία παρακολουθούνται

για την ανεύρεση ανωμαλιών, δεικτών παραβίασης και άλλων δυνητικά δυσμενών συμβάντων
-DE.CM-01: Δίκτυα και δικτυακές υπηρεσίες παρακολουθούνται για την ανεύρεση δυνητικά δυσμενών συμβάντων
-DE.CM-02: Το φυσικό περιβάλλον παρακολουθείται για την ανεύρεση δυνητικά δυσμενών συμβάντων
-DE.CM-03: Η δραστηριότητα του προσωπικού και η χρήση της τεχνολογίας παρακολουθούνται για την ανεύρεση δυνητικά δυσμενών συμβάντων
-DE.CM-06: Οι δραστηριότητες και οι υπηρεσίες εξωτερικών παρόχων υπηρεσιών παρακολουθούνται για την ανεύρεση δυνητικά δυσμενών συμβάντων
-DE.CM-09: Παρακολουθείται το υπολογιστικό υλικό και λογισμικό, τα περιβάλλοντα εκτέλεσης και τα δεδομένα τους για την ανεύρεση δυνητικά δυσμενών συμβάντων.

- Ανάλυση ανεπΙθύμητων συμβάντων (DE.AE): ανάλυση ανωμαλιών, δεικτών παραβίασης και άλλων δυνητικά ανεπιθύμητων συμβάντων για τον χαρακτηρισμό συμβάντων και τον εντοπισμό συμβάντων κυβερνοασφάλειας

-DE.AE-02: Ανάλυση δυνητικά ανεπιθύμητων συμβάντων για την καλύτερη κατανόηση των σχετικών δραστηριοτήτων
-DE.AE-03: Οι πληροφορίες συσχετίζονται από πολλαπλές πηγές
-DE. AE-04: Ο εκτιμώμενος αντίκτυπος και η έκταση των ανεπιθύμητων συμβάντων είναι κατανοητά
-DE.AE-06: Οι πληροφορίες σχετικά με τα ανεπιθύμητα συμβάντα παρέχονται σε εξουσιοδοτημένο προσωπικό και εργαλεία
-DE.AE-07: Οι πληροφορίες σχετικά με τις απειλές στον κυβερνοχώρο και άλλες πληροφορίες σχετικά με το πλαίσιο ενσωματώνονται στην ανάλυση
-DE.AE-08: Τα συμβάντα δηλώνονται όταν τα ανεπιθύμητα συμβάντα πληρούν τα καθορισμένα κριτήρια

ΑΠΑΝΤΗΣΗ (RS): Αναλαμβάνονται ενέργειες σχετικά με ένα εντοπισμένο περιστατικό κυβερνοασφάλειας

• Διαχείριση περιστατικών (RS.MA): Διαχείριση των αντιδράσεων σε εντοπισμένα περιστατικά κυβερνοασφάλειας

-RS.MA-01: Το σχέδιο αντιμετώπισης περιστατικών εκτελείται σε συντονισμό με τα σχετικά τρίτα μέρη μόλις δηλωθεί ένα περιστατικό
-RS.MA-02: Οι αναφορές περιστατικών ταξινομούνται και επικυρώνονται
-RS.MA-03: Τα περιστατικά κατηγοριοποιούνται και ιεραρχούνται
-RS.MA-04: Τα περιστατικά κλιμακώνονται ή αναβαθμίζονται ανάλογα με τις ανάγκες ο
-RS.MA-05: Εφαρμόζονται τα κριτήρια για την έναρξη αποκατάστασης περιστατικών

• Ανάλυση συμβάντων (RS.AN): Διεξάγονται έρευνες για να διασφαλιστεί η αποτελεσματική ανταπόκριση και να υποστηριχθούν οι δραστηριότητες εγκληματολογίας και ανάκτησης.

-RS.AN-03: Ανάλυση διενεργείται για να διαπιστωθεί τι έλαβε χώρα κατά τη διάρκεια ενός συμβάντος και η βασική αιτία του συμβάντος
-RS.AN-06: Καταγράφονται οι ενέργειες που εκτελούνται κατά τη διάρκεια μιας έρευνας και διατηρείται η ακεραιότητα και η προέλευση των αρχείων
-RS.AN-07: Συλλέγονται τα δεδομένα του συμβάντος και διατηρείται η ακεραιότητα και η προέλευσή τους
-RS.AN-08: Το μέγεθος ενός συμβάντος εκτιμάται και επικυρώνεται.

• Αναφορά και επικοινωνία για την αντιμετώπιση περιστατικών (RS.CO): Οι δραστηριότητες απόκρισης συντονίζονται με τους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς, όπως απαιτείται από νόμους, κανονισμούς ή πολιτικές.

-RS.CO-02: Οι εσωτερικοί και εξωτερικοί ενδιαφερόμενοι φορείς ενημερώνονται για τα περιστατικά
-RS.CO-03: Οι πληροφορίες κοινοποιούνται σε καθορισμένους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς

• Μετριασμός περιστατικών (RS.MI): Πραγματοποιούνται δραστηριότητες για την πρόληψη της επέκτασης ενός συμβάντος και τον μετριασμό των επιπτώσεών του
-RS.MI-01: Τα συμβάντα περιορίζονται
-RS.MI-02: Τα συμβάντα εξαλείφονται

ΑΝΑΚΤΗΣΗ (RC): Αποκαθίστανται τα περιουσιακά στοιχεία και οι λειτουργίες που επηρεάζονται από ένα περιστατικό κυβερνοασφάλειας.

• Εκτέλεση σχεδίου αποκατάστασης περιστατικών (RC.RP): Εκτελούνται δραστηριότητες αποκατάστασης για να εξασφαλιστεί η λειτουργική διαθεσιμότητα των συστημάτων και υπηρεσιών που επηρεάζονται από περιστατικά κυβερνοασφάλειας.

-RP-01: Το τμήμα αποκατάστασης του σχεδίου αντιμετώπισης συμβάντος εκτελείται μόλις ξεκινήσει από τη διαδικασία αντιμετώπισης συμβάντος
-RC.RP-02: Οι δράσεις αποκατάστασης επιλέγονται, προσδιορίζονται, ιεραρχούνται και εκτελούνται.
-RP-03: Η ακεραιότητα των αντιγράφων ασφαλείας και άλλων μέσων αποκατάστασης επαληθεύεται πριν από τη χρήση τους για την αποκατάσταση
-RC.RP-04: Οι κρίσιμες λειτουργίες της αποστολής και η διαχείριση κινδύνων κυβερνοασφάλειας λαμβάνονται υπόψη για τη θέσπιση επιχειρησιακών κανόνων μετά το συμβάν
-RC.RP-05: Επαληθεύεται η ακεραιότητα των αποκαταστημένων περιουσιακών στοιχείων, αποκαθίστανται τα συστήματα και οι υπηρεσίες και επιβεβαιώνεται η κανονική κατάσταση λειτουργίας
-RC.RP-06: Κηρύσσεται το τέλος της αποκατάστασης του συμβάντος βάσει κριτηρίων και ολοκληρώνεται η σχετική με το συμβάν τεκμηρίωση

• Επικοινωνία αποκατάστασης περιστατικού (RC.CO): Δραστηριότητες αποκατάστασης συντονίζονται με εσωτερικά και εξωτερικά μέρη .
-RC.CO-03: Οι δραστηριότητες αποκατάστασης και η πρόοδος στην αποκατάσταση των επιχειρησιακών δυνατοτήτων κοινοποιούνται στους καθορισμένους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς
-RC.CO-04: Ενημέρωση του κοινού για την αποκατάσταση του συμβάντος με τη χρήση εγκεκριμένων μεθόδων και μηνυμάτων.

2.2.3 Σε ποιον εφαρμόζεται το CSF NIST;

Ορισμένοι οργανισμοί με έδρα τις ΗΠΑ υποχρεούνται να συμμορφώνονται με το CSF NIST. Ωστόσο, για τους περισσότερους οργανισμούς, η συμμόρφωση είναι προαιρετική. Πολλοί επιλέγουν να συμμορφωθούν για να διαβεβαιώσουν τους εαυτούς τους και τους πελάτες **τους** ότι τα συστήματα, το δίκτυο και τα δεδομένα τους είναι όσο το δυνατόν πιο ασφαλή από ένα περιστατικό κυβερνοασφάλειας.

Επιπλέον, η συμμόρφωση με το NIST CSF μπορεί να διευκολύνει τη συμμόρφωση με άλλα πλαίσια ασφάλειας, όπως το πρότυπο ασφάλειας δεδομένων της βιομηχανίας καρτών πληρωμών (PCI DSS) και ο νόμος Sarbanes-Oxley (SOX). Το NIST CSF διέπει επίσης τη συμμόρφωση με το Federal Information Processing Standard Publication 200 (FIPS 200), το οποίο είναι υποχρεωτικό για τις οντότητες που συνδέονται με την κυβέρνηση. Η οδηγία NIST CSF είναι ευέλικτη και μπορεί να προσαρμοστεί ώστε να ανταποκρίνεται στις μοναδικές ανάγκες και απαιτήσεις κάθε συγκεκριμένης περιοχής ή κλάδου.
Το CSF NIST χρησιμοποιεί επίσης μια σειρά από βαθμίδες για την αξιολόγηση της τρέχουσας διαχείρισης κινδύνων, του περιβάλλοντος απειλών και των προτύπων συμμόρφωσης μιας εταιρείας. Οι πληροφορίες αυτές χρησιμοποιούνται για να διαπιστωθεί

πού βρίσκεται η επιχείρηση όσον αφορά τη στάση της στον τομέα της κυβερνοασφάλειας.[81]
Το σύστημα βαθμίδων έχεI ως εξής:
Βαθμίδα 1 – Μερική: Αυτό είναι το σημείο εκκίνησης για τις περισσότερες επιχειρήσεις όπου η διαχείριση κινδύνων δεν εφαρμόζεται σωστά και η ασφάλεια στον κυβερνοχώρο δεν είναι τυποποιημένη.
Βαθμίδα 2 – Ενημερωμένη: ως προς τον κίνδυνο Εδώ υπάρχει ένα επίπεδο διαχείρισης κινδύνου, ωστόσο τα πρωτόκολλα αυτά δεν είναι τυποποιημένα σε ολόκληρη την εταιρεία.
Βαθμίδα 3 – Επαναλαμβανόμενο: Σε αυτό το σημείο, υπάρχει μια επίσημη και οργανωμένη στρατηγική κυβερνοασφάλειας με εκλεπτυσμένες πολιτικές και πρωτόκολλα.
Βαθμίδα 4 – Προσαρμοστικό: Στην τελευταία βαθμίδα, η εταιρεία επιδεικνύει εκτεταμένη ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας και εφαρμόζει διεξοδικές στρατηγικές

διαχείρισης κινδύνων που ενημερώνονται από πληροφορίες σχετικά με τις απειλές. Ενώ ο NIST συνιστά στις εταιρείες που βρίσκονται στο Tier 1 να προχωρήσουν στο Tier 2, ο οργανισμός σημείωσε επίσης ότι κάθε επίπεδο δεν μπορεί να συγκριθεί με το επίπεδο ωριμότητας. Οι εταιρείες θα πρέπει να ανεβαίνουν στον κατάλογο των βαθμίδων μόνο όταν μπορούν να το αντέξουν οικονομικά και αυτό μειώνει αποτελεσματικά συγκεκριμένους κινδύνους κυβερνοασφάλειας. Οι παραπάνω βαθμίδες μπορούν στη συνέχεια να χρησιμοποιηθούν για τη δημιουργία του προφίλ σας στο πλαίσιο NIST CyberSecurity Framework. Το προφίλ του πλαισίου είναι ένας οδικός χάρτης του πού βρίσκεται η επιχείρησή σας και πού θέλει να βρεθεί στο μέλλον. Θα αναφερθούμε τώρα σε περισσότερες λεπτομέρειες σχετικά με αυτό και σε παραδείγματα προφίλ του πλαισίου NIST για την κυβερνοασφάλεια για να εργαστείτε προς τα πάνω.

Παραδείγματα προφίλ πλαIσίου κυβερνοασφάλεIας NIST [82]
Ένα προφίλ πλαισίου σας επιτρέπει να αποκτήσετε μια σαφή εικόνα της τρέχουσας κατάστασης της εταιρείας σας στον κυβερνοχώρο σε σχέση με τη διαχείριση κινδύνων, τις επιχειρηματικές απαιτήσεις και τους χρησιμοποιούμενους πόρους. Το προφίλ του πλαισίου CSF θα δώσει στην επιχείρησή σας ένα τρέχον προφίλ και ένα προφίλ-στόχο που θα περιγράφουν αντίστοιχα λεπτομερώς τα στοιχεία της τρέχουσας κατάστασης κυβερνοασφάλειας και τα επιθυμητά στοιχεία. Η σύγκριση του τρέχοντος προφίλ και του προφίλ-στόχου θα δώσει στην επιχείρησή σας ένα σχέδιο βελτίωσης που μπορεί να αναληφθεί σε δράση. Το προφίλ του πλαισίου της επιχείρησής σας θα προσφέρει κατευθυντήριες γραμμές που θα ευθυγραμμίζονται με τους οργανωτικούς και κλαδικούς στόχους, θα λαμβάνουν υπόψη τις νομικές ή κανονιστικές απαιτήσεις και τις βέλτιστες πρακτικές του κλάδου και θα αντικατοπτρίζουν τις προτεραιότητες της διαχείρισης κινδύνων.

Παρακάτω παρατίθενται τα σημαντικά παραδείγματα προφίλ του NIST CyberSecurity :
-NIST IR 8183 - Προφίλ κατασκευής του πλαισίου κυβερνοασφάλειας
-NIST IR 8183r1 - Πλαίσιο ασφάλειας στον κυβερνοχώρο Έκδοση 1.1 Προφίλ κατασκευής Αναθ. 1
-NIST IR 8310 (Draft) - Προφίλ εκλογικής υποδομής πλαισίου κυβερνοασφάλειας
-NIST IR 8323 Revision 1 - Foundational PNT Profile: Εφαρμογή του πλαισίου κυβερνοασφάλειας για την υπεύθυνη χρήση υπηρεσιών PNT
-NIST IR 8374 - Διαχείριση κινδύνων από Ransomware: Προφίλ πλαισίου κυβερνοασφάλειας
-NIST IR 8406 - Προφίλ πλαισίου κυβερνοασφάλειας για το υγροποιημένο φυσικό αέριο
-NIST IR 8441 (σχέδιο) - Προφίλ πλαισίου κυβερνοασφάλειας για υβριδικά δορυφορικά δίκτυα (HSN)
-NIST IR 8467 (Draft) - Προφίλ πλαισίου κυβερνοασφάλειας για γονιδιωματικά δεδομένα
-NIST IR 8473 - CyberSecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure (Προφίλ πλαισίου κυβερνοασφάλειας για υποδομές ακραίας ταχείας φόρτισης

ηλεκτρικών οχημάτων)

-NIST TN 2051 - Προφίλ πλαισίου κυβερνοασφάλειας έξυπνου δικτύου
-Πώς να χρησιμοποιήσετε το προφίλ του πλαισίου κυβερνοασφάλειας για περιβάλλοντα συνδεδεμένων οχημάτων - U.S. Transportation
-Προφίλ πλαισίου κυβερνοασφάλειας Excel για περιβάλλοντα συνδεδεμένων οχημάτων - Μεταφορές των ΗΠΑ
-Προφίλ πλαισίου κυβερνοασφάλειας για τη ναυτιλία - Ακτοφυλακή των ΗΠΑ
-Προφίλ πλαισίου κυβερνοασφάλειας για τη θαλάσσια μεταφορά χύδην υγρών - Ακτοφυλακή των ΗΠΑ, προφίλ υπεράκτιων δραστηριοτήτων, προφίλ επιβατηγών πλοίων
-Προφίλ πλαισίου κυβερνοασφάλειας για τον τομέα των επικοινωνιών (ραδιοτηλεοπτικό, καλωδιακό, δορυφορικό, ασύρματο και ενσύρματο τμήμα) - Federal Communications Commission's The Communications Security, Reliability, and Interoperability Council (CSRIC) IV.

2.3 Επιθέσεις και Στατιστικά

Παρακάτω θα δούμε κάποιες μεγάλες κυβερνοεπιθέσεις που έχουν συμβεί στο παρελθόν , αληθινές περιπτώσεις οι οποίες έκρουσαν τον κώδωνα του κινδύνου στον κόσμο της ναυτιλίας και έδωσαν το έναυσμα στους διεθνείς ναυτιλιακούς οργανισμούς και στους νομοθέτες να σχεδιάσουν και στη συνέχεια να υιοθετήσουν νομοθετήματα και γενικούς κανονισμούς που αφορούν στην προστασία όσων εμπλέκονται σε μια κυβερνοεπίθεση.

2.3.1 Λιμάνι της Αμβέρσας – Port of Antwerp

Το λιμάνι της Αμβέρσας υπήρξε στόχος κυβερνοεπίθεσης, η οποία ξεκίνησε το 2011 και διήρκεσε πάνω από δύο χρόνια. Η επίθεση εκμεταλλεύτηκε το σύστημα ηλεκτρονικής απελευθέρωσης εμπορευματοκιβωτίων, γνωστό ως ERS, που είχε εισαχθεί στο λιμάνι το 2005. Το ERS λειτουργούσε με την αποστολή μοναδικών ηλεκτρονικών κωδικών, αντί φορτωτικών εγγράφων, στους παραλήπτες, στους πράκτορες, καθώς και στον τερματικό σταθμό μέσω email, οι οποίοι ήταν απαραίτητοι για την παραλαβή των εμπορευματοκιβωτίων. Το 2011, μια ομάδα εισβολέων παραβίασε το σύστημα αυτό και απέκτησε πρόσβαση σε δεδομένα που παρείχαν πληροφορίες για τη θέση και την ασφάλεια των εμπορευματοκιβωτίων στο λιμάνι. Αυτό τους επέτρεψε να κρύβουν παράνομα ναρκωτικά και όπλα μεταξύ των νόμιμων φορτίων και να τα διακινούν στη χώρα. Οι αρχές αποκάλυψαν την απάτη και τη διαρροή δεδομένων όταν οι δράστες, που δρούσαν ανενόχλητοι για μεγάλο διάστημα, υπερεκτίμησαν τη δυνατότητά τους και άρχισαν να αφαιρούν ολόκληρα εμπορευματοκιβώτια από τον σταθμό. Χρησιμοποίησαν κυβερνο- επίθεση τύπου Advanced Persistent Threat (APT). Η προηγμένη μόνιμη απειλή (APT) είναι ένας ευρύς όρος που χρησιμοποιείται για να περιγράψει μια εκστρατεία επίθεσης κατά την οποία ένας εισβολέας ή μια ομάδα εισβολέων εγκαθιστά μια παράνομη, μακροχρόνια παρουσία σε ένα δίκτυο με σκοπό την εξόρυξη εξαιρετικά ευαίσθητων δεδομένων. Παρόμοιες επιθέσεις σημειώθηκαν το 2018 στα λιμάνια της Βαρκελώνης και του Σαν Ντιέγκο. Αυτή η υπόθεση ανέδειξε τα ανεπαρκή μέτρα κυβερνοασφάλειας στο λιμάνι, υπογραμμίζοντας ότι η παραβίαση στόχευε στη διάπραξη ποινικών εγκλημάτων και καταδεικνύοντας την ανάγκη για άμεσα μέτρα προστασίας του κυβερνοχώρου [83].

2.3.2 Maersk

Το πιο γνωστό περιστατικό κυβερνοεπίθεσης στη ναυτιλία σημειώθηκε στις 27 Ιουνίου 2017, όταν η δανέζικη εταιρία Mærsk «χτυπήθηκε» από το κακόβουλο λογισμικό NOTPetya (Κακόβουλο λογισμικό το οποίο εμποδίζει την πρόσβαση των ανθρώπων στα προσωπικά τους δεδομένα, μέχρι να καταβληθούν λύτρα $300 σε κρυπτονόμισμα (bITcoin). Η επίθεση θεωρήθηκε ότι προκλήθηκε έμμεσα στο πλαίσιο μιας ευρείας κυβερνοεπίθεσης και έδειξε ότι ακόμη και σε τέτοιες περιπτώσεις, οι συνέπειες μπορεί να είναι τεράστιες. Συγκεκριμένα, η επίθεση έπληξε τις λειτουργίες της Mærsk σε παγκόσμιο επίπεδο, επηρεάζοντας και 17 τερματικά της σε διάφορα λιμάνια, δύο εκ των οποίων βρίσκονται στο Ρότερνταμ. Αυτά τα τερματικά υπολειτουργούσαν, και ορισμένα φορτία δεν έφτασαν στους σωστούς προορισμούς λόγω των προβλημάτων στο πληροφοριακό σύστημα της εταιρίας. Με δεδομένο ότι τα πλοία της Mærsk μεταφέρουν περίπου το 20% των παγκόσμιων εμπορευματοκιβωτίων, το περιστατικό έδειξε πόσο δύσκολο είναι για μια τόσο μεγάλη εταιρία να ανταποκριθεί όταν το IT της έχει παραβιαστεί. Για την πλήρη αποκατάσταση της λειτουργίας της, η Mærsk εγκατέστησε 4.000 νέους servers, 45.000 νέους υπολογιστές και
2.500 εφαρμογές, ολοκληρώνοντας τη διαδικασία μέσα σε 10 ημέρες, ενώ υπό φυσιολογικές συνθήκες θα απαιτούνταν περίπου 6 μήνες.
Ο πρόεδρος της A.P. Møller – Mærsk, Jim Hagemann Snabe, μίλησε στο Παγκόσμιο Οικονομικό Φόρουμ του 2017 για τα ζητήματα κυβερνοασφάλειας που προέκυψαν από αυτή την εμπειρία. Σύμφωνα με τον ίδιο:

1. Η επίθεση απέδειξε ότι όλες οι εταιρίες, ανεξαρτήτως μεγέθους, έχουν ελλείψεις στην κυβερνοασφάλεια. Η ασφάλεια στον κυβερνοχώρο πρέπει να αποτελεί προτεραιότητα και να δίνει ανταγωνιστικό πλεονέκτημα.
2. Από την αρχή της επίθεσης, η Mærsk δημοσίευσε ανοιχτά το περιστατικό στο TwITter και ενημέρωνε τακτικά για τα βήματα αποκατάστασης, με στόχο άλλες εταιρίες να αντλήσουν γνώσεις από αυτό. Ο κ. Snabe τόνισε ότι η εταιρία προσπάθησε να αναδείξει το μέγεθος του προβλήματος, καθώς η πρόληψη είναι πιο σημαντική από την αντίδραση σε τέτοιες επιθέσεις. Η επίθεση στη Mærsk έδειξε την ανάγκη προσαρμογής των εταιριών στα νέα δεδομένα, καθώς, όπως ανέφερε και ο William P. Doyle, «Αφού η Mærsk έπεσε θύμα κυβερνοεπίθεσης, κάτι ανάλογο μπορεί να συμβεί σε οποιονδήποτε». Η δημοσιοποίηση των λεπτομερειών της επίθεσης θεωρήθηκε σημαντική για την αλλαγή νοοτροπίας στον τομέα της κυβερνοασφάλειας. Σήμερα, οι εταιρίες δίνουν ιδιαίτερη προσοχή στο ζήτημα αυτό, ειδικά λόγω της ισχύος του κανονισμού MSC.428(98) από τον IMO, που από την 1η Ιανουαρίου 2021 απαιτεί από τα πλοία που εμπίπτουν στον ISM να έχουν μέτρα πρόληψης για την κυβερνοασφάλεια [84].
Σύμφωνα με τις κατηγορίες και υποκατηγορίες του CSF 2.0 κάποια προτεινόμενα μέτρα για αποφυγή μίας τέτοιας επίθεσης σε ρεαλιστικό σενάριο θα ήταν τα εξής:
- Εκπαίδευση και κατάρτιση των εργαζομένων σχετικά με τις απαιτήσεις της κυβερνοασφάλειας (ID.AE-001)
- Εφαρμογή μέτρων ασφάλειας δικτύου και πρόσβασης (AC.CI-002)
- Κατασκευή ενδιαφέρουσας αρχιτεκτονικής πληροφορικών συστημάτων (ID.AM- 003)
- Συνεχής παρακολούθηση και ανίχνευση κινδύνων (DS.RP-001)
- BW Group's

Λιγότερο από έναν μήνα μετά την κυβερνοεπίθεση που δέχτηκε η δανέζικη ναυτιλιακή εταιρία Maersk, μία ακόμη εταιρία, η BW Group, βρέθηκε στόχος επιτήδειων χάκερς. Συγκεκριμένα, οι υπολογιστές στα γραφεία της εταιρίας στη Σιγκαπούρη παραβιάστηκαν, με αποτέλεσμα να διακοπεί η επικοινωνία της εταιρίας με τον εξωτερικό κόσμο και να περιοριστεί σε ηλεκτρονικά μηνύματα προς τους πελάτες και τα πληρώματα των πλοίων. Εκπρόσωπος της εταιρίας ανέφερε ότι η επίθεση δεν προκλήθηκε από ransomware, αλλά δεν έγινε σαφές αν κατά την παραβίαση κλάπηκαν οικονομικά στοιχεία ή δεδομένα της BW. Μετά το περιστατικό, η εταιρία προχώρησε στη λήψη των απαραίτητων μέτρων για να αποτρέψει παρόμοιες επιθέσεις στο μέλλον και να καλύψει τις υπάρχουσες αδυναμίες στο σύστημα κυβερνοασφάλειάς της [85].

2.3.3 Clarkson PLC

Στις 29 Νοεμβρίου 2017, ο βρετανικός ναυλομεσιτικός οίκος Clarkson PLC ανακοίνωσε με επίσημο δελτίο τύπου ότι είχε σημειωθεί μη εξουσιοδοτημένη πρόσβαση στα υπολογιστικά συστήματα της εταιρίας στο Ηνωμένο Βασίλειο. Η παραβίαση οδήγησε στην κλοπή προσωπικών δεδομένων πελατών, όπως ημερομηνίες γέννησης, στοιχεία διαβατηρίων και τραπεζικοί λογαριασμοί, ενώ οι δράστες ζήτησαν λύτρα για να μην τα δημοσιοποιήσουν. Μετά από έρευνα, οι αρχές διαπίστωσαν ότι η επίθεση προήλθε από έναν συγκεκριμένο και απομονωμένο λογαριασμό χρήστη, ο οποίος απενεργοποιήθηκε στη συνέχεια. Αξιοσημείωτο είναι ότι η παραβίαση έγινε αντιληπτή στις 7 Νοεμβρίου 2017, παρόλο που διήρκησε έξι μήνες, από τις 31 Μαΐου έως τις 4 Νοεμβρίου του ίδιου έτους [86]. Μετά την επίθεση, η Clarkson PLC κατέβαλε κάθε προσπάθεια για να διαχειριστεί αποτελεσματικά το συμβάν, διασφαλίζοντας ότι οι λειτουργίες της συνέχιζαν απρόσκοπτα και ότι οι πελάτες της προστατεύονταν. Επίσης, έλαβε πρόσθετα μέτρα ασφαλείας για να αποτρέψει παρόμοια περιστατικά στο μέλλον και εξέτασε σε βάθος την επίθεση για να ενισχύσει την κυβερνοασφάλεια της.Το περιστατικό της Clarkson PLC τονίζει ότι οι κυβερνοεπιθέσεις και η κυβερνοασφάλεια δεν αφορούν μόνο τα πλοία, τα λιμάνια και τις ναυτιλιακές εταιρίες με στενή έννοια, αλλά επηρεάζουν ολόκληρο το ναυτιλιακό οικοσύστημα, όπως μεσίτες, ασφαλιστές, προμηθευτές και ναυλωτές. Αυτό υπογραμμίζει την ανάγκη για άμεση αντιμετώπιση των κυβερνο- απειλών και για ανάπτυξη προληπτικών μέτρων ασφαλείας, τα οποία είναι πιο επίκαιρα και απαραίτητα από ποτέ [87].

2.3.4 Cosco US

Στις 24 Ιουλίου 2018, οι κυβερνοεγκληματίες επέκτειναν τη λίστα των θυμάτων τους, προσθέτοντας σε αυτήν την Cosco Shipping Lines, καθώς οι λειτουργίες της εταιρίας στις Ηνωμένες Πολιτείες δέχθηκαν επίθεση. Με ανακοίνωση που δημοσιεύθηκε την επόμενη ημέρα στο Facebook, η Cosco ενημέρωσε τους πελάτες της ότι λόγω της κατάρρευσης του δικτύου, τα τηλεφωνικά συστήματα λειτουργούσαν με προβλήματα και η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου δεν διεξαγόταν ομαλά στην περιοχή που έλαβε χώρα η επίθεση. Για να περιορίσει τη ζημιά μόνο στις αμερικανικές της δραστηριότητες, η εταιρία αποσύνδεσε το αμερικανικό δίκτυο από τις υπόλοιπες περιοχές, προστατεύοντας έτσι τα υπόλοιπα συστήματά της από πιθανή επέκταση της επίθεσης, αποφεύγοντας έτσι μια γενικευμένη κατάρρευση.
Η επίθεση προκάλεσε επίσης κάποια προβλήματα στις λειτουργίες του τερματικού Pier J στο λιμάνι του Long Beach. Ωστόσο, η εταιρία διαβεβαίωσε ότι όλα τα πλοία της λειτουργούσαν κανονικά και δεν επηρεάστηκαν από την επίθεση. Η ταχεία ανάκαμψη της Cosco δείχνει ότι η εταιρία είχε προετοιμαστεί και είχε λάβει μέτρα πρόληψης, έχοντας μάθει από την κυβερνοεπίθεση στην Mærsk έναν χρόνο νωρίτερα. Χάρη στην ετοιμότητα αυτή, η Cosco μπόρεσε να επαναφέρει τις διαδικασίες της και να επανέλθει σχεδόν στην κανονική λειτουργία της μέσα σε μία εβδομάδα. Βοηθητικό ρόλο σε αυτήν την ταχεία αποκατάσταση έπαιξε και το γεγονός ότι η συγκεκριμένη επίθεση δεν ήταν τόσο σοβαρή και επιζήμια όσο εκείνη που είχε πλήξει την Mærsk [88].

Πίνακας 6. Κυβερνο-επιθέσεις στο χώρο της Ναυτιλίας το 2020. [29]

Ημερομηνία	Εταιρεία/Οργανισμός	Τοποθεσία	Τύπος Περιστατικού	Κακόβουλο Λογισμικό
Απρίλιος 2020	Mediterranean Shipping Company (MSC)	Γενεύη, Ελβετία	Κακόβουλο Λογισμικό	Άγνωστο
Απρίλιος 2020	DESMI	Δανία	Ransomware	Άγνωστο
Μάιος 2020	Τερματικός Σταθμός Shahid Rajaee	Ιράν	Μη Αναγνωρισμένος Χάκερ	Άγνωστο
Μάιος 2020	Toll	Αυστραλία	Ransomware	Nefilim
Μάιος 2020	Anglo-Eastern	Χονγκ Κονγκ	Ransomware	Άγνωστο
Ιούνιος 2020	Vard	Διεθνές	Ransomware	Άγνωστο
Αύγουστος 2020	Carnival Corporation	Διεθνές	Ransomware	Άγνωστο
Σεπτέμβριος 2020	CMA CGM SA	Ασία-Ειρηνικός	Ransomware	Ragnar Locker
Σεπτέμβριος 2020	Ρυμουλκό των ΗΠΑ	Λουιζιάνα, Ηνωμένες Πολιτείες	Email Ηλεκτρονικό ψάρεμα	Άγνωστο

Οκτώβριος 2020	Διεθνής Ναυτιλιακή Οργάνωση (IMO)	Διεθνές	Κακόβουλο Λογισμικό	Άγνωστο
Οκτώβριος 2020	Λιμενική Αρχή του Ιράν	Ιράν	Μη Αναγνωρισμένος Χάκερ	Άγνωστο
Οκτώβριος 2020	Red Funnel	Ηνωμένο Βασίλειο	Μη Αναγνωρισμένος Χάκερ	Άγνωστο
Νοέμβριος 2020	Λιμάνι του Kennewick	Ουάσινγκτον, Ηνωμένες Πολιτείες	Ransomware	Άγνωστο

2.4 Σύνοψη του 2ου Κεφαλαίου

Στην δεύτερη ενότητα της πτυχιακής μου παρουσιάζω την κυβερνοασφάλεια στη ναυτιλία, με ιδιαίτερη έμφαση στο πλαίσιο κυβερνοασφάλειας του NIST (NIST CSF) και τους τρόπους με τους οποίους αυτό μπορεί να βοηθήσει στον εντοπισμό, την προστασία και την αποκατάσταση από κυβερνοεπιθέσεις. Παρουσιάζονται αναλυτικά οι κινδύνοι που προκύπτουν από την ενσωμάτωση τεχνολογιών πληροφοριών (IT) και λειτουργικών τεχνολογιών (OT) στα πλοία, εξηγώντας πώς αυτές οι τεχνολογίες είναι ευάλωτες σε επιθέσεις. Με τα στοιχεία της ενότητας, συνειδητοποιούμε πως στο σημερινό παγκοσμιοποιημένο περιβάλλον της ναυτιλίας, η ενσωμάτωση των τεχνολογιών IT και OT αναμφίβολα προσφέρει τεράστια οφέλη, βελτιώνοντας την απόδοση, την αποτελεσματικότητα και την επικοινωνία. Ωστόσο, η σύγκλιση αυτών των τεχνολογιών αυξάνει και τον κίνδυνο των κυβερνοεπιθέσεων, με σοβαρές συνέπειες για την ασφάλεια των πλοίων και των ναυτικών λειτουργιών. Το NIST CSF προσφέρει ένα σαφές και δομημένο πλαίσιο για την αξιολόγηση και τον περιορισμό αυτών των κινδύνων, παρέχοντας στα ναυτιλιακά συστήματα τις κατάλληλες διαδικασίες για την ανίχνευση, προστασία, απόκριση και ανάκαμψη από πιθανές απειλές. Μέσα από τη σωστή εφαρμογή και την ευθυγράμμιση με τις οδηγίες του NIST, η ναυτιλία μπορεί να ενισχύσει την ανθεκτικότητά της, διασφαλίζοντας όχι μόνο την ασφάλεια των πληροφοριών αλλά και τη συνέχεια των επιχειρησιακών διαδικασιών και την προστασία των κρίσιμων λειτουργιών στη θάλασσα.

3. Κυβερνοασφάλεια NIST

Στο 3ο Κεφάλαιο θα αναλύσω την διαχείριση ρίσκου σε κάθε ενέργεια μίας ναυτιλιακής, τους ρόλους και τις αρμοδιότητες των οντοτήτων μίας εταιρίας, την εκπαίδευση που πρέπει να γίνει για την εκμάθηση των ρίσκων και των κινδύνων. Επίσης αναφέρω πως γίνεται ρεαλιστικά η αξιολόγηση, ο υπολογισμός των κινδύνων καθώς και η ρύθμιση των επιπέδων του όσον αφορά την κυβερνο-ασφάλεια. Επεκτείνοντας την έρευνα, εξηγώ το σχέδιο έκτακτης ανάγκης που καθορίζει η κάθε ναυτιλιακή ξεχωριστά για την ίδια, τις πολιτικές προστασίας, και τα «Policies» που ακολουθούν καθώς και τα συστήματα και τους πιθανούς στόχους μίας σύγχρονης ναυτιλιακής εταιρίας. Τα παραπάνω πλάνα έχουν αναπτυχθεί βάση των αναγνωρισμένων πλαισίων ασφάλειας και κυβερνοασφάλειας, το IMO Resolution MSC.428(98), τα Guidelines on Cyber Security onboard Ships, το BIMCO, το USCG Cyber Bulletins, το UK Cyber Security Code of Practice for ships και το EU Regulation 2016/679, τα οποία θα αναλύσω στο υποκεφάλαιο 3.3. Στην Τρίτη ενότητα θα παρουσιάσω στοιχεία από το Σχέδιο διαχείρισης της ασφάλειας στον κυβερνοχώρο μίας μεγάλης ναυτιλιακής εταιρίας. Το σχέδιο αυτό περιέχει εμπιστευτικές πληροφορίες συνεπώς η επωνυμία της εταιρίας δεν θα αποτελεί κομμάτι του κεφαλαίου και της πτυχιακής μου, ενώ δεν θα υπάρχουν αναφορές- πηγές για τις πληροφορίες που θα παραθέσω στα υποκεφάλαια 3.1 και 3.2.

3.1 Διαχείριση ρίσκου

3.1.1 Διαδικασία Ασφάλειας στον κυβερνοχώρο

Τα σχέδια και οι διαδικασίες της εταιρείας για τη διαχείριση των κινδύνων στον κυβερνοχώρο θα πρέπει να θεωρούνται συμπληρωματικά προς τις υφιστάμενες απαιτήσεις διαχείρισης κινδύνων ασφάλειας και προστασίας που περιέχονται στον Διεθνή Κώδικα Διαχείρισης Ασφάλειας (ISM) και στον Διεθνή Κώδικα Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ISPS). Η ασφάλεια στον κυβερνοχώρο θα πρέπει να εξετάζεται σε όλα τα επίπεδα της εταιρείας, από την ανώτερη διοίκηση στη στεριά έως το πλήρωμα επί του πλοίου, ως αναπόσπαστο μέρος της κουλτούρας ασφάλειας και προστασίας που είναι απαραίτητη για την ασφαλή και αποτελεσματική λειτουργία των πλοίων.

Υπάρχουν έξι βήματα που πρέπει να εξεταστούν προκειμένου να ενισχυθεί η ευαισθητοποίηση και να αναπτυχθεί ένα υψηλού επιπέδου σύστημα διαχείρισης της ασφάλειας στον κυβερνοχώρο στην εταιρεία (τόσο στις εγκαταστάσεις των γραφείων όσο και στον διαχειριζόμενο στόλο)

- Προσδιορισμός των απειλών

Προσδιορισμός και κατανόηση των εξωτερικών απειλών στον κυβερνοχώρο για το πλοίο και την Εταιρεία. Κατανοήστε την εσωτερική απειλή για την ασφάλεια στον κυβερνοχώρο που προέρχεται από την ακατάλληλη χρήση και την έλλειψη ευαισθητοποίησης.

- Προσδιορισμός των τρωτών σημείων

Ανάπτυξη καταλόγων των συστημάτων επί του πλοίου και του γραφείου με άμεσες και έμμεσες συνδέσεις επικοινωνίας. Κατανόηση των συνεπειών μιας απειλής για την ασφάλεια στον κυβερνοχώρο στα εν λόγω συστήματα. Κατανοήστε τις δυνατότητες και τους περιορισμούς των υφιστάμενων μέτρων προστασίας.

- Αξιολόγηση της έκθεσης σε κίνδυνο

Προσδιορίστε την πιθανότητα εκμετάλλευσης των ευπαθειών από εσωτερικές απειλές. Επιπλέον, προσδιορίστε την πιθανότητα έκθεσης των τρωτών σημείων από ακατάλληλη χρήση των συστημάτων και του εξοπλισμού. Προσδιορίστε τον αντίκτυπο στην ασφάλεια και την προστασία από την εκμετάλλευση κάθε μεμονωμένου ή συνδυασμού ευπαθειών

- Ανάπτυξη μέτρων προστασίας καl ανίχνευσης

Μειώστε την πιθανότητα εκμετάλλευσης ευπαθειών μέσω μέτρων προστασίας. Μείωση του δυνητικού αντίκτυπου της εκμετάλλευσης μιας ευπάθειας.

- Δημιουργία σχεδίων έκτακτης ανάγκης

Ανάπτυξη σχεδίου αντιμετώπισης για τη μείωση των επιπτώσεων των απειλών που πραγματοποιούνται στην ασφάλεια και την προστασία του πλοίου και της Εταιρείας.

- Αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο

Αντιμετωπίστε τις απειλές ασφάλειας στον κυβερνοχώρο που πραγματοποιούνται χρησιμοποιώντας το σχέδιο αντιμετώπισης. Αξιολογήστε τον αντίκτυπο της

αποτελεσματικότητας του σχεδίου απόκρισης και επαναξιολογήστε τις απειλές και τα τρωτά σημεία.

3.1.2 Ρόλοι και Αρμοδιότητες

Ανώτατη διοίκηση: Παρέχει τη διοικητική κατεύθυνση και υποστήριξη για την ασφάλεια των πληροφοριών και εγκρίνει επίσημα την πολιτική ασφάλειας των πληροφοριών της εταιρείας

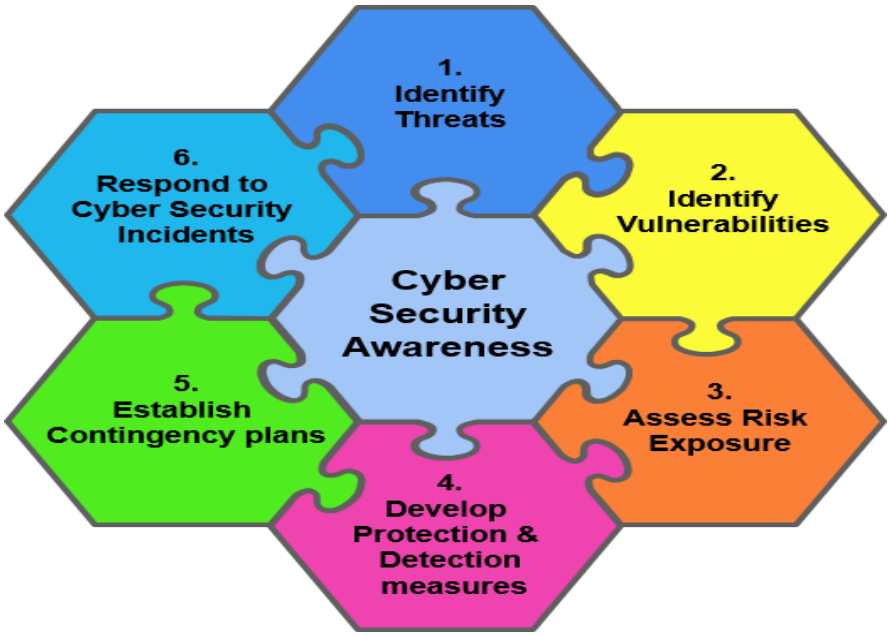
Διευθυντής ασφάλειας στον κυβερνοχώρο: Είναι υπεύθυνος για τη δημοσίευση, τη διανομή, τη συντήρηση και την αναθεώρηση της πολιτικής. Μπορεί επίσης να έχει τα καθήκοντα του Διευθυντή Τεχνολογίας Πληροφοριών.
Προϊστάμενος τμημάτων: Θα πρέπει να υποστηρίζουν ενεργά και να εφαρμόζουν την πολιτική ασφάλειας στον κυβερνοχώρο εντός των τμημάτων τους. Θα πρέπει επίσης να διασφαλίζουν ότι το προσωπικό είναι ενήμερο για τις αρμοδιότητές του καθώς και για τα θέματα ασφάλειας γενικά.
Διευθυντής τεχνολογίας πληροφοριών: Θα πρέπει να διασφαλίζει την ορθή εφαρμογή της πολιτικής ασφάλειας πληροφοριών και των υποστηρικτικών διαδικασιών.
Προσωπικό πληροφορικής: Θα πρέπει να είναι υπεύθυνο για την προστασία των περιουσιακών στοιχείων σύμφωνα με την πολιτική ασφάλειας πληροφοριών και τις υποστηρικτικές διαδικασίες.
Χρήστες: Θα πρέπει να ενεργούν σύμφωνα με την πολιτική ασφάλειας στον κυβερνοχώρο της εταιρείας και τις υποστηρικτικές διαδικασίες.
Χρήστες εντός του σκάφους: Θα πρέπει να ενεργούν σύμφωνα με την πολιτική ασφάλειας στον κυβερνοχώρο της εταιρείας και τις υποστηρικτικές διαδικασίες.
SSO (Υπεύθυνος Ασφάλειας Πλοίου): Εκτός από τις ευθύνες του για τη φυσική ασφάλεια (σύμφωνα με το σχέδιο ασφάλειας πλοίου), είναι επίσης υπεύθυνος για την εφαρμογή της πολιτικής και των διαδικασιών ασφάλειας στον κυβερνοχώρο της Εταιρείας επί του πλοίου.
CySO (Υπεύθυνος ασφάλειας στον κυβερνοχώρο): Ο CySO είναι υπεύθυνος για όλες τις πτυχές της ασφάλειας των συστημάτων που λειτουργούν στον κυβερνοχώρο του πλοίου, δηλαδή τόσο για τα συστήματα IT, όσο και για τα συστήματα OT και επικοινωνιών.

3.1.3 Εκπαίδευση

Όλοι οι εργαζόμενοι της Εταιρείας και, κατά περίπτωση, οι χρήστες τρίτων (όπως οι υπεργολάβοι), θα πρέπει να λαμβάνουν την κατάλληλη εκπαίδευση. Οι χρήστες θα πρέπει να είναι κατάλληλα εκπαιδευμένοι ώστε να υποστηρίζουν την Πολιτική Ασφάλειας στον Κυβερνοχώρο, καθώς και τις διαδικασίες ασφαλείας της Εταιρείας και τη σωστή χρήση των επιχειρησιακών και πληροφοριακών διαδικασιών και συστημάτων της. Θα πρέπει επίσης να λαμβάνουν εκπαίδευση σχετικά με τη χρήση των σωστών μέσων επεξεργασίας πληροφοριών, όπως οι διαδικασίες σύνδεσης και η πολιτική για τη χρήση πακέτων λογισμικού, πριν από την παροχή πρόσβασης σε πληροφορίες, συστήματα ή υπηρεσίες.

Οι εργαζόμενοι θα πρέπει να κατανοούν γιατί η ασφάλεια είναι σημαντική, ποιες είναι οι πολιτικές της εταιρείας και ποιες είναι οι δικές τους ευθύνες. Ο Διευθυντής Πληροφορικής είναι υπεύθυνος για την εκπαίδευση του προσωπικού του Γραφείου της Εταιρείας.

Ο CySO είναι υπεύθυνος για την εκπαίδευση του προσωπικού επί του πλοίου. Οι Marine/Technical Superintendents κατά τη διάρκεια των επισκέψεών τους στα πλοία θα πρέπει να παρέχουν πρόσθετη εκπαίδευση για τα στοιχεία ασφάλειας στον κυβερνοχώρο.



Εικόνα 7. Από τι συνίσταται η επίγνωση γύρω από την κυβερνοασφάλεια

3.1.4 Διαχειρίζοντας το ρίσκο

Η ναυτιλιακή βιομηχανία έχει μακρά ιστορία επιτυχίας στη διαχείριση κινδύνων. Οι ναυτικοί και οι λιμενεργάτες εντοπίζουν και αξιολογούν τους κινδύνους σε κάθε βάρδια και βάρδια. Οι φορείς εκμετάλλευσης πλοίων και εγκαταστάσεων θα πρέπει να εξετάζουν τον κυβερνοχώρο μαζί με τους φυσικούς, τον ανθρώπινο παράγοντα και άλλους κινδύνους που ήδη αντιμετωπίζουν.

Είναι σημαντικό να προστατεύονται τα κρίσιμα συστήματα και δεδομένα με πολλαπλά επίπεδα μέτρων προστασίας που λαμβάνουν υπόψη το ρόλο του προσωπικού, των διαδικασιών και της τεχνολογίας:
- να αυξηθεί η πιθανότητα εντοπισμού ενός περιστατικού στον κυβερνοχώρο
-να αυξηθεί η προσπάθεια και οι πόροι που απαιτούνται για την προστασία των πληροφοριών, των δεδομένων ή της διαθεσιμότητας των συστημάτων IT και OT.

Η προσέγγιση «άμυνα σε βάθος» ενθαρρύνει τον συνδυασμό των εξής:
- φυσική ασφάλεια του πλοίου σύμφωνα με το σχέδιο ασφάλειας πλοίου (ΣΑΠ)
- προστασία των δικτύων, συμπεριλαμβανομένης της αποτελεσματικής τμηματοποίησης
- ανίχνευση εισβολών
- λευκή λίστα λογισμικού
- έλεγχο πρόσβασης και χρηστών
- κατάλληλες διαδικασίες σχετικά με τη χρήση αφαιρούμενων μέσων και πολιτικές κωδικών πρόσβασης
- την ευαισθητοποίηση του προσωπικού σχετικά με τον κίνδυνο και την εξοικείωση με τις κατάλληλες διαδικασίες.

Οι εταιρικές πολιτικές και διαδικασίες που περιλαμβάνονται στο παρόν σχέδιο έχουν εκδοθεί για να διασφαλιστεί ότι η ασφάλεια στον κυβερνοχώρο λαμβάνεται υπόψη στο πλαίσιο της

συνολικής προσέγγισης για τη διαχείριση των κινδύνων ασφάλειας και προστασίας. Η πολυπλοκότητα και η δυνητική επιμονή των απειλών στον κυβερνοχώρο σημαίνει ότι λαμβάνεται επίσης υπόψη η προσέγγιση «άμυνα σε βάθος».
Ο εξοπλισμός και τα δεδομένα που προστατεύονται από επίπεδα μέτρων προστασίας είναι πιο ανθεκτικά στις επιθέσεις στον κυβερνοχώρο.

Στα πλοία, όπου τα επίπεδα ολοκλήρωσης μεταξύ των συστημάτων στον κυβερνοχώρο μπορεί να είναι υψηλά, η άμυνα σε βάθος λειτουργεί μόνο εάν τα τεχνικά και διαδικαστικά μέτρα προστασίας εφαρμόζονται σε στρώματα σε όλα τα ευάλωτα και ολοκληρωμένα συστήματα. Αυτή είναι η «άμυνα σε βάθος» και χρησιμοποιείται για να αποτρέψει την καταστρατήγηση των τρωτών σημείων ενός συστήματος για την παράκαμψη των μέτρων προστασίας ενός άλλου συστήματος.

3.1.5 Αξιολόγηση κινδύνων στον κυβερνοχώρο

Αξιολόγηση του κινδύνου: Η ασφάλεια στον κυβερνοχώρο θα πρέπει να ξεκινά από το ανώτερο διοικητικό επίπεδο μιας εταιρείας, αντί να ανατίθεται αμέσως στον υπεύθυνο ασφαλείας του πλοίου ή στον επικεφαλής του τμήματος πληροφορικής. Υπάρχουν διάφοροι λόγοι για αυτό συμβαίνουν τα παρακάτω.

1. Οι πρωτοβουλίες για την ενίσχυση της ασφάλειας στον κυβερνοχώρο μπορεί ταυτόχρονα να επηρεάσουν τις συνήθεις επιχειρηματικές διαδικασίες και λειτουργίες, καθιστώντας τες πιο χρονοβόρες ή δαπανηρές. Συνεπώς, αποτελεί στρατηγική ευθύνη των ανώτερων στελεχών να αξιολογούν και να αποφασίζουν σχετικά με τις αντισταθμίσεις μεταξύ κινδύνου και ανταμοιβής.

2. Ορισμένες πρωτοβουλίες που θα αυξήσουν την ασφάλεια στον κυβερνοχώρο σχετίζονται με τις επιχειρηματικές διαδικασίες και την εκπαίδευση του πληρώματος και όχι με τα συστήματα IT και, ως εκ τούτου, πρέπει να εδραιωθούν οργανωτικά εκτός του τμήματος IT.

3. Οι πρωτοβουλίες που αυξάνουν την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο ενδέχεται να αλλάξουν τον τρόπο με τον οποίο η εταιρεία αλληλεπιδρά με τους πελάτες, τους προμηθευτές και τις αρχές και να επιβάλουν νέες απαιτήσεις για τη συνεργασία μεταξύ των μερών. Η απόφαση για το αν και πώς θα προωθηθούν αλλαγές σε αυτές τις σχέσεις είναι απόφαση της ανώτερης διοίκησης.

4. Μόνο όταν αποφασιστούν οι τρεις παραπάνω πτυχές θα είναι δυνατόν να περιγραφούν με σαφήνεια οι απαιτήσεις IT της στρατηγικής ασφάλειας στον κυβερνοχώρο, και αυτό είναι το στοιχείο που μπορεί να ανατεθεί στο τμήμα IT.

5. Με βάση τις στρατηγικές αποφάσεις σε γενικές γραμμές και τις αντισταθμίσεις κινδύνου και ανταμοιβής, θα πρέπει να καταρτιστούν σχετικά σχέδια έκτακτης ανάγκης σε σχέση με τη διαχείριση περιστατικών στον κυβερνοχώρο, εάν αυτά συμβούν.

A. Οι έλεγχοι στον κυβερνοχώρο που έχουν ήδη εφαρμοστεί από την εταιρεία και επί των

πλοίων της.
Β. Πολλοί ενδιαφερόμενοι εμπλέκονται συχνά στη λειτουργία και τη ναύλωση ενός πλοίου με αποτέλεσμα ενδεχομένως να μην υπάρχει υπευθυνότητα για την υποδομή ΙΤ.
Γ. Το πλοίο που βρίσκεται σε απευθείας σύνδεση και ο τρόπος με τον οποίο διασυνδέεται με άλλα τμήματα της παγκόσμιας αλυσίδας εφοδιασμού.
Δ. Επιχειρησιακά κρίσιμες και εμπορικά ευαίσθητες πληροφορίες που μοιράζονται με παρόχους υπηρεσιών στην ξηρά.
Ε. Η διαθεσιμότητα και η χρήση ελεγχόμενων από υπολογιστή κρίσιμων συστημάτων για την ασφάλεια του πλοίου και την προστασία του περιβάλλοντος.
Τα στοιχεία αυτά θα πρέπει να λαμβάνονται υπόψη και τα σχετικά μέρη τους να ενσωματώνονται στις πολιτικές ασφαλείας της εταιρείας, στα συστήματα διαχείρισης της ασφάλειας και στα σχέδια ασφαλείας του πλοίου. Πρέπει να τηρούνται όλες οι σχετικές εθνικές νομοθεσίες και οι κανονισμοί του κράτους σημαίας, ενώ σε ορισμένες περιπτώσεις μπορεί να χρειαστεί να χρησιμοποιηθούν εναλλακτικές μέθοδοι μείωσης του κινδύνου.

- ΠροσδΙΟρΙσμός της τρωτότητας

Θα πρέπει να γίνει αξιολόγηση των πιθανών απειλών που μπορεί ρεαλιστικά να αντιμετωπιστούν αρχικά. Θα πρέπει να ακολουθήσει αξιολόγηση των συστημάτων και των διαδικασιών επί του πλοίου και στις εγκαταστάσεις γραφείων, προκειμένου να χαρτογραφηθεί η ευρωστία τους για την αντιμετώπιση του τρέχοντος επιπέδου απειλής. Αυτές οι εκτιμήσεις τρωτότητας θα πρέπει στη συνέχεια να αποτελέσουν τη βάση για μια συζήτηση/εργαστήριο σε επίπεδο ανώτερων στελεχών. Μπορεί να διευκολυνθεί από εσωτερικούς εμπειρογνώμονες ή να υποστηριχθεί από εξωτερικούς εμπειρογνώμονες με γνώση της ναυτιλιακής βιομηχανίας και των βασικών διαδικασιών της, με αποτέλεσμα τη χάραξη στρατηγικής με επίκεντρο τους βασικούς κινδύνους.
Η αυξανόμενη πολυπλοκότητα των πλοίων και η συνδεσιμότητά τους με υπηρεσίες που παρέχονται από τα δίκτυα της ξηράς μέσω του διαδικτύου, καθιστά τα συστήματα επί του πλοίου όλο και πιο εκτεθειμένα σε επιθέσεις στον κυβερνοχώρο. Από την άποψη αυτή, τα συστήματα αυτά μπορεί να είναι ευάλωτα είτε ως τρόπος πραγματοποίησης μιας επίθεσης στον κυβερνοχώρο, είτε ως σύστημα που επηρεάζεται εξαιτίας μιας επιτυχημένης επίθεσης στον κυβερνοχώρο.

Σε γενικές γραμμές, τα αυτόνομα συστήματα θα είναι λιγότερο ευάλωτα σε κυβερνοεπιθέσεις σε σύγκριση με εκείνα που είναι συνδεδεμένα σε μη ελεγχόμενα δίκτυα

ή απευθείας στο διαδίκτυο. Θα πρέπει να δοθεί προσοχή στην κατανόηση του τρόπου με τον οποίο τα κρίσιμα συστήματα του πλοίου μπορεί να συνδέονται σε μη ελεγχόμενα δίκτυα. Κατά τον τρόπο αυτό, θα πρέπει να λαμβάνεται υπόψη ο ανθρώπινος παράγοντας, καθώς πολλά περιστατικά ξεκινούν από ενέργειες του προσωπικού. Τα συστήματα επί του σκάφους θα μπορούσαν να περιλαμβάνουν:

1. Συστήματα διαχείρισης φορτίου. Τα ψηφιακά συστήματα που χρησιμοποιούνται για τη διαχείριση και τον έλεγχο του φορτίου, συμπεριλαμβανομένου του επικίνδυνου φορτίου, μπορούν να διασυνδεθούν με διάφορα συστήματα στην ξηρά. Τέτοια συστήματα μπορεί να περιλαμβάνουν εργαλεία παρακολούθησης αποστολών που είναι διαθέσιμα στους φορτωτές μέσω του διαδικτύου. Διασυνδέσεις αυτού του είδους καθιστούν τα συστήματα διαχείρισης φορτίου και τα δεδομένα στα δηλωτικά φορτίου ευάλωτα σε κυβερνοεπιθέσεις.

2. Συστήματα γέφυρας. Η αυξανόμενη χρήση ψηφιακών, δικτυωμένων συστημάτων

πλοήγησης, με διασυνδέσεις με τα δίκτυα της ξηράς για ενημέρωση και παροχή υπηρεσιών, καθιστούν τα συστήματα αυτά ευάλωτα σε κυβερνοεπιθέσεις. Τα συστήματα γέφυρας που δεν είναι συνδεδεμένα με άλλα δίκτυα μπορεί να είναι εξίσου ευάλωτα, καθώς συχνά χρησιμοποιούνται αφαιρούμενα μέσα για την ενημέρωση τέτοιων συστημάτων από άλλα ελεγχόμενα ή μη ελεγχόμενα δίκτυα. Ένα περιστατικό στον κυβερνοχώρο μπορεί να επεκταθεί σε άρνηση παροχής υπηρεσιών ή χειραγώγηση και, ως εκ τούτου, μπορεί να επηρεάσει όλα τα συστήματα που σχετίζονται με τη ναυσιπλοΐα, συμπεριλαμβανομένων των ECDIS, GNSS, AIS, VDR και Radar/ARPA.

3. Συστήματα διαχείρισης της πρόωσης και των μηχανημάτων και ελέγχου της ισχύος. Η χρήση ψηφιακών συστημάτων για την παρακολούθηση και τον έλεγχο των μηχανημάτων επί του σκάφους, της πρόωσης και του συστήματος διεύθυνσης καθιστούν τα συστήματα αυτά ευάλωτα σε επιθέσεις στον κυβερνοχώρο. Η ευπάθεια αυτών των συστημάτων μπορεί να αυξηθεί όταν χρησιμοποιούνται σε συνδυασμό με την εξ αποστάσεως παρακολούθηση βάσει κατάστασης ή/και όταν ενσωματώνονται με τον εξοπλισμό πλοήγησης και επικοινωνιών σε πλοία που χρησιμοποιούν ολοκληρωμένα συστήματα γέφυρας.

4. Συστήματα ελέγχου πρόσβασης. Ψηφιακά συστήματα που χρησιμοποιούνται για την υποστήριξη του ελέγχου πρόσβασης για τη διασφάλιση της φυσικής ασφάλειας και της ασφάλειας ενός πλοίου και του φορτίου του, συμπεριλαμβανομένων της επιτήρησης, του συναγερμού ασφαλείας του πλοίου και των ηλεκτρονικών συστημάτων «προσωπικού επί του πλοίου».

5. Συστήματα εξυπηρέτησης και διαχείρισης επιβατών. Τα ψηφιακά συστήματα που χρησιμοποιούνται για τη διαχείριση της περιουσίας, την επιβίβαση και τον έλεγχο πρόσβασης ενδέχεται να περιέχουν πολύτιμα δεδομένα που σχετίζονται με τους επιβάτες.

6. Δημόσια δίκτυα που απευθύνονται στους επιβάτες. Σταθερά ή ασύρματα δίκτυα συνδεδεμένα στο διαδίκτυο που εγκαθίστανται επί του πλοίου προς όφελος των επιβατών, για παράδειγμα συστήματα ψυχαγωγίας επισκεπτών. Τα συστήματα αυτά θα πρέπει να θεωρούνται μη ελεγχόμενα και δεν θα πρέπει να συνδέονται με κανένα κρίσιμο για την ασφάλεια σύστημα επί του σκάφους.

7. Διοικητικά συστήματα και συστήματα πρόνοιας του πληρώματος. Τα εν πλω δίκτυα υπολογιστών που χρησιμοποιούνται για τη διοίκηση του πλοίου ή την ευημερία του πληρώματος είναι ιδιαίτερα ευάλωτα όταν παρέχουν πρόσβαση στο διαδίκτυο και ηλεκτρονικό ταχυδρομείο. Μπορούν να αξιοποιηθούν από επιτιθέμενους στον κυβερνοχώρο για να αποκτήσουν πρόσβαση σε συστήματα και δεδομένα επί του σκάφους. Τα συστήματα αυτά θα πρέπει να θεωρούνται ανεξέλεγκτα και δεν θα πρέπει να συνδέονται με κανένα κρίσιμο για την ασφάλεια σύστημα επί του πλοίου.

8. Συστήματα επικοινωνίας. Η διαθεσιμότητα σύνδεσης στο διαδίκτυο μέσω δορυφόρου ή/και άλλων ασύρματων επικοινωνιών μπορεί να αυξήσει την ευπάθεια των πλοίων. Οι μηχανισμοί κυβερνοάμυνας που εφαρμόζονται από τον πάροχο υπηρεσιών θα πρέπει να εξετάζονται προσεκτικά, αλλά δεν θα πρέπει να βασίζονται αποκλειστικά στην ασφάλεια

κάθε συστήματος και δεδομένων του πλοίου.
Ευάλωτες πληροφορίες καl δεδομένα
-Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή δεδομένα σχετικά με το πλοίο, το πλήρωμα, το φορτίο και τους επιβάτες.
- Απώλεια της ακεραιότητας πληροφοριών και δεδομένων που αφορούν την ασφαλή και αποτελεσματική λειτουργία του πλοίου μετά από μη εξουσιοδοτημένη τροποποίηση.
- Απώλεια της διαθεσιμότητας πληροφοριών ή δεδομένων λόγω καταστροφής πληροφοριών και δεδομένων ή διακοπής των υπηρεσιών.

Πίνακας 7. πλαίσιο για την αξιολόγηση της τρωτότητας και του αντικτύπου τους.

Potential Impact	Definition	In practice
LOW	Η απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας θα μπορούσε να αναμένεται να έχει περιορισμένες δυσμενείς επιπτώσεις στην εταιρεία και το πλοίο, τα οργανωτικά περιουσιακά στοιχεία ή τα άτομα	Μια περιορισμένη δυσμενής επίπτωση σημαίνει ότι μια παραβίαση της ασφάλειας μπορεί: -προκληθεί απλή υποβάθμιση της λειτουργίας του πλοίου σε βαθμό και διάρκεια ώστε ο φορέας να είναι σε θέση να εκτελεί τα κύρια καθήκοντά του, αλλά η αποτελεσματικότητα των λειτουργιών να μειωθεί λίγο· -Να προκληθεί μικρή ζημία στα περιουσιακά στοιχεία του οργανισμού -Να προκληθεί μικρή οικονομική ζημία -Να έχει ως αποτέλεσμα μικρή ζημειά σε άτομα

MODERATE	Η απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας θα μπορούσε να αναμένεται να έχει σημαντικές δυσμενείς επιπτώσεις σε εταιρείες και πλοία, περιουσιακά στοιχεία εταιρειών και πλοίων ή άτομα	Μια περιορισμένη δυσμενής επίπτωση σημαίνει ότι από μια παραβίαση της ασφάλειας μπορεί: -προκληθεί όχι σημαντική υποβάθμιση της λειτουργίας του πλοίου σε βαθμό και διάρκεια ώστε ο φορέας να είναι σε θέση να εκτελεί τα κύρια καθήκοντά του, αλλά η αποτελεσματικότητα των λειτουργιών να μειωθεί σημαντικά· -Να προκληθεί όχι σημαντική ζημία στα περιουσιακά στοιχεία του οργανισμού -Να προκληθεί όχι σημαντική οικονομική ζημία -Να έχει ως αποτέλεσμα σημαντική βλάβη σε άτομα που δεν συνεπάγεται απώλεια ζωής ή σοβαρούς απειλητικούς για τη ζωή τραυματισμούς.
HIGH	Η απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας αναμένεται να έχει σοβαρές ή καταστροφικές δυσμενείς επιπτώσεις στις λειτουργίες της εταιρείας και των πλοίων, στα περιουσιακά στοιχεία της εταιρείας και του πλοίου, ή Άτομα. οργανισμού· έχουν ως αποτέλεσμα σημαντικές οικονομικές ζημίες· έχουν ως αποτέλεσμα σοβαρή ή καταστροφική βλάβη σε άτομα που συνεπάγεται απώλεια ζωής ή σοβαρούς απειλητικούς για τη ζωή τραυματισμούς.	Μια εκτεταμένη δυσμενής επίπτωση σημαίνει ότι από μια παραβίαση της ασφάλειας μπορεί: -προκληθεί σημαντική υποβάθμιση της λειτουργίας του πλοίου σε βαθμό και διάρκεια ώστε ο φορέας να είναι σε θέση να εκτελεί τα κύρια καθήκοντά του, αλλά η αποτελεσματικότητα των λειτουργιών να μειωθεί σημαντικά· -Να προκληθεί σημαντική ζημία στα περιουσιακά στοιχεία του οργανισμού -Να προκληθεί σημαντική οικονομική ζημία -Να έχει ως αποτέλεσμα σημαντική βλάβη σε άτομα που δεν συνεπάγεται απώλεια ζωής ή σοβαρούς απειλητικούς για τη ζωή τραυματισμούς.

- Στάδια Αξιολόγηση κινδύνων της εταιρείας

Για την αξιολόγηση του κινδύνου στον κυβερνοχώρο, ορίστε ένα υπεύθυνο άτομο και συγκροτήστε μια ομάδα που να περιλαμβάνει χειριστές, διαχειριστές έκτακτης ανάγκης, ειδικούς σε θέματα ασφάλειας, προστασίας και τεχνολογίας πληροφοριών. Η διαδικασία εκτίμησης κινδύνου θα προχωρήσει ως εξής:

1. Προσδιορισμός των υφιστάμενων τεχνικών και διαδικαστικών ελέγχων για την προστασία των εν πλω συστημάτων τεχνολογίας πληροφοριών (IT) και λειτουργικής τεχνολογίας (OT). Περισσότερες πληροφορίες μπορούν να βρεθούν με τους κρίσιμους ελέγχους ασφαλείας,
2. Προσδιορισμός των ευάλωτων συστημάτων IT και OT, των συγκεκριμένων

ευπαθειών που εντοπίστηκαν, συμπεριλαμβανομένων των ανθρώπινων παραγόντων, και των πολιτικών και διαδικασιών που διέπουν τη χρήση αυτών των συστημάτων,

3. Προσδιορισμός και αξιολόγηση των βασικών λειτουργιών επί του πλοίου που είναι ευάλωτες σε επιθέσεις στον κυβερνοχώρο. Αυτές οι βασικές λειτουργίες θα πρέπει να προστατεύονται προκειμένου να αποφεύγεται η διακοπή των εμπορικών λειτουργιών και να διασφαλίζεται η ασφάλεια του πληρώματος, του πλοίου και του θαλάσσιου περιβάλλοντος- και

3. Προσδιορισμός πιθανών περιστατικών στον κυβερνοχώρο και των επιπτώσεών τους στις βασικές λειτουργίες του πλοίου, καθώς και της πιθανότητας εμφάνισής τους, προκειμένου να καθοριστούν και να ιεραρχηθούν τα μέτρα μετριασμού.

• Αξιολογήσεις κινδύνων από τρίτους

Προκειμένου να καλύψει περισσότερες πτυχές κινδύνου κατά τη διάρκεια των δραστηριοτήτων της (στη στεριά και επί του πλοίου), η Εταιρεία μπορεί να ζητήσει τη συνδρομή τρίτων μερών προκειμένου να εντοπίσει τα τρωτά σημεία της. Οι αξιολογήσεις κινδύνων από τρίτους εμβαθύνουν και εντοπίζουν τους κινδύνους και τα κενά που ενδέχεται να μην εντοπιστούν κατά την αυτοαξιολόγηση. Μπορούν επίσης να πραγματοποιηθούν δοκιμές διείσδυσης σε κρίσιμες υποδομές IT για να διαπιστωθεί κατά πόσον το πραγματικό επίπεδο άμυνας αντιστοιχεί στο επιθυμητό επίπεδο που ορίζεται στη στρατηγική ασφάλειας στον κυβερνοχώρο

3.1.6 Στάδια αξιολόγησης κινδύνων στον κυβερνοχώρο

- Στάδιο 1: Δραστηριότητες πριν από την αξιολόγηση

Πριν από την έναρξη της αξιολόγησης της ασφάλειας στον κυβερνοχώρο (επί του πλοίου ή στην ξηρά), θα πρέπει να εκτελούνται οι ακόλουθες δραστηριότητες:

1. Χαρτογράφηση των βασικών λειτουργιών και συστημάτων του πλοίου ή της εταιρείας και των επιπέδων δυνητικού αντικτύπου τους, για παράδειγμα με τη χρήση του μοντέλου CIA,
2. Προσδιορισμός των κύριων παραγωγών του κρίσιμου εξοπλισμού IT και OT του πλοίου ή της ξηράς,
3. Επανεξέταση της λεπτομερούς τεκμηρίωσης των κρίσιμων συστημάτων OT και IT και των διεπαφών τους,
4. Προσδιορισμός των σημείων επαφής για την ασφάλεια στον κυβερνοχώρο σε καθέναν από τους παραγωγούς και δημιουργία σχέσεων εργασίας μαζί τους,
5. Επανεξέταση της λεπτομερούς τεκμηρίωσης σχετικά με τη συντήρηση και την υποστήριξη των συστημάτων IT και OT του πλοίου ή της ξηράς,
6. Καθορίστε τις συμβατικές απαιτήσεις και υποχρεώσεις που μπορεί να έχει ο πλοιοκτήτης/φορέας εκμετάλλευσης πλοίου για τη συντήρηση και υποστήριξη των δικτύων και του εξοπλισμού του πλοίου,
7. Υποστήριξη, εάν είναι απαραίτητο, της εκτίμησης κινδύνου με εξωτερικό εμπειρογνώμονα για την ανάπτυξη λεπτομερών σχεδίων και τη συμπερίληψη παραγωγών και παρόχων υπηρεσιών

- Στάδιο 2: Αξιολόγηση πλοίου (ή γραφείου)

Στόχος της αξιολόγησης του δικτύου ενός πλοίου (ή Γραφείου) και των συστημάτων και

συσκευών του είναι να εντοπιστούν τυχόν ευπάθειες που θα μπορούσαν να θέσουν σε κίνδυνο ή να οδηγήσουν σε απώλεια υπηρεσιών του εξοπλισμού, του συστήματος, του δικτύου ή ακόμη και του πλοίου. Αυτά τα τρωτά σημεία και οι αδυναμίες θα μπορούσαν να εμπίπτουν σε μία από τις δύο κύριες κατηγορίες:

1. Τεχνικές, όπως ελαττώματα λογισμικού, ή ξεπερασμένα ή μη επιδιορθωμένα συστήματα, ή
2. Σχεδιασμός, όπως διαχείριση πρόσβασης ή σφάλματα εφαρμογής.

Οι δραστηριότητες που εκτελούνται στο πλαίσιο της αξιολόγησης θα περιλαμβάνουν μια ανασκόπηση της κατασκευής και της διαμόρφωσης των υπολογιστών, των διακομιστών, των δρομολογητών και των τειχών προστασίας. Θα πρέπει επίσης να περιλαμβάνει ανασκοπήσεις όλων των διαθέσιμων εγγράφων και διαδικασιών ασφάλειας στον κυβερνοχώρο για τα συνδεδεμένα συστήματα και τις συσκευές ΟΤ.

- Στάδιο 3: Απολογισμός και ανασκόπηση/αναφορά τρωτότητας

Μετά την αξιολόγηση, κάθε ευπάθεια που εντοπίστηκε θα πρέπει να αξιολογηθεί ως προς τις πιθανές επιπτώσεις της και την πιθανότητα εκμετάλλευσής της. Οι συνιστώμενες τεχνικές ή/και διαδικαστικές διορθωτικές ενέργειες θα πρέπει να προσδιορίζονται για κάθε ευπάθεια σε μια τελική έκθεση.

Η έκθεση αξιολόγησης της ασφάλειας στον κυβερνοχώρο θα πρέπει να περιλαμβάνει:

1. Περίληψη - σύνοψη υψηλού επιπέδου των αποτελεσμάτων, των συστάσεων και του συνολικού προφίλ ασφάλειας του αξιολογούμενου περιβάλλοντος, εγκατάστασης ή πλοίου,
2. Τεχνικά ευρήματα - λεπτομερή, σε μορφή πίνακα, ανάλυση των ευπαθειών που ανακαλύφθηκαν, την πιθανότητα εκμετάλλευσής τους, τον επακόλουθο αντίκτυπο, καθώς και κατάλληλες τεχνικές συμβουλές για την επιδιόρθωση και τον μετριασμό των ευπαθειών,
3. Κατάλογος ενεργειών κατά προτεραιότητα - οι προτεραιότητες που αποδίδονται θα πρέπει να αντικατοπτρίζουν την αποτελεσματικότητα του μέτρου, το κόστος, την εφαρμοσιμότητα κ.λπ. Είναι σημαντικό ο κατάλογος αυτός να μην αποτελεί κατάλογο υπηρεσιών και προϊόντων που θα ήθελε να πουλήσει ο τρίτος αξιολογητής κινδύνου, αντί να είναι ένας πλήρης κατάλογος των διαθέσιμων επιλογών
4. Συμπληρωματικά στοιχεία - ένα συμπλήρωμα που περιέχει τις τεχνικές λεπτομέρειες όλων των βασικών ευρημάτων και τη συνολική ανάλυση των κρίσιμων ελαττωμάτων. Το τμήμα αυτό θα πρέπει επίσης να περιλαμβάνει δείγματα δεδομένων που ανακτήθηκαν κατά τη διάρκεια της δοκιμής διείσδυσης κρίσιμων ή υψηλού κινδύνου ευπαθειών,
5. Παραρτήματα - λεπτομερή αρχεία όλων των δραστηριοτήτων που διεξήγαγε η ομάδα αξιολόγησης της ασφάλειας στον κυβερνοχώρο και των εργαλείων που χρησιμοποιήθηκαν κατά τη διάρκεια της δέσμευσης.

- Στάδιο 4: Ενημέρωση από τον παραγωγό

Αφού ο πλοιοκτήτης έχει την ευκαιρία να εξετάσει, να συζητήσει και να αξιολογήσει τα ευρήματα, ένα υποσύνολο των ευρημάτων μπορεί να χρειαστεί να αποσταλεί στους παραγωγούς των επηρεαζόμενων συστημάτων. Οποιαδήποτε ευρήματα, τα οποία εγκρίνονται από τον πλοιοκτήτη για κοινοποίηση στους παραγωγούς, θα μπορούσαν να αναλυθούν περαιτέρω με την υποστήριξη εξωτερικών εμπειρογνωμόνων, οι οποίοι θα πρέπει να συνεργαστούν με το σημείο επαφής του παραγωγού για την ασφάλεια στον κυβερνοχώρο, ώστε να διασφαλιστεί ότι επιτυγχάνεται πλήρης κατανόηση των κινδύνων και των τεχνικών χαρακτηριστικών του προβλήματος. Αυτή η υποστηρικτική δραστηριότητα έχει ως στόχο να διασφαλίσει ότι οποιοδήποτε σχέδιο αποκατάστασης που αναπτύσσεται από τον παραγωγό είναι ολοκληρωμένο από τη φύση του και η σωστή λύση για την εξάλειψη των τρωτών σημείων που έχουν εντοπιστεί.

Εικόνα 8. Περιγράφεται η συνολική διαδικασία αξιολόγησης κινδύνων

3.1.7 Διαδικασία αξιολόγησης κινδύνων της εταιρίας

- Επιλογή Εργασίας / Καθορισμός Λειτουργίας

Οι οδηγίες πρέπει να παρέχονται είτε με τη μορφή προκαθορισμένου δείκτη είτε με τη μορφή καταλόγου εργασιών που πρέπει να αξιολογηθούν είτε με τη μορφή πλήρους καταλόγου της Βιβλιοθήκης Αξιολογήσεων Κινδύνου που μπορεί να αναπτυχθεί. Όλα τα καθήκοντα που ορίζονται πρέπει να είναι διαχειρίσιμα και πρέπει να αποφεύγονται οι γενικές εκφράσεις.

- Επιλογή ομάδας αξιολόγησης κινδύνων

Μια ομάδα από 1 έως 5 άτομα θα πρέπει να διενεργεί μια αξιολόγηση κινδύνων. Πρέπει να τηρούνται οι ακόλουθες αρχές:

Α. Θα πρέπει να αποφεύγεται ο ζυγός αριθμός ατόμων που εκτελούν την εκτίμηση κινδύνου.

Β. Διασφαλίστε ότι ΟΛΑ τα σχετικά τμήματα συμμετέχουν δεόντως στη διαδικασία εκτίμησης κινδύνου, όπως μπορεί να είναι απαραίτητο

Γ. Τα μέλη της ομάδας εκτίμησης κινδύνων πρέπει να είναι εκπαιδευμένα στην εκτίμηση κινδύνων και να είναι εξοικειωμένα με την προς εκτίμηση λειτουργία. Ο σχηματισμός ομάδας από έμπειρο προσωπικό έχει το πλεονέκτημα της πιο ρεαλιστικής άποψης για τον τρόπο εκτέλεσης της εργασιακής δραστηριότητας. Επιπλέον, οι εργαζόμενοι θα νιώσουν μεγαλύτερη συμμετοχή στη διαδικασία, αυξάνοντας έτσι την ευαισθητοποίησή τους σε θέματα υγείας και ασφάλειας και βρίσκοντας ρεαλιστικές απαντήσεις σε τυχόν προβληματικές περιοχές που εντοπίζονται.

- Καθορισμός των Όρων Αξιολόγησης Κινδύνου

Το έντυπο Αξιολόγησης Κινδύνου πρέπει να συμβουλευτείτε σχετικά με τους Όρους που μπορούν να εφαρμοστούν για κάθε Αξιολόγηση Κινδύνου. Μεταξύ άλλων, μπορούν να ληφθούν υπόψη οι ακόλουθες συνθήκες: α. Λειτουργία του πλοίου β. Ώρα της ημέρας γ. Συνθήκες θάλασσας δ. Φωτισμός ε. Θερμοκρασία αέρα στ. Εμπειρία / εξοικείωση του προσωπικού που συμμετέχει στη λειτουργία ζ. Ειδικές συνθήκες (π.χ. λειτουργία με παλίρροιες, ρεύματα κ.λπ.) Όπως αναφέρθηκε παραπάνω, οι συνθήκες αυτές αναφέρονται σε λειτουργίες επί του πλοίου, τις οποίες αντικατοπτρίζει περισσότερο ο παρών οδηγός. Σε περίπτωση διαφορετικών καθηκόντων ή δραστηριοτήτων της εταιρείας, οι όροι θα πρέπει να τροποποιούνται ανάλογα με τις ανάγκες.

- ΠροσδΙΟρΙσμός κΙΝδύνων καΙ συνεπεΙών

Επειδή οι κίνδυνοι είναι η πηγή των γεγονότων που μπορούν να οδηγήσουν σε ανεπιθύμητες συνέπειες, οι αναλύσεις για την κατανόηση της έκθεσης σε κινδύνους πρέπει να αρχίσουν με την κατανόηση των κινδύνων που υπάρχουν. Όταν εξετάζουμε τους κινδύνους της ναυτιλίας, κάποιοι θα μπορούσαν γρήγορα να τους συσχετίσουν με την ανατροπή του πλοίου, την προσάραξη, την πυρκαγιά στο πλοίο κ.λπ. Σύμφωνα με τον ορισμό της λέξης «κίνδυνος», ο οποίος ορίζει ότι κίνδυνος είναι η δυνατότητα πρόκλησης ανεπιθύμητων συνεπειών, γεγονότα όπως η ανατροπή ή η «απώλεια ευστάθειας» στην πραγματικότητα δεν είναι κίνδυνοι, αλλά γεγονότα ή συμβάντα. Οι κίνδυνοι είναι δυνατότητες πρόκλησης τέτοιων γεγονότων. Ιστορικά, ενώ οι «κίνδυνοι της θάλασσας» ήταν καλά αναγνωρισμένοι, έτειναν να θεωρούνται δεδομένοι. Οι κίνδυνοι διαφέρουν ανάλογα με τον τύπο του σκάφους και το σενάριο λειτουργίας. Οι κίνδυνοι κατά τη λειτουργία ενός πετρελαιοφόρου είναι διαφορετικοί από εκείνους ενός επιβατηγού πλοίου. Οι κίνδυνοι στην ανοικτή θάλασσα είναι διαφορετικοί από εκείνους σε μια προσέγγιση σε λιμάνι.

- Βαθμολογήστε την πΙθανότητα & τη σοβαρότητα

Αφού εντοπιστούν οι κίνδυνοι ενός συστήματος ή μιας διαδικασίας, το επόμενο βήμα κατά την εκτέλεση μιας εκτίμησης κινδύνου είναι η εκτίμηση της πιθανότητας και της σοβαρότητας καθενός από αυτούς. Ο καλύτερος τρόπος για να αποδώσετε μια πιθανότητα σε ένα συμβάν είναι να ερευνήσετε τις βιομηχανικές βάσεις δεδομένων και να εντοπίσετε καλά ιστορικά δεδομένα συχνότητας που αφορούν το συμβάν που αναλύεται. Η σοβαρότητα είναι μια εκτίμηση της στατιστικά αναμενόμενης έκθεσης της ζωής, της περιουσίας, του περιβάλλοντος και της φήμης στον κίνδυνο ενδιαφέροντος και των επιπτώσεων που σχετίζονται με αυτό το επίπεδο έκθεσης. Για την αξιολόγηση του κινδύνου συμβουλευτείτε τη σχετική αφίσα «Αξιολόγηση κινδύνου» και σημειώστε τα ακόλουθα:

Α. Αξιολογήστε τη σοβαρότητα των συνεπειών στην επιλεγμένη κλίμακα (1 έως 5)

Β. Αξιολογήστε την ομοιόμορφη κουκούλα ή τη συχνότητα του κινδύνου στην επιλεγμένη

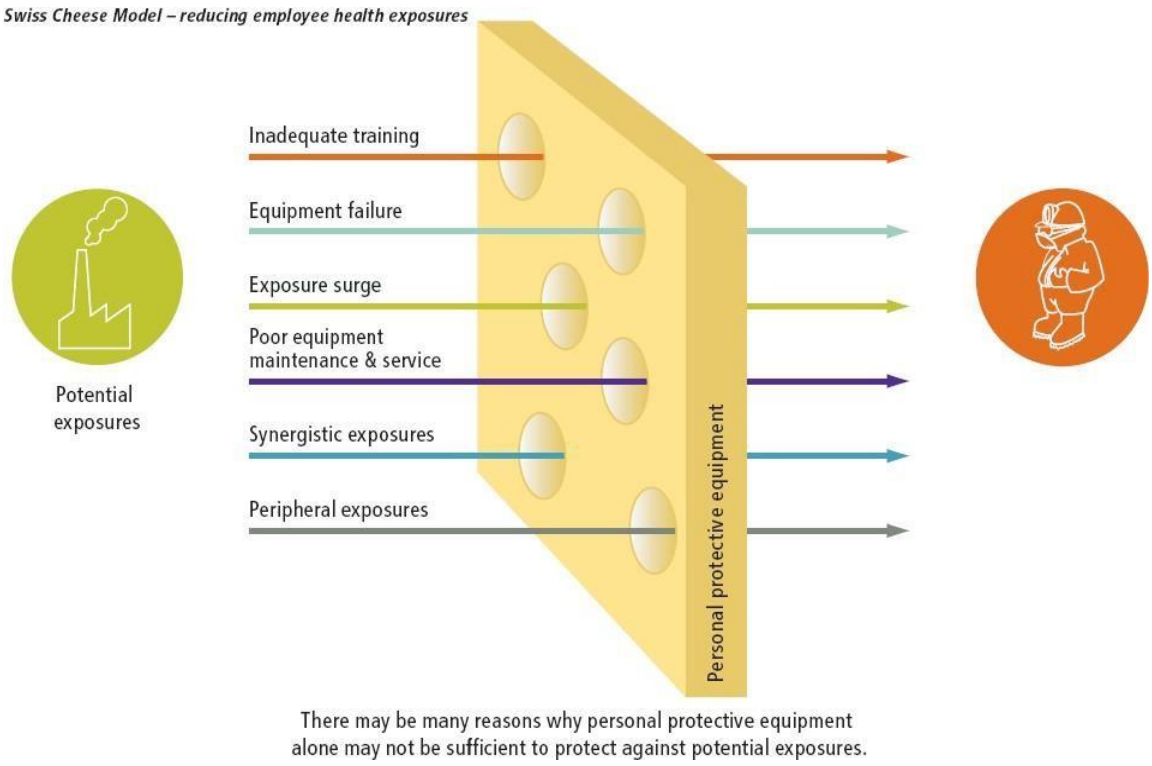
κλίμακα (1 έως 5)

Γ. Αξιολόγηση της βαθμολογίας κινδύνου με τον υπολογισμό της σοβαρότητας επί την αντίστοιχη συχνότητα

Δ. Καθορίστε την κατηγορία κινδύνου σύμφωνα με τη βαθμολογία της αξιολόγησης κινδύνου και σύμφωνα με την αφίσα αξιολόγησης κινδύνου (πίνακας για την αξιολόγηση κινδύνου περιλαμβάνεται στην αφίσα μαζί με την επεξήγηση ή τις κατηγορίες σοβαρότητας/πιθανότητας)

- Ελέγξτε την αξIOλόγηση κINδύνου (χωρίς ελέγχους)

Αφού προσδιοριστούν οι κίνδυνοι και τα πιθανά ατυχήματα ή συμβάντα για ένα σύστημα ή μια διαδικασία και εκτιμηθεί η πιθανότητα και η σοβαρότητα που συνδέονται με αυτά τα συμβάντα, θα πρέπει να εξεταστεί η αξιολόγηση των σχετικών κινδύνων που συνδέονται με τα συμβάντα. Αρχικά θα πρέπει να γίνει μια εκτίμηση για την αποδοχή του αποτελέσματος. Είναι ανεκτό ή όχι; Οι κίνδυνοι εξετάζονται χωρίς ελέγχους και προφυλάξεις ασφαλείας για να δούμε το αποτέλεσμα και την έκβαση της διαδικασίας. Στις περισσότερες περιπτώσεις το αποτέλεσμα θα πρέπει να είναι μη αποδεκτό λόγω των συνεπειών και της σοβαρότητας των επιπτώσεων στη ζωή, την περιουσία, το περιβάλλον και τη φήμη



Εικόνα 9. Η ανικανότητα του προσωπικού προστατευτικού εξοπλισμού να εμποδίσει πιθανές

Τα ακόλουθα σημεία θα πρέπεI πάντα να θυμόμαστε:
Α. Όλοι οι κίνδυνοι πρέπει να καταχωρούνται στο έντυπο. Εάν απαιτούνται περισσότερα από ένα έντυπα, χρησιμοποιήστε πρόσθετο έντυπο και σημειώστε το όπως απαιτείται.
Β. Να καταχωρείτε πάντα τη σοβαρότητα και την πιθανότητα (συχνότητα) σύμφωνα με την πραγματική ζωή και την προηγούμενη εμπειρία.
Γ. Αφού ληφθούν οι απαραίτητες πληροφορίες, το επόμενο στάδιο είναι η αξιολόγηση των κινδύνων (RISK RATING SCORE).
Δ. Η βαθμολογία αξιολόγησης κινδύνου χρησιμοποιείται για να βοηθήσει στην αξιολόγηση του Κινδύνου και για να αποφασιστεί ποια δράση απαιτείται, εάν απαιτείται.
Ε. Ο συνολικός κίνδυνος μπορεί να προσδιοριστεί χρησιμοποιώντας τον ακόλουθο τύπο: Βαθμολογία κινδύνου = Σοβαρότητα x Πιθανότητα ή Βαθμολογία κινδύνου = Συνέπειες x Συχνότητα
ΣΤ. Εάν η Βαθμολογία Αξιολόγησης Κινδύνου είναι χαμηλή λόγω της εφαρμογής αποτελεσματικών μέτρων ελέγχου, πρέπει να αναληφθεί δράση για να διασφαλιστεί ότι τα μέτρα αυτά παραμένουν σε ισχύ.

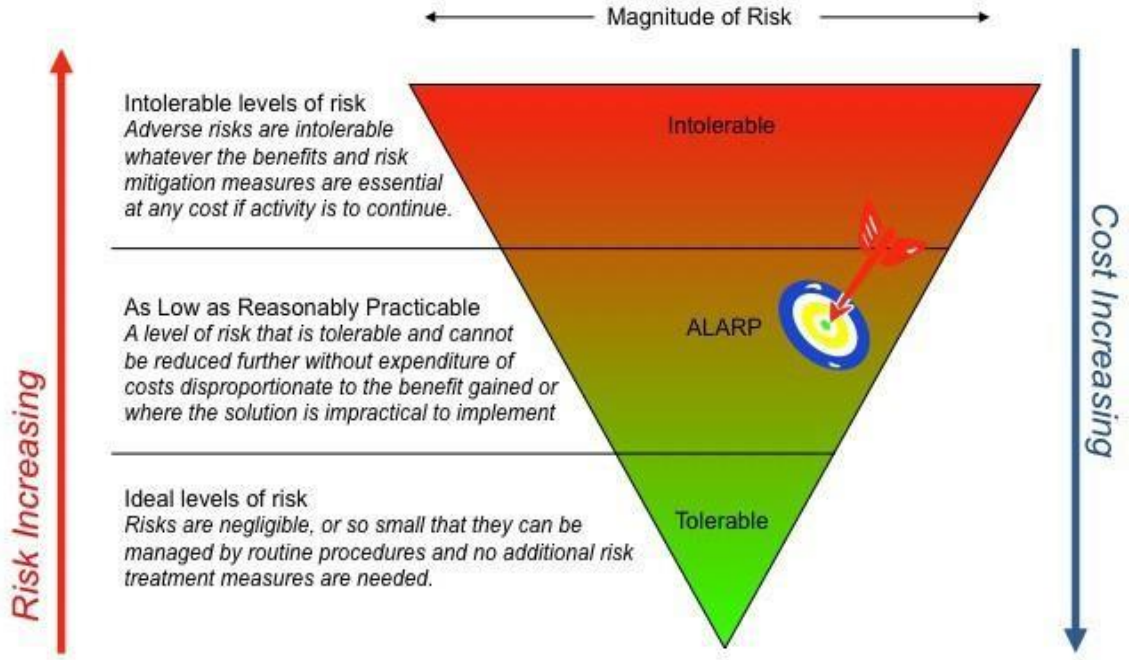
- Λήψη κατάλληλων μέτρων ελέγχου

Η βασική αρχή του ελέγχου των κινδύνων στο χώρο εργασίας είναι είτε η εξάλειψη του κινδύνου είτε ο έλεγχος των πιθανών συνεπειών του. Κάθε μέτρο ελέγχου που εισάγεται θα πρέπει να σχεδιάζεται έτσι ώστε:
1. Μείωση της πιθανής σοβαρότητας του τραυματισμού που θα μπορούσε να προκληθεί, για παράδειγμα, με την παροχή πάντα ζωνών ασφαλείας σε άτομα που εργάζονται ψηλά, ή με πρόσθετες περιπολίες, ή με πρόσθετη επίβλεψη της εργασίας, για άλλες εργασίες.
2. Μείωση της πιθανότητας να συμβεί ένας τραυματισμός με την εισαγωγή κατάλληλων μέτρων ελέγχου.

Θα πρέπεI Να σημεIωθεί ότI:
Α. Ο κίνδυνος ελέγχεται καλύτερα με την απομάκρυνση του κινδύνου,
Β. Η δραστηριότητα ή η διεργασία θα πρέπει, όπου είναι εφικτό, να αντικατασταθεί με μια λιγότερο επικίνδυνη (αν και θα απαιτηθεί νέα εκτίμηση κινδύνου),
Γ. Τα ασφαλή συστήματα εργασίας χρησιμοποιούνται συνήθως σε συνδυασμό με άλλα μέτρα,
Δ. Πρέπει πάντα να παρέχεται επαρκής διδασκαλία, ενημέρωση και εκπαίδευση,
Ε. Πρέπει να παρέχονται επαρκή επίπεδα επίβλεψης για να διασφαλίζεται η χρήση των μέτρων ελέγχου,
ΣΤ. Τα μέσα ατομικής προστασίας πρέπει να παρέχονται ως έσχατη λύση.
Προτεραιότητα πρέπει πάντα να δίνεται στα μέτρα που προστατεύουν τους περισσότερους ανθρώπους. Η απομάκρυνση του κινδύνου από το χώρο εργασίας συνεπάγεται τη μικρότερη προσπάθεια για την αποτελεσματική διαχείριση, ενώ η παροχή ΜΑΠ συνεπάγεται τη μεγαλύτερη.
Όταν αποφασίζεται ποια μέτρα ελέγχου μπορεί να απαιτούνται, θα πρέπει να λαμβάνονται υπόψη τυχόν νομικές, ηθικές ή εταιρικές απαιτήσεις, κώδικες πρακτικής ή οδηγίες, βιομηχανικά πρότυπα ή βέλτιστες πρακτικές.

- Διασφάλιση ότI Ο κίνδυνος είναI αποδεκτός

Ο κίνδυνος πρέπει να μειώνεται πάντοτε σε επίπεδα ALARP (ALARP = As Low As Reasonably Practicable). Αυτό σημαίνει ότι ο κίνδυνος θα πρέπει να μειωθεί στο μέγιστο δυνατό βαθμό με τη χρήση των υφιστάμενων πόρων.
Εάν ο προκύπτων κίνδυνος εξακολουθεί να παραμένει στην περιοχή υψηλού κινδύνου (αφίσα αξιολόγησης κινδύνου), τότε ΔΕΝ πρέπει να ξεκινήσει ΚΑΜΙΑ επιχείρηση ΠΡΙΝ ο κίνδυνος μειωθεί σε αποδεκτά επίπεδα.



Εικόνα 10. Παρουσίαση του μέγεθος του κινδύνου

Η μείωση του κινδύνου ALARP δεν σημαίνει ότι ο εντοπισμένος κίνδυνος δεν θα μπορούσε να προκαλέσει περιστατικό. Πρακτικά σημαίνει ότι το επίπεδο κινδύνου είναι ανεκτό και δεν μπορεί να μειωθεί περαιτέρω με τα μέτρα ελέγχου που είμαστε σε θέση να εφαρμόσουμε.

- Διασφάλιση της επιτυχούς διαχείρισης όλων των κινδύνων

Ανά πάσα στιγμή η ομάδα που διενεργεί την εκτίμηση κινδύνου θα πρέπει να διασφαλίζει ότι η πλήρης διαδικασία αποτελεσματικής διαχείρισης των κινδύνων έχει εφαρμοστεί σωστά και έχει ενσωματωθεί στην εκτίμηση κινδύνου. Το περίγραμμα της αποτελεσματικής διαχείρισης των κινδύνων περιγράφεται ως εξής στα ακόλουθα στάδια:

1. Είναι οι άνθρωποι, το περιβάλλον, τα περιουσιακά στοιχεία ή η φήμη της εταιρείας εκτεθειμένα σε πιθανή βλάβη;
2. Ποιες είναι οι αιτίες και οι συνέπειες;

Αξιολόγηση 3. Πόσο πιθανή είναι η απώλεια ελέγχου;

4. Ποιος είναι ο κίνδυνος και είναι ALARP;
5. Μπορούν να εξαλειφθούν τα αίτια; Έλεγχος 6. Ποιοι έλεγχοι απαιτούνται;
7. Πόσο αποτελεσματικοί είναι αυτοί οι έλεγχοι ;

8. Μπορούν να μετριαστούν οι πιθανές συνέπειες ή επιπτώσεις;
9. Ποια μέτρα ανάκαμψης απαιτούνται;
10. Είναι οι δυνατότητες ανάκαμψης κατάλληλες και επαρκείς ;

- Τεκμηρίωση της εκτίμησης κΙΝδύνου

Η αξιολόγηση κινδύνων που προκύπτει θα πρέπει να τεκμηριώνεται με τη χρήση του σχετικού εντύπου και να φυλάσσεται μαζί με τις άλλες αξιολογήσεις κινδύνων στη βιβλιοθήκη των αξιολογήσεων κινδύνων που τηρείται στην εταιρεία.

Το ευρετήριο της Βιβλιοθήκης Αξιολόγησης Κινδύνων πρέπει να ενημερώνεται με τα στοιχεία της αξιολόγησης κινδύνων.

- Ανασκόπηση της αξΙΟλόγησης

Η εφαρμογή των μέτρων ελέγχου πρέπει να παρακολουθείται και να καταγράφεται και να γίνεται αξιολόγηση των ελέγχων, ώστε να διασφαλίζεται ότι παραμένουν στη θέση τους και έχουν το επιθυμητό αποτέλεσμα. Οι διενεργηθείσες αξιολογήσεις κινδύνου θα πρέπει να επανεξετάζονται περιοδικά για να διασφαλίζεται η εφαρμογή των υφιστάμενων διαδικασιών/προϋποθέσεων και η περιοδικότητα μπορεί να ποικίλλει ανάλογα με το επίπεδο επικινδυνότητας της λειτουργίας/της εργασίας/του συστήματος.

Σε περίπτωση σημαντικής αλλαγής των συνθηκών, του προσωπικού ή των μέτρων ελέγχου, τότε η όλη διαδικασία πρέπει να εφαρμοστεί εκ νέου, ώστε το τελικό αποτέλεσμα και το υπολογιζόμενο επίπεδο κινδύνου να περιλαμβάνουν όλους τους νέους παράγοντες και συνθήκες.

Η διαδικασία εκτίμησης κινδύνου δεν σταματά ποτέ, διότι το σύστημα θα χρησιμοποιεί την προηγούμενη εμπειρία, τα νέα μέτρα θα βασίζονται σε βεΟΤιωμένα μέτρα κ.ο.κ.

3.1.8 Υπολογισμός του κινδύνου

Η εκτίμηση του κινδύνου συνίσταται σε μια αντικειμενική αξιολόγηση του κινδύνου στην οποία οι παραδοχές και οι αβεβαιότητες εξετάζονται και παρουσιάζονται με σαφήνεια. Μέρος της δυσκολίας στη διαχείριση κινδύνου είναι ότι η μέτρηση και των δύο μεγεθών στα οποία αφορά η αξιολόγηση κινδύνου - της σοβαρότητας και της πιθανότητας - μπορεί να είναι πολύ δύσκολο να μετρηθεί. για τον υπολογισμό του επιπέδου κινδύνου σε ένα έργο , μια δραστηριότητα ή μια λειτουργία χρησιμοποιούνται πίνακες κινδύνου για να καθοριστεί αν ο κίνδυνος (ως αποτέλεσμα ενός κινδύνου) είναι ανεκτός ή όχι.

3.1.9 Πίνακας κινδύνων

Ο πίνακας κινδύνων είναι το ΠΙΟ ΣΗΜΑΝΤΙΚΟ εργαλείο για την αξιολόγηση των κινδύνων. Το πιο συνηθισμένο είναι ο πίνακας 5x5 που χρησιμοποιείται προκειμένου να εφαρμοστεί η αξιολόγηση κινδύνων. Ο πίνακας κινδύνων μπορεί να επεκταθεί ώστε να περιλαμβάνει περισσότερες γραμμές και στήλες, ανάλογα με το πόσο επιμελώς επιθυμεί η εταιρεία να διακρίνει τις κατηγορίες. Οι όροι που χρησιμοποιούνται για την πιθανότητα και τη συνέπεια μπορούν να αλλάξουν για να βοηθηθεί η κατανόηση. Για παράδειγμα, η πιθανότητα μπορεί να εκφραστεί με τους όρους «μία φορά ανά ταξίδι», «μία φορά ανά έτος πλοίου» ή «μία φορά ανά έτος στόλου», και η συνέπεια μπορεί να γίνει πιο συγκεκριμένη με τη χρήση των όρων «τραυματισμός πρώτων βοηθειών», «σοβαρός τραυματισμός» ή «θάνατος», χωρίς να ξεχνάμε τις συνέπειες για την περιουσία και το περιβάλλον.

Πίνακας 8. 5x5 Risk Matrix

RAM Settings and Risk Rating		LIKELIHOOD				
		1 Improbable	2 Remote	3 Possible	4 Likely	5 Certain
SEVERITY	1 Negligible	1	2	3	4	5
	2 Minor	2	4	6	8	10
	3 Significant	3	6	9	12	15
	4 Critical	4	8	12	16	20
	5 Catastrophic	5	10	15	20	25

- Επίπεδο κΙΝδύνου

Ο πίνακας κινδύνου υπολογίζει τη βαθμολογία κινδύνου και οδηγεί στα ίδια συμπεράσματα για το επίπεδο κινδύνου. Υπάρχουν τρεις κατηγορίες επιπέδου κινδύνου όπως περιγράφεται παρακάτω, Υψηλός, Μέτριος και Χαμηλός.

Το υπολογιζόμενο επίπεδο κινδύνου καθορίζει είτε μια ενέργεια, εργασία ή λειτουργία θα πραγματοποιηθεί με τα εφαρμοζόμενα μέτρα ελέγχου είτε όχι. Η κοινή πρακτική καθορίζει τα αποδεκτά επίπεδα κινδύνου σύμφωνα με τον παράγοντα ALARP.

- Χαμηλό: Δεν απαιτούνται πρόσθετοι έλεγχοι, εκτός εάν μπορούν να εφαρμοστούν με πολύ χαμηλό κόστος (από άποψη χρόνου, χρήματος και προσπάθειας). Οι δράσεις για την περαιτέρω μείωση αυτών των κινδύνων έχουν χαμηλή προτεραιότητα. Θα πρέπει να ληφθούν μέτρα για να διασφαλιστεί η διατήρηση των ελέγχων.
- Μέτρια: Θα πρέπει να εξετάζεται κατά πόσον οι κίνδυνοι μπορούν να μειωθούν, κατά περίπτωση, σε ανεκτό επίπεδο και κατά προτίμηση σε αποδεκτό επίπεδο, αλλά θα πρέπει να λαμβάνεται υπόψη το κόστος των πρόσθετων μέτρων μείωσης των κινδύνων. Τα μέτρα μείωσης των κινδύνων θα πρέπει να εφαρμοστούν εντός καθορισμένης χρονικής περιόδου. Θα πρέπει να ληφθούν μέτρα για να διασφαλιστεί ότι οι έλεγχοι διατηρούνται, ιδίως εάν η περιοχή των επιπέδων κινδύνου συνδέεται με επιβλαβείς συνέπειες.
- Υψηλός: Ο κίνδυνος είναι απαράδεκτος. Απαιτούνται ουσιαστικές βελτιώσειςστα μέτρα ελέγχου του κινδύνου, ώστε ο κίνδυνος να μειωθεί σε ανεκτό ή αποδεκτό επίπεδο. Η δραστηριότητα εργασίας πρέπει να διακοπεί έως ότου εφαρμοστούν έλεγχοι κινδύνου που μειώνουν τον κίνδυνο ώστε να μην είναι πλέον πολύ υψηλός.

Εάν το ρίσκο δεν είναι δυνατόν να περιοριστεί τότε η εργασία θα πρέπει να παραμείνει απαγορευμένη.

3.2 Σχέδιο έκτακτης ανάγκης και πολιτικής προστασίας

3.2.1 Σχέδιο διαχείρισης της ασφάλειας στον κυβερνοχώρο

• ΔιαδΙκασία σχεδίου έκτακτης ανάγκης.

Η εταιρεία, προκειμένου να προστατεύσει τον εξοπλισμό και το σύστημα γραφείου από επιθέσεις στον κυβερνοχώρο, ανέπτυξε αυτό το σχέδιο. Το σχέδιο βασίζεται στους ακόλουθους κανόνες:

Α. Προσδιορισμός των πιθανών συστημάτων που ενδέχεται να υποστούν επίθεση Β. Ενέργειες που πρέπει να αναληφθούν για την αντιμετώπιση
Γ. Στοιχεία επικοινωνίας

Τα σχέδια αποκατάστασης πρέπει να είναι προσβάρlσιμα από τους αξιωματικούς επί του σκάφους σύμφωνα με τις αρμοδιότητές τους που ορίζονται στα σχέδια. Ο σκοπός και το πεδίο εφαρμογής κάθε συγκεκριμένου σχεδίου θα πρέπει να καθορίζονται και να γίνονται κατανοητά από τα στελέχη και το πιθανό εξωτερικό προσωπικό IT. Θα πρέπει να είναι διαθέσιμες βασικές εγκαταστάσεις δημιουργίας αντιγράφων ασφαλείας πληροφοριών και λογισμικού, ώστε να διασφαλίζεται ότι η ανάκαμψη μπορεί να πραγματοποιηθεί μετά από ένα συμβάν στον κυβερνοχώρο.

• Προστασία από τΙς δραστηρΙότητες τρίτων

Η εταιρεία έχει κατανοήσει πλήρως τα συστήματα OT και IT του πλοίου και τον τρόπο με τον οποίο τα συστήματα αυτά συνδέονται και ενσωματώνονται με την πλευρά της ξηράς. Αυτό απαιτεί κατανόηση όλων των συστημάτων που βασίζονται σε υπολογιστή επί του πλοίου και του τρόπου με τον οποίο η ασφάλεια, οι λειτουργίες και οι επιχειρήσεις μπορούν να τεθούν σε κίνδυνο από ένα περιστατικό στον κυβερνοχώρο.

Επιπλέον, η Εταιρεία απαιτεί να λαμβάνονται υπόψη τα ακόλουθα όσον αφορά τους παραγωγούς και τα τρίτα μέρη, συμπεριλαμβανομένων των εργολάβων και των παρόχων υπηρεσιών:

1. Η ευαισθητοποίηση και οι διαδικασίες κυβερνοασφάλειας του παραγωγού και του παρόχου υπηρεσιών: Πολλές από αυτές τις εταιρείες δεν διαθέτουν εκπαίδευση και διακυβέρνηση για την ευαισθητοποίηση στον κυβερνοχώρο στις δικές τους οργανώσεις και αυτό μπορεί να αποτελεί περισσότερες πηγές ευπάθειας, οι οποίες θα μπορούσαν να οδηγήσουν σε περιστατικά στον κυβερνοχώρο. Οι εταιρείες θα πρέπει να διαθέτουν επικαιροποιημένη εταιρική πολιτική για την ασφάλεια στον κυβερνοχώρο, η οποία περιλαμβάνει διαδικασίες κατάρτισης και διακυβέρνησης για προσβάσιμα συστήματα IT και OT επί του σκάφους.

3. Η ωριμότητα των διαδικασιών ασφάλειας στον κυβερνοχώρο ενός τρίτου μέρους: Η εταιρεία θα πρέπει να διερευνήσει την εσωτερική διακυβέρνηση για την ασφάλεια των δικτύων στον κυβερνοχώρο και να επιδιώξει να αποκτήσει διαβεβαίωση ασφάλειας στον κυβερνοχώρο κατά την εξέταση μελλοντικών συμβάσεων και υπηρεσιών. Αυτό είναι ιδιαίτερα σημαντικό όταν καλύπτεται η ασφάλεια δικτύου, εάν το πλοίο πρόκειται να διασυνδεθεί με τον τρίτο.

3.2.2 Ευπάθεια

Προκειμένου να προσδιοριστεί η τρωτότητα ενός εξοπλισμού ή συστήματος, η Εταιρεία αξιολόγησε τον παράγοντα του πόσο εύκολο ή/και σύνηθες είναι να δεχθεί ο εξοπλισμός

κυβερνοεπίθεση.
Η εταιρεία προσδιόρισε τρία επίπεδα τρωτότητας:
- Χαμηλό: Το σύστημα μπορεί να δεχθεί δύσκολα επίθεση ή να μπλοκαριστεί
- Μέτριο: Το σύστημα μπορεί να δεχτεί επίθεση και υπό σημαντικές συνθήκες μπορεί να τεθεί εκτός λειτουργίας ή να μπλοκαριστεί / παραβιαστεί.
- Υψηλό: Το σύστημα μπορεί πολύ εύκολα να δεχθεί επίθεση / να καταστραφεί ή να παραβιαστεί από κυβερνοεπιτιθέμενο.

3.2.3 Κρίσιμος εξοπλισμός

Η εταιρεία θεωρεί κρίσιμο κάθε εξοπλισμό που μπορεί να θέσει σε κίνδυνο την ασφάλεια των σκαφών, την ασφάλεια ή την περιουσία του προσωπικού (πλήρωμα ή εργαζόμενοι στην ξηρά), το περιβάλλον, το φορτίο ή τη φήμη ή τα συμφέροντα της εταιρείας.

3.2.4 Προσδιορισμός των συστημάτων

Πίνακας 9. Ανάλυση συστημάτων τα οποία έχουν εντοπιστεί ως πιθανοί στόχοι κυβερνοεπίθεσης.

#	Συστήματα / Εξοπλισμός	VulnerabilITy	Κρίσιμος Εξοπίσμός		Παρατηρήσεις
			YES	NO	
1.	Συστήματα επικοινωνίας	Μέτρια	✓		
2.	Ασύρματα δίκτυα (WLAN)	Υψηλή	✓		
3.	Αναγγελίες και γενικά συστήματα συναγερμού	Χαμηλή	✓		
4.	Συστήματα ελέγχου πρόσβασης	Χαμηλή	✓		
5.	Συστήματα επιτήρησης όπως δίκτυο CCTV	Χαμηλή	✓		
6.	Δρομολογητές	Υψηλή	✓		
7.	Διακόπτες	Μέτρια	✓		
8.	Τείχη προστασίας	Υψηλή	✓		
9.	Εικονικά ιδιωτικά δίκτυα (VPN)	Υψηλή	✓		
10.	Εικονικό LAN(s) (VLAN)	Υψηλή			**Δεν υφίσταται**
11.	Συστήματα πρόληψης εισβολής	Μέτρια	✓		
12.	Συστήματα καταγραφής συμβάντων ασφαλείας	Χαμηλή	✓		
13.	Διοικητικά συστήματα	Χαμηλή	✓		
14.	Πρόσβαση Wi-Fi ή LAN στο διαδίκτυο των εργαζομένων, για παράδειγμα όπου οι εργαζόμενοι μπορούν συνδέουν τις δικές τους επινοήσει	Υψηλή	✓		

3.2.5 Κέντρο επιχειρήσεων ασφαλείας (SOC)

Ένα SOC ενεργεί ως κεντρική μονάδα που ασχολείται με θέματα ασφάλειας που επηρεάζουν τα κυβερνο-φυσικά συστήματα που βρίσκονται σε ένα πλοίο ή στόλο πλοίων ή είναι συνδεδεμένα με αυτά, συμπεριλαμβανομένων εκείνων που αφορούν την ασφάλεια στον κυβερνοχώρο. Το SOC μπορεί να είναι ο καθιερωμένος χώρος της Εταιρείας για την ομάδα αντιμετώπισης έκτακτης ανάγκης.ξηρά), το περιβάλλον, το φορτίο ή τη φήμη ή τα συμφέροντα της εταιρείας

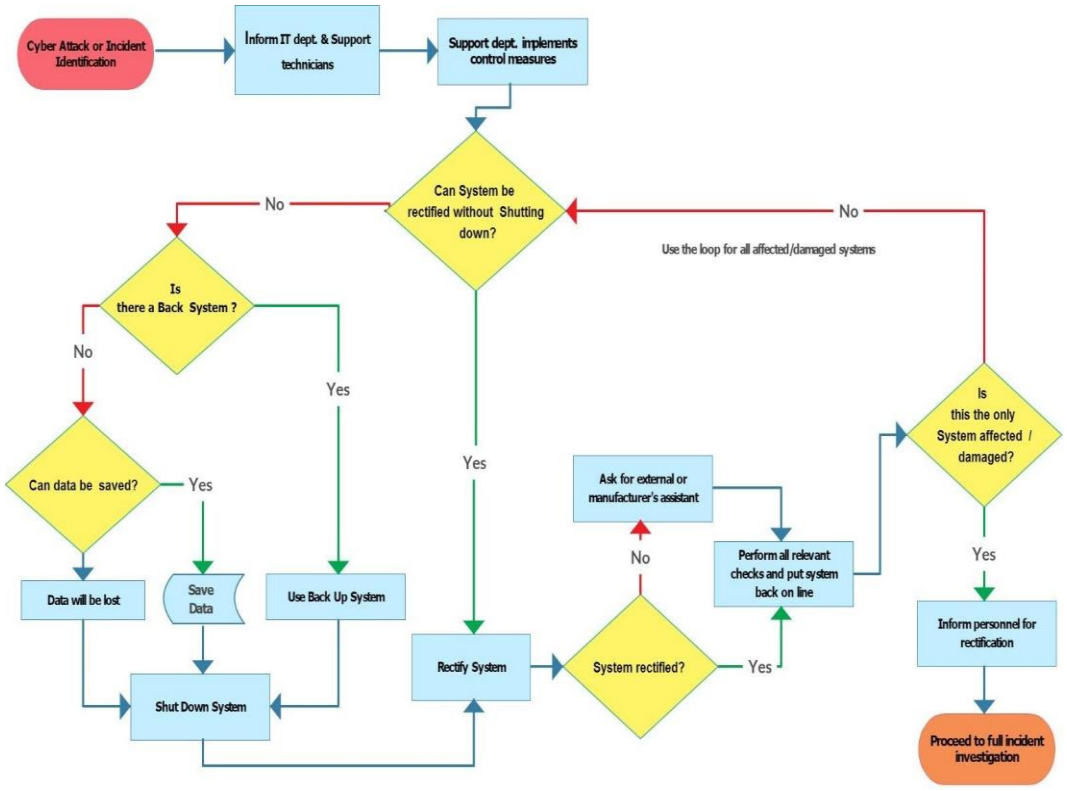
Οι βασικές λειτουργίες ενός SOC είναι οι εξής:

- Να παρατηρεί, διατηρώντας επίγνωση της κατάστασης, δηλαδή να κατανοεί τις πιθανές, αναδυόμενες και πραγματικές απειλές για τις λειτουργίες του πλοίου. Η παρατήρηση περιλαμβάνει την ανίχνευση μη εξουσιοδοτημένων αλλαγών στα συστήματα του πλοίου ή στα δεδομένα του πλοίου, μη ασφαλών τρόπων λειτουργίας και μη εξουσιοδοτημένης πρόσβασης σε περιουσιακά στοιχεία του πλοίου.
- Προσανατολισμός, με την ανάλυση του κινδύνου για τις λειτουργίες από νέες ή αλλαγμένες απειλές και τον προσδιορισμό του κατά πόσον απαιτούνται προληπτικά μέτρα για τη μείωση του κινδύνου σε αποδεκτό επίπεδο.
- Αποφασίστε ποια ενέργεια μπορεί να είναι κατάλληλη είτε για την άρνηση περαιτέρω πρόσβασης στο περιουσιακό στοιχείο του πλοίου είτε για την αντιμετώπιση του συμβάντος με τον προσδιορισμό κατάλληλων ελέγχων ασφαλείας.
- Ενεργεί, εφαρμόζοντας την αποφάσεις.

3.2.6 Άσκηση ασφάλειας στον κυβερνοχώρο

Είναι σημαντικό το αρμόδιο προσωπικό να εκτελεί τακτικά ασκήσεις ασφάλειας στον κυβερνοχώρο, προκειμένου να συμβάλει στη διατήρηση της αποτελεσματικότητας της ικανότητας απόκρισης. Οι ασκήσεις ασφάλειας στον κυβερνοχώρο θα μπορούσαν, κατά περίπτωση, να εμπνέονται από πραγματικά γεγονότα και να αποτελούν προσομοιώσεις περιστατικών μεγάλης κλίμακας που κλιμακώνονται και μετατρέπονται σε κρίσεις στον κυβερνοχώρο. Αυτό προσφέρει την ευκαιρία να αναλυθούν προηγμένα τεχνικά περιστατικά ασφάλειας στον κυβερνοχώρο, αλλά και να βοηθήσουν στην αντιμετώπιση της επιχειρησιακής συνέχειας και της διαχείρισης κρίσεων. Μια άσκηση στον κυβερνοχώρο πρέπει να διεξάγεται μία φορά το χρόνο (ετησίως), προκειμένου να ενισχυθεί η ανταπόκριση του προσωπικού σε ξηρά και επί του πλοίου. Στο Παράρτημα Α υπάρχουν ορισμένα περιστατικά που θα πρέπει να χρησιμοποιηθούν ως παραδείγματα προκειμένου να ελεγχθεί η ανταπόκριση όλων των συμμετεχόντων. Τα αποτελέσματα της άσκησης θα πρέπει να διανεμηθούν σε ολόκληρο τον στόλο με τα διδάγματα που αντλήθηκαν και τα σχόλια του γραφείου.

Η μορφή της αλληλογραφίας των μηνυμάτων τυποποιήθηκε στα SMS που θα χρησιμοποιηθούν για ηλεκτρονικά μηνύματα ή ανταλλαγή μηνυμάτων και αξιολόγηση της άσκησης.



Εικόνα 11. Αντιμετώπιση περιστατικών στον κυβερνοχώρο του γραφείου.

ΠΟΛΙΤΙΚΉ ΑΣΦΆΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΏΡΟ

ΣΤΟΧΟΣ

Η EUROPEAN PRODUCT CARRIERS LTD, προκειμένου να αντιμετωπίσει θέματα ασφάλειας στον κυβερνοχώρο, δημοσίευσε την ακόλουθη πολιτική ασφάλειας στον κυβερνοχώρο. Σκοπός και στόχος της παρούσας Πολιτικής Ασφάλειας στον Κυβερνοχώρο είναι η προστασία των περιουσιακών στοιχείων πληροφοριών της εταιρείας από όλες τις απειλές, εσωτερικές ή εξωτερικές, σκόπιμες ή τυχαίες, ώστε να διασφαλίζεται η συνέχεια των λειτουργιών, να ελαχιστοποιούνται οι ζημίες και να μεγιστοποιείται η απόδοση των επενδύσεων και των σχετικών ευκαιριών του κλάδου.

Πολιτική

1. Η ανώτατη διοίκηση έχει εγκρίνει την πολιτική ασφάλειας στον κυβερνοχώρο.

2. Αποτελεί πολιτική της EUROPEAN PRODUCT CARRIERS LTD να διασφαλίζει ότι:

a. Οι πληροφορίες και τα συστήματα που έχουν αναγνωριστεί ως ευάλωτα σε επιθέσεις στον κυβερνοχώρο θα προστατεύονται από την απώλεια: της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

b. Θα πληρούνται οι κανονιστικές και νομοθετικές απαιτήσεις.

c. Έχουν εκπονηθεί σχέδια έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο προς υποστήριξη.

d. Η εκπαίδευση για την ασφάλεια στον κυβερνοχώρο θα είναι διαθέσιμη σε όλο το προσωπικό.

e. Όλες οι παραβιάσεις της ασφάλειας των πληροφοριών, πραγματικές ή ύποπτες, θα αναφέρονται και θα διερευνώνται από τον διευθυντή πληροφορικής.

f. Τα συνεργαζόμενα τρίτα μέρη (πάροχοι υπηρεσιών, παραγωγοί κ.λπ.) θα επανεξετάζονται όσον αφορά την πολιτική και τις επιδόσεις τους στον τομέα της ασφάλειας στον κυβερνοχώρο.

1. Για την υποστήριξη αυτής της πολιτικής έχουν δημιουργηθεί οδηγίες και διαδικασίες. Σε αυτές περιλαμβάνονται ο χειρισμός περιστατικών, η δημιουργία αντιγράφων ασφαλείας πληροφοριών, η πρόσβαση στο σύστημα, ο έλεγχος ιών και η κρυπτογράφηση.
2. Ο ρόλος και η ευθύνη του καθορισμένου διαχειριστή πληροφορικής είναι να διαχειρίζεται την ασφάλεια των πληροφοριών και να παρέχει συμβουλές και καθοδήγηση σχετικά με την εφαρμογή της πολιτικής για την ασφάλεια στον κυβερνοχώρο.
3. Ο καθορισμένος ιδιοκτήτης της πολιτικής ασφάλειας στον κυβερνοχώρο έχει την άμεση ευθύνη για τη διατήρηση και την αναθεώρηση της πολιτικής.
4. Όλοι οι διευθυντές είναι άμεσα υπεύθυνοι για την εφαρμογή της Πολιτικής Ασφάλειας στον Κυβερνοχώρο εντός των τμημάτων τους.
5. Είναι ευθύνη κάθε υπαλλήλου/μέλους του συνεργείου να τηρεί την Πολιτική Ασφάλειας στον Κυβερνοχώρο.

3.3 Πλαίσια Κυβερνοασφάλειας και σύγκριση με το NIST CSF

Το παραπάνω πλάνο διαχείρισης της κυβερνοασφάλειας έχει αναπτυχθεί βάση των εξής πλαισίων:

- IMO Resolution MSC.428(98)
- The Guidelines on Cyber Security onboard Ships-BIMCO
- USCG Cyber Bulletins
- UK Cyber Security Code of Practice for ships
- EU Regulation 2016/679

3.3.1 IMO Guidelines – Ολοκληρωμένοι - χρήσιμοι Οδηγοί από τον IMO

Η ναυτιλιακή βιομηχανία, αρχικά απρόθυμη να αναγνωρίσει την απειλή των κυβερνοεπιθέσεων, πλέον αντιλαμβάνεται τη σοβαρότητα του κινδύνου και αναλαμβάνει δράση για την προστασία της. Στις 16 Ιουνίου 2016, ο IMO δημοσίευσε τις "Ενδιάμεσες Οδηγίες για τη Διαχείριση Κινδύνων Κυβερνοχώρου στη Ναυτιλία", που αποσκοπούν στην προστασία της ναυτιλίας από τρέχουσες και μελλοντικές απειλές. Αυτές οι οδηγίες αντικαταστάθηκαν το 2017 με ένα πιο ολοκληρωμένο σχέδιο, με τίτλο "Measures to Enhance Marinetime Security”1 που επικεντρώνεται στην ανάγκη για αποτελεσματική διαχείριση των κινδύνων κυβερνοχώρου (cyber risk management) και τονίζει τη σημασία της τεχνολογίας για την ασφαλή λειτουργία των ναυτιλιακών συστημάτων. Ο IMO παρέχει ένα γενικό πλαίσιο και ενθαρρύνει κάθε εταιρεία να καθορίσει τα κατάλληλα μέτρα για την κυβερνοασφάλειά της. Το έγγραφο των ΗΠΑ τον Απρίλιο του 2017 επισήμανε ότι η ανεπαρκής κυβερνοασφάλεια μπορεί να απειλήσει την ασφάλεια των πλοίων και πρότεινε μια ολιστική προσέγγιση στη διαχείριση των κινδύνων, ενσωματώνοντας τους κινδύνους του κυβερνοχώρου στο υπάρχον σύστημα ασφαλείας των πλοίων. Η αξιολόγηση και διαχείριση αυτών των κινδύνων θα πρέπει να γίνεται σύμφωνα με τον Διεθνή Κώδικα Διαχείρισης Ασφάλειας (ISM). Το MSC 98/5/2, το MSC.1/Circ.1526 και το MSC-FAL.1/Circ.3 έθεσαν γερά θεμέλια για την ενίσχυση της κυβερνοασφάλειας και η συμβολή τους θα μπορούσε να χαρακτηριστεί από τη ναυτιλιακή βιομηχανία ως το πρώτο βήμα στην αντιμετώπιση των κυβερνοεπιθέσεων [89].

3.3.2 The Guidelines on Cybersecurity onboard Ships-BIMCO

Το BINCO cyberSecurity framework είναι ένα πλάνο για την προστασία της πληροφορικής υποδομής της ναυτιλίας από cyber threats. Το framework βασίζεται στα principe της International Marinetime Organization (IMO) και έχει αναπτυχθεί ειδικά για τους τομέα της ναυτιλίας [55].

Κεντρικές αρχές του πλαίσιου BINCO:

1. Προσαφικότητα: Είναι σχεδιασμένο για να είναι εύκολη στην εφαρμογή και στον τομέα της ναυτιλίας.

2. Προσαρμοσμένο: Κατάλληλα φτιαγμένες ειδικά για τους τομέα της ναυτιλίας, λαμβάνοντας υπόψη τις ιδιαίτερες ανάγκες και περιοχές του τομέα.
3. Ολιστικό: Συμπεριλαμβάνει όλους τους τομείς της πληροφορικής υποδομής, από τα ΤΠ μέχρι και τα ΛΤ συστήματα.
4. Βασισμένο σε κινδύνους: Βασίζεται στην αξιολόγηση των κινδύνων και στην ανάπτυξη στρατηγικών για την αντιμετώπιση τους.
5. Συνεχής βελτίωση: Προβλέπει συνεχείς αναθεωρήσεις και βελτιώσεις του πλαισίου.

Κλειδιά στοιχεία του BINCO πλαισίου:

- Σαρωτική αναγνώριση και απάντηση σε cyber threats
- Προστασία των πληροφορικών υποδομών
- Συνεχής εκπαίδευση και κατάρτιση του προσωπικού
- Διαφύλαξη των δεδομένων
- Συνεργασία μεταξύ των εταίρων και των φορέων

Σύγκριση με το NIST CSF :
Ο BINCO framework είναι πιο ειδικός και προσαρμοσμένος στον τομέα της ναυτιλίας σε σχέση με το NIST CSF. Ο BINCO:

- Καταλληλίζει ειδικά τις ανάγκες της ναυτιλίας
- Περιλαμβάνει ειδικά μέτρα για τα ΟΤ συστήματα
- Προσαρμόζεται καλύτερα στις ιδιαίτερες συνθήκες της ναυτιλίας

Ωστόσο, ο BINCO framework βασίζεται στα ίδια γενικά αρχιτεκτονικά στοιχεία όπως το NIST CSF, συμπεριλαμβανομένης της αρχιτεκτονικής πληροφορικών συστημάτων και των μέτρων ασφάλειας δικτύου.
Ο BINCO framework προτείνει επίσης την εφαρμογή των οδηγιών του International Marinetime Organization (IMO) για τη cyberSecurity, οι οποίες είναι πιο ειδικές για τον τομέα της ναυτιλίας σε σχέση με άλλες διεθνείς οδηγίες.
Συνολικά, ο BINCO framework παρέχει ένα προσαρμοσμένο πλάνο για την προστασία της πληροφορικής υποδομής στη ναυτιλία, λαμβάνοντας υπόψη τις ιδιαίτερες ανάγκες και περιοχές του τομέα.

3.3.3. Marinetime Transportation Security Act (MTSA) [90]

Το Σχέδιο Ασφάλειας MTSA Σκοπός του Σχεδίου Ασφάλειας είναι να αποτυπώσει τα ισχύοντα μέτρα ασφάλειας, τις διαδικασίες και άλλες αρμοδιότητες που θα αποτρέψουν τα τρωτά σημεία. Το σχέδιο ασφάλειας μπορεί να περιλαμβάνει:

- Ευθύνες και καθήκοντα των CSOs, FSOs, VSOs
- Απαιτήσεις κατάρτισης
- Απαιτήσεις TWIC
- Απαιτήσεις ασκήσεων και ασκήσεων
- Απαιτήσεις τήρησης αρχείων
- Συντήρηση εξοπλισμού ασφαλείας και επικοινωνιών

- Δήλωση διαδικασιών ασφαλείας (DoS)
- Απαιτήσεις για ελέγχους και τροποποιήσεις

• Facility Security Officer (FSO)
– The person designated as responsible for the development, implementation, revision and maintenance of the FSP; liaison to the Coast Guard COTP and Company and Vessel Security Officers.
• Vessel Security Officer (VSO) FSO
– The person onboard the vessel, accountable to the Master, designated by the company as responsible for Security of the vessel, including implementation and maintenance of the VSP; liaison with the FSO and the vessel's CSO.
• Το ΠιστοποιητIκό Αναγνώρισης Εργαζομένων στIς Μεταφορές (TWIC)
- Το TWIC είναι ένα πιστοποιητικό αναγνώρισης για όλο το προσωπικό που απαιτεί πρόσβαση χωρίς συνοδεία σε ασφαλείς περιοχές εγκαταστάσεων και πλοίων που υπόκεινται σε ρυθμίσεις MTSA.
- Στα άτομα που πληρούν τις απαιτήσεις επιλεξιμότητας TWIC θα εκδοθεί ένα ανθεκτικό στην παραποίηση διαπιστευτήριο που περιέχει το βιομετρικό στοιχείο του εργαζομένου (πρότυπο δακτυλικού αποτυπώματος), ώστε να είναι δυνατή η θετική σύνδεση μεταξύ της κάρτας και του ατόμου.
- Η κατοχή TWIC δεν εγγυάται πρόσβαση. Το άτομο πρέπει να έχει εξουσιοδότηση πρόσβασης σε ρυθμιζόμενες περιοχές.
- Η TWIC είναι μια πρωτοβουλία που διαχειρίζεται η Διοίκηση Ασφάλειας Μεταφορών (TSA).
Όλα τα πρόσωπα που χρειάζονται πρόσβαση UNESCORTED σε εγκαταστάσεις και σκάφη που υπόκεινται σε ρυθμίσεις MTSA, όπως εφαρμόζεται στο σχέδιο ασφαλείας, χρειάζονται TWIC. Παραδείγματα: Οδηγοί φορτηγών, λιμενεργάτες, εμπορικοί ναυτικοί, εργολάβοι κ.λπ.

3.3.4 USCG Cyber Bulletins [91]

Οι USCG Cyber Bulletins (UnITed States Coast Guard) αποτελούν πολύτιμο εργαλείο για την κυβερνοασφάλεια στον ναυτιλιακό τομέα, προσφέροντας εξειδικευμένες οδηγίες και προτάσεις που ανταποκρίνονται στις μοναδικές ανάγκες της ναυτιλίας. Αυτή η εξειδίκευση τα καθιστά πιο κατάλληλα σε σχέση με γενικές οδηγίες κυβερνοασφάλειας, που συνήθως δεν ανταποκρίνονται πλήρως στις ιδιαιτερότητες του κλάδου.

Τα Cyber Bulletins λειτουργούν συμπληρωματικά προς το πλαίσιο του Marinetime Transportation Security Act (MTSA), παρέχοντας στοχευμένες κατευθύνσεις για την αντιμετώπιση των απειλών στον κυβερνοχώρο ειδικά για τη ναυτιλία. Αυτή η εναρμόνιση με το MTSA ενισχύει την προστασία των πληροφοριακών συστημάτων και την ασφάλεια των λειτουργιών στον ναυτιλιακό τομέα.
Μια επιπλέον σημαντική διάσταση είναι η εστίαση στα συστήματα Operational Technology (OT), τα οποία αποτελούν κρίσιμα στοιχεία για την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων. Αυτή η έμφαση είναι καίρια για την προστασία των επιχειρησιακών λειτουργιών.
Τέλος, οι Bulletins παρέχουν τακτική ενημέρωση για τις τελευταίες απειλές στον κυβερνοχώρο και τις βέλτιστεςπρακτικές, επιτρέποντας στους ναυτιλιακούς φορείς να αντιδρούν έγκαιρα στις νέες προκλήσεις και να διατηρούν την κυβερνοασφάλειά τους σε υψηλά επίπεδα.

3.3.5 UK Cyber Security Code of Practice for ships

Το UK Cyber Security Code of Practice for Ships, που εκδόθηκε το 2017, αποτελεί ένα σημαντικό εργαλείο για την προστασία της ναυτιλίας από cyber threats. Αυτό το κείμενο έχει σχεδιαστεί ειδικά για τους τομείς της ναυτιλίας και λαμβάνει υπόψη τις ιδιαίτερες ανάγκες και περιοχές του τομέα.

Μια βασική διαφορά αυτού του πλαισίου είναι η στενή συνεργασία με τις διεθνείς οδηγίες της International Marinetime Organization (IMO). Το κείμενο προτείνει συγκεκριμένες βέλτιστεςπρακτικές και οδηγίες που είναι πλήρως βασισμένες πάνω στις ήδη υπάρχουσες IMO κατευθυντήριες γραμμές. Το κείμενο επίσης προτείνει μια σαρωτική ανάλυση για την αναγνώριση και ανίχνευση των κυβερνο-απειλών. Αυτό είναι ιδιαίτερα σημαντικό για τους τομείς της ναυτιλίας που έχουν περιορισμένη ανθεκτικότητα σε επιθέσεις. Προτείνει συνεχείς αναθεωρήσεις και βελτιώσειςτου πλαισίου κυβερνο-ασφάλειας, λαμβάνοντας υπόψη τις εξελίξεις στις κυβερνο-απειλών και τις νέες τεχνολογίες [92].

Κέντρο επιχειρήσεων ασφαλείας (SOC):
Ένα SOC λειτουργεί ως κεντρική μονάδα που ασχολείται με θέματα ασφάλειας που επηρεάζουν την κυβερνο-φυσική συστήματα σε ένα πλοίο ή σε ένα στόλο πλοίων ή σε ένα πλοίο, συμπεριλαμβανομένων εκείνων που σχετίζονται με τον κυβερνοχώρο. ασφάλεια. Μπορεί να αποτελεί μέρος του επιχειρησιακού κέντρου μιας εταιρείας που επιβλέπει τη λειτουργία ενός αριθμού πλοίων, συμπεριλαμβανομένης της διαχείρισης της επιχειρησιακής συνέχειας και της καταστροφής αποκατάστασης.
Σημείωση: Η φύση ή η κλίμακα οποιουδήποτε SOC θα εξαρτηθεί από το μέγεθος και τη φύση του πλοίου και/ή στόλου. Σε περίπτωση που η εταιρεία διαθέτει υφιστάμενο κέντρο επιχειρήσεων, το SOC μπορεί να αποτελεί μέρος του και θα πρέπει να αντιμετωπίζει την ασφάλεια με ολιστικό τρόπο, δηλαδή να περιλαμβάνει το προσωπικό, φυσική και κυβερνοασφάλεια. Οι βασικές λειτουργίες ενός SOC, είναι οι εξής:
(α) να παρατηρεί, διατηρώντας επίγνωση της κατάστασης, δηλαδή να κατανοεί τις πιθανές, αναδυόμενες και πραγματικές απειλές για τις λειτουργίες του πλοίου. Η παρατήρηση περιλαμβάνει την ανίχνευση μη εξουσιοδοτημένων αλλαγών στα συστήματα του πλοίου ή στα δεδομένα του πλοίου, μη ασφαλών τρόπων λειτουργίας και μη εξουσιοδοτημένη πρόσβαση σε περιουσιακά στοιχεία του πλοίου.
(β) προσανατολισμός, με την ανάλυση του κινδύνου για τις επιχειρήσεις από νέες ή μεταβαλλόμενες απειλές και προσδιορισμό του κατά πόσον απαιτούνται προληπτικά μέτρα για τη μείωση του κινδύνου σε μια αποδεκτό επίπεδο.
(γ) αποφασίζει ποια ενέργεια μπορεί να είναι κατάλληλη είτε για να αρνηθεί περαιτέρω πρόσβαση στο πλοίο περιουσιακού στοιχείου είτε να ανταποκριθεί στο συμβάν προσδιορίζοντας τους κατάλληλους ελέγχους ασφαλείας.
(δ) ενεργεί, εφαρμόζοντας την απόφαση (τις αποφάσεις).

3.3.6 EU Regulation 2016/679 [93]

Η προστασία προσωπικών δεδομένων στη ναυτιλία απαιτεί μια ολιστική προσέγγιση κυβερνοασφάλειας, που ενσωματώνει τον προγραμματισμό προστασίας από την αρχή (privacy by design) και προεπιλεγμένες πολιτικές ασφάλειας (privacy by default) για όλα τα δεδομένα προσωπικής φύσης. Αυτό σημαίνει ότι η προστασία πρέπει να σχεδιάζεται και να εφαρμόζεται από την αρχή και όχι ως μεταγενέστερη προσθήκη. Επιπλέον, η συλλογή και επεξεργασία δεδομένων πρέπει να περιορίζεται στα απολύτως απαραίτητα για τις ναυτιλιακές λειτουργίες, τηρώντας το θεμελιώδες δικαίωμα της ελάχιστης επεξεργασίας δεδομένων που προβλέπει ο GDPR. Η διαφάνεια είναι απαραίτητη, ώστε να διασφαλίζεται ότι οι χρήστες ενημερώνονται για

τη συλλογή και χρήση των δεδομένων τους και ότι παρέχουν τη συναίνεσή τους όπου απαιτείται. Για λειτουργίες υψηλού κινδύνου, όπως η παρακολούθηση πλοίων, είναι υποχρεωτικές οι εκτιμήσεις αντικτύπου προστασίας δεδομένων (DPIA) για τον εντοπισμό και τη μείωση πιθανών κινδύνων. Εάν υπάρξει παραβίαση δεδομένων, το σχέδιο πρέπει να προβλέπει την άμεση ενημέρωση των ενδιαφερόμενων ατόμων και των αρμόδιων αρχών. Η συμμόρφωση με τα δικαιώματα των ατόμων, όπως το δικαίωμα πρόσβασης και διαγραφής, πρέπει να είναι διασφαλισμένη, ενώ για διεθνείς μεταφορές δεδομένων, το σχέδιο πρέπει να συμμορφώνεται με τις απαιτήσεις του GDPR. Απαιτείται επίσης σαφής καθορισμός ρόλων και ευθυνών για την υλοποίηση του πλάνου κυβερνοασφάλειας, καθώς και η διατήρηση αρχείων δραστηριοτήτων για την υποστήριξη της συμμόρφωσης. Αυτές οι αρχές διασφαλίζουν ότι το σχέδιο κυβερνοασφάλειας όχι μόνο προστατεύει από τις διαδικτυακές απειλές, αλλά και συμμορφώνεται με τις ευρωπαϊκές ρυθμίσεις για την προστασία δεδομένων, κάτι κρίσιμο για τις ναυτιλιακές εταιρείες που δραστηριοποιούνται στην ΕΕ.

3.3.7 ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, είναι ο οργανισμός της Ένωσης που αποσκοπεί να διασφαλίσει υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη.

Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΙΤΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο.
Η υιοθέτηση του CSF του NIST επέτρεψε στη ναυτιλιακή βιομηχανία να αντιμετωπίσει καλύτερα απειλές στον κυβερνοχώρο, να ενισχύσει τις στρατηγικές διαχείρισης κινδύνων και να προστατεύσει κρίσιμα περιουσιακά στοιχεία των επιχειρήσεων. Παρέχει ένα εκτεταμένο πλαίσιο που βοηθά τις εταιρείες στην ανάπτυξη ισχυρών λύσεων κυβερνοασφάλειας προσαρμοσμένων στις ιδιαίτερες ανάγκες τους, γι' αυτό και το συνιστά ο IMO. Με την ευθυγράμμιση με το CSF του NIST, η ναυτιλιακή βιομηχανία μπορεί να ενισχύσει τη στάση της στον τομέα της κυβερνοασφάλειας και να προωθήσει ένα πιο ασφαλές και ανθεκτικό περιβάλλον για τις ναυτιλιακές επιχειρήσεις. Έτσι, όλα τα πλαίσια κυβερνοασφάλειας για την ναυτιλία έχουν πάρει πολλαπλά στοιχεία και αυτούσια κομμάτια από το NIST CSF.

3.4 Σύνοψη του 3ου Κεφαλαίου

Στην 3η Ενότητα παρήχα μια λεπτομερή διερεύνηση των πρακτικών κυβερνοασφάλειας ειδικά για τη ναυτιλιακή βιομηχανία, με έμφαση στη διαχείριση κινδύνων, την προστασία πολιτικών και τον σχεδιασμό έκτακτης ανάγκης στις ναυτιλιακές εταιρείες, παραθέτοντας στοιχεία και πληροφορίες μέσα από το ιδιωτικό-εμπιστευτικό για την εταιρία «CYBER SECURITY MANAGEMENTPLAN». Το κεφάλαιο δίνει έμφαση στην πολύπλοκη διασύνδεση των συστημάτων επιχειρησιακής τεχνολογίας (OT) και πληροφορικής (IT) στο ναυτιλιακό περιβάλλον, αναδεικνύοντας τις ευπάθειές τους σε κυβερνοεπιθέσεις. Περιγράφονται οι βασικές πτυχές του πλαισίου κυβερνοασφάλειας, συμπεριλαμβανομένων στρατηγικών για τον μετριασμό των κινδύνων, την προστασία των κρίσιμων λειτουργιών και την εφαρμογή σχεδίων απόκρισης και ανάκαμψης για πιθανά περιστατικά. Επιπλέον, το κεφάλαιο υπογραμμίζει την ανάγκη οι ναυτιλιακές εταιρείες να θεσπίσουν ολοκληρωμένα πρωτόκολλα κυβερνοασφάλειας που να συμμορφώνονται με διεθνείς κανονισμούς, όπως αυτοί του IMO και της BIMCO, πρωτόκολλα τα οποία έχουν επηρεαστεί βαθιά από το πλαίσιο κυβερνοασφάλειας NIST. Τέτοια μέτρα είναι απαραίτητα για τη διασφάλιση ευαίσθητων πληροφοριών και τη διατήρηση της επιχειρησιακής συνέχειας. Η ενσωμάτωση πλαισίων όπως το Πλαίσιο Κυβερνοασφάλειας (CSF) του NIST αποτελεί μια βιώσιμη πορεία για την ενίσχυση αυτών των μέτρων, υποστηρίζοντας τις εταιρείες στον εντοπισμό, την προστασία, την ανίχνευση και την αντίδραση στις απειλές στον κυβερνοχώρο, ενώ παράλληλα ενισχύει τη συνολική ανθεκτικότητα έναντι όλο και πιο εξελιγμένων επιθέσεων.

4. Κυβερνοασφάλεια NIST

4.1 Σύνοψης της μελέτης

Η παρούσα πτυχιακή εργασία εξετάζει την εφαρμογή του πλαισίου κυβερνοασφάλειας του NIST (NIST CyberSecurity Framework – CSF) στον τομέα της ναυτιλίας, με στόχο την προστασία των κρίσιμων ναυτιλιακών συστημάτων τόσο της Πληροφορικής (IT) όσο και των Λειτουργικών Τεχνολογιών (OT). Καθώς η ναυτιλιακή βιομηχανία εξαρτάται ολοένα και περισσότερο από τις τεχνολογίες πληροφορικής και επικοινωνιών για πλοήγηση, επικοινωνία και διαχείριση logistics, η εργασία αυτή εστιάζει στις ιδιαίτερες προκλήσεις κυβερνοασφάλειας που αντιμετωπίζουν οι ναυτιλιακές εταιρείες, καθώς και στην αναγκαιότητα εφαρμογής ενός αξιόπιστου πλαισίου όπως το NIST CSF για την προστασία από απειλές στον κυβερνοχώρο.

Η πρώτη Ενότητα παρέχει μια εισαγωγή και ιστορική αναδρομή του NIST (National Instituteof Standards and Technology) και την εξέλιξή του στον τομέα των προτύπων ασφαλείας. Αναλύονται οι βασικοί στόχοι και στοιχεία του πλαισίου, ενώ εξετάζεται η σημασία του NIST CSF για τη ναυτιλιακή βιομηχανία, καθώς και οι υποδομές και τεχνολογίες που ενσωματώνονται στον τομέα. Το κεφάλαιο ολοκληρώνεται με την ανάλυση των ιδιαίτερων κυβερνοαπειλών που αντιμετωπίζουν τα ναυτιλιακά συστήματα, τονίζοντας τα τρωτά σημεία που προκύπτουν λόγω της διασύνδεσης μεταξύ των OT και IT συστημάτων.

Στην δεύτερη Ενότητα, η εργασία εξετάζει τη μεθοδολογία αξιολόγησης και μετρίασης κινδύνου που προτείνεται από το NIST CSF, καθώς και τα ειδικά χαρακτηριστικά του πλαισίου που το καθιστούν προσαρμόσιμο στις ανάγκες της ναυτιλίας. Στην ενότητα αυτή περιγράφονται οι βασικές λειτουργίες του πλαισίου, οι οποίες περιλαμβάνουν τον εντοπισμό (Identify), την προστασία (PrOTect), την ανίχνευση (Detect), την απόκριση (Respond) και την ανάκτηση (Recover). Η ενότητα επίσης παρουσιάζει στατιστικά και παραδείγματα επιθέσεων στον τομέα της ναυτιλίας, υπογραμμίζοντας τη σημασία της προληπτικής στρατηγικής για την προστασία των κρίσιμων συστημάτων από περιστατικά κυβερνοεπιθέσεων.

Η Ενότητα 3, είναι αφιερωμένη στην πρακτική εφαρμογή του NIST CSF στις ναυτιλιακές εταιρείες, περιλαμβάνοντας λεπτομερή στοιχεία από μια πραγματική εταιρεία. Μέσα από αυτή την ανάλυση, γίνεται σαφές πως το πλαίσιο αυτό μπορεί να προσφέρει ολοκληρωμένη υποστήριξη για τη διαχείριση κινδύνων, την ανάπτυξη πολιτικών προστασίας και την εφαρμογή σχεδίων έκτακτης ανάγκης. Συγκρίνονται, επίσης, το NIST CSF με άλλα πλαίσια κυβερνοασφάλειας, υποδεικνύοντας τα πλεονεκτήματα του NIST για τη ναυτιλιακή βιομηχανία, όπως η προσαρμοστικότητα και η αποτελεσματικότητα στην ενίσχυση της ανθεκτικότητας απέναντι σε απειλές.

Συμπεράσματα

Η μελέτη μου επικεντρώθηκε στην εφαρμογή του πλαισίου κυβερνοασφάλειας NIST (CSF) στη ναυτιλιακή βιομηχανία, επιδιώκοντας την ενίσχυση της προστασίας των κρίσιμων τεχνολογικών συστημάτων Πληροφορικής (IT) και Λειτουργικής Τεχνολογίας (OT) των ναυτιλιακών εταιρειών. Λαμβάνοντας υπόψη την αυξανόμενη εξάρτηση της ναυτιλίας από τις διασυνδεδεμένες τεχνολογίες για πλοήγηση, επικοινωνία και εφοδιαστική, κατέληξα ότι η ύπαρξη αποτελεσματικών μέτρων ασφάλειας είναι ζωτικής σημασίας για τη διατήρηση της επιχειρησιακής συνέχειας και τη συμμόρφωση με τους διεθνείς κανονισμούς. Η έρευνά μου ανέδειξε ότι το NIST CSF παρέχει ένα ολοκληρωμένο σύνολο βέλτιστωνπρακτικών, που βοηθούν στον εντοπισμό των κινδύνων, την προστασία των συστημάτων, την έγκαιρη ανίχνευση απειλών, και την αποτελεσματική απόκριση σε περιστατικά, ενώ παράλληλα συμβάλλει στην ανθεκτικότητα του οργανισμού σε ένα διαρκώς μεταβαλλόμενο ψηφιακό περιβάλλον. Επεκτείνοντας τα συμπεράσματά μου σχετικά με την επένδυση στο πλαίσιο κυβερνοασφάλειας NIST CSF, είναι σαφές ότι το πλαίσιο αυτό δεν περιορίζεται απλώς σε μία σειρά τεχνικών οδηγιών ή μέτρων προστασίας. Αντίθετα, προσφέρει στις ναυτιλιακές επιχειρήσεις μια ολιστική προσέγγιση στη διαχείριση των κυβερνοκινδύνων, προσαρμόζοντας τις αρχές και τις πρακτικές του σε διαφορετικά μεγέθη και δομές οργανισμών. Η έρευνά μου επιβεβαιώνει ότι η χρήση του NIST CSF ενισχύει την ανθεκτικότητα των ναυτιλιακών συστημάτων έναντι απειλών, καθώς καλύπτει ολοκληρωμένα και σε βάθος τα στάδια της αναγνώρισης, της προστασίας, της ανίχνευσης, της απόκρισης και της αποκατάστασης. Παράλληλα, μέσω της ενσωμάτωσης του NIST CSF, οι ναυτιλιακές εταιρείες αποκτούν αυξημένη ικανότητα παρακολούθησης και ανταπόκρισης σε περιστατικά, ενώ μπορούν να αντιμετωπίζουν πιο αποτελεσματικά τις επιπτώσεις κυβερνοεπιθέσεων στην επιχειρησιακή συνέχεια. Η επένδυση σε αυτό το πλαίσιο δημιουργεί ένα δυναμικό μοντέλο ασφάλειας που προσαρμόζεται στις ταχέως εξελισσόμενες ψηφιακές απειλές, ενισχύοντας όχι μόνο την ασφάλεια των δεδομένων, αλλά και την αξιοπιστία των λειτουργιών του πλοίου, την προστασία των εμπορικών συναλλαγών και την ασφάλεια των πληρωμάτων. Το NIST CSF βοηθά τις επιχειρήσεις να αναπτύξουν μια ισχυρή κουλτούρα ασφάλειας, εκπαιδεύοντας το προσωπικό και εδραιώνοντας σαφείς πολιτικές που μειώνουν τον κίνδυνο ανθρώπινου σφάλματος και βεΟΤιώνουν τη συμμόρφωση με διεθνείς κανονισμούς ασφαλείας. Επιπλέον, η μελέτη μου αναδεικνύει τη δυνατότητα του πλαισίου να λειτουργεί ως βασικό εργαλείο για τον συντονισμό με διεθνείς φορείς και ρυθμιστικές αρχές, προωθώντας την ασφάλεια στην παγκόσμια ναυτιλία. Οι πρακτικές και οι κατευθυντήριες γραμμές που εισάγει ενισχύουν τη διαλειτουργικότητα και τη συνεργασία μεταξύ των ναυτιλιακών οργανισμών, ενώ παράλληλα ενδυναμώνουν τη δυνατότητα αντιμετώπισης κυβερνοαπειλών που μπορούν να θέσουν σε κίνδυνο τις διασυνοριακές εφοδιαστικές αλυσίδες. Συμπερασματικά, το NIST CSF αποτελεί όχι μόνο ένα πολύτιμο μέσο για την άμεση προστασία των ναυτιλιακών συστημάτων, αλλά και έναν κρίσιμο παράγοντα για την επίτευξη μιας συνολικής ασφάλειας που ενισχύει την ανταγωνιστικότητα και τη βιωσιμότητα των ναυτιλιακών εταιρειών σε ένα ευρύτερο και πλέον αλληλεξαρτώμενο ψηφιακό περιβάλλον. Η μελέτη περιλάμβανε επίσης συγκριτική ανάλυση με άλλα πλαίσια κυβερνοασφάλειας, καταδεικνύοντας ότι το NIST CSF υπερέχει σε προσαρμοστικότητα και διαχειριστική αποτελεσματικότητα, καθιστώντας το κατάλληλο για ναυτιλιακές εταιρείες κάθε μεγέθους. Επιπλέον, μέσω πρακτικής εφαρμογής σε πραγματική ναυτιλιακή εταιρεία, ανέδειξα την αξία του NIST CSF στην ανάπτυξη στρατηγικών διαχείρισης κινδύνων και έκτακτης ανάγκης, που είναι απαραίτητες για την προστασία έναντι κυβερνοεπιθέσεων. Τα συμπεράσματα αυτά ενισχύουν την άποψη ότι η επένδυση σε ολοκληρωμένα πλαίσια κυβερνοασφάλειας, όπως το NIST CSF, είναι κρίσιμη για τη βιωσιμότητα και την ασφαλή λειτουργία των ναυτιλιακών εταιρειών, προστατεύοντας τα δεδομένα και τις διαδικασίες τους από εξελιγμένες κυβερνοαπειλές.

Πίνακας ορολογίας

Ορολογίες στα Αγγλικά :

Cybersecurity	The practice of protecting systems, networks, and programs from digital attacks.
NIST CSF	A framework developed by NIST to improve cybersecurity risk management.
Risk Assessment	The process of identifying, evaluating, and prioritizing risks to cybersecurity.
Vulnerability	A weakness in a system that can be exploited by threats to gain unauthorized access.
Threat	A potential cause of an unwanted incident that may harm a system or organization.
Incident Response Plan	A set of instructions to detect, respond to, and recover from cybersecurity incidents.
Encryption	The process of converting data into a coded format to prevent unauthorized access.
Authentication	The process of verifying the identity of a user or system.
Multi-Factor Authentication	A security process that requires two or more authentication factors.
Phishing	A type of cyberattack where attackers trick users into revealing sensitive information.
Malware	Malicious software designed to damage, disrupt, or gain unauthorized access to systems.
Firewall	A network security device that monitors and controls incoming and outgoing traffic.
Zero Trust Architecture	A security model that assumes no trust for users inside or outside the network.
Security Operations Center (SOC)	A centralized unit that monitors and analyzes cybersecurity incidents in real time.
Patch Management	The process of managing updates to software to fix vulnerabilities or bugs.

Ορολογίες στα Ελληνικά :

Κυβερνοασφάλεια	Η πρακτική προστασίας συστημάτων, δικτύων και προγραμμάτων από ψηφιακές επιθέσεις.
Πλαίσιο NIST CSF	Ένα πλαίσιο που αναπτύχθηκε από το NIST για τη βελτίωση της διαχείρισης κινδύνων κυβερνοασφάλειας.
Αξιολόγηση Κινδύνου	Η διαδικασία αναγνώρισης, αξιολόγησης και προτεραιοποίησης κινδύνων στην κυβερνοασφάλεια.
Ευπάθεια	Μια αδυναμία σε σύστημα που μπορεί να εκμεταλλευτεί μια απειλή για μη εξουσιοδοτημένη πρόσβαση.
Απειλή	Πιθανή αιτία ενός ανεπιθύμητου περιστατικού που μπορεί να βλάψει σύστημα ή οργανισμό.
Σχέδιο Αντιμετώπισης Περιστατικών	Ένα σύνολο οδηγιών για την ανίχνευση, αντιμετώπιση και αποκατάσταση κυβερνοεπιθέσεων.
Κρυπτογράφηση	Η διαδικασία μετατροπής δεδομένων σε κωδικοποιημένη μορφή για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
Αυθεντικοποίηση	Η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη ή συστήματος.
Πολυπαραγοντική Αυθεντικοποίηση	Μια διαδικασία ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης.
Φίσινγκ	Μια μορφή κυβερνοεπίθεσης όπου οι επιτιθέμενοι ξεγελούν χρήστες για να αποκαλύψουν ευαίσθητες πληροφορίες.
Κακόβουλο Λογισμικό	Κακόβουλο λογισμικό που έχει σχεδιαστεί για να προκαλέσει ζημιά ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα.
Τείχος Προστασίας	Μια συσκευή ασφαλείας δικτύου που ελέγχει την εισερχόμενη και εξερχόμενη κίνηση.
Αρχιτεκτονική Zero Trust	Ένα μοντέλο ασφάλειας που δεν εμπιστεύεται κανέναν χρήστη εντός ή εκτός του δικτύου.
Κέντρο Επιχειρήσεων Ασφαλείας (SOC)	Ένα κεντρικό τμήμα που παρακολουθεί και

	αναλύει περιστατικά κυβερνοασφάλειας σε πραγματικό χρόνο.
Διαχείριση Ενημερώσεων	Η διαδικασία διαχείρισης ενημερώσεων λογισμικού για την επιδιόρθωση ευπαθειών ή σφαλμάτων.

Πίνακας αρκτικόλεξων-ακρωνυμίων

Αγγλικά Ακρωνύμια:

Πίνακας Συντομογραφιών	
AIS	Automatic Identification System
ALARP	As Low As Reasonably Practicable
BWS	Ballast Water System
CAIC	Control, Availability, Integrity, and Confidentiality
CIA	Confidentiality, Integrity, and Availability
CSF	CyberSecurity Framework
DE	Detection
ECDIS	Electronic Chart Display and Information System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GPS	Global Positioning System
GV.SC	Governance Supply Chain
ICS	Industrial Control Systems
ID.AM	Asset Management
ID.IM	Information Management
IMO	International Marinetime Organization
INS	Integrated Navigation System
IOT	Internet of Things
ISCM	Information Security Continuous MonIToring
ISM	International Safety Management
ISO	International Organization for Standardization
IT	Information Technology
MITM	Man-In-The-Middle
MTSA	Marine time Transportation Security Act
NIST	National Instituteof Standards and Technology
OT	Operational Technology
PKI	Public Key Infrastructure
PR	Protection
PR.AA	Access Control
RADAR	Radio Detection and Ranging
RMF	Risk Management Framework
RF	Radio Frequency
SMB	Server Message Block
SMS	Short Message Service

SP	Special Publication
TTP	Tactics, Techniques, and Procedures
VOIP	Voice Over Internet Protocol
VSAT	Very Small Aperture Terminal
WLAN	Wireless Local Area Network

Ελληνικά Ακρωνύμια:

Πίνακας Συντομογραφιών	
ΑΣΑ	Αυτόματο Σύστημα Αναγνώρισης
ΟΧΕΛΕ	Όσο Χαμηλά Είναι Λογικά Εφικτό
ΣΝΕ	Σύστημα Νερού Έρματος
ΕΔΑΕ	Έλεγχος, Διαθεσιμότητα, Ακεραιότητα και Εμπιστευτικότητα
ΕΑΔ	Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα
ΠΚΑ	Πλαίσιο Κυβερνοασφάλειας
Α	Ανίχνευση
ΗΟΧΠΣ	Ηλεκτρονική Οθόνη Χαρτών και Πληροφοριακό Σύστημα
ΟΠΕΠ	Ομοσπονδιακά Πρότυπα Επεξεργασίας Πληροφοριών
ΟΝΑΠ	Ομοσπονδιακός Νόμος για την Ασφάλεια Πληροφοριών
ΠΣΕΘ	Παγκόσμιο Σύστημα Εντοπισμού Θέσης
ΔΕΑ	Διακυβέρνηση Εφοδιαστικής Αλυσίδας
ΣΒΕ	Συστήματα Βιομηχανικού Ελέγχου
ΔΠΣ	Διαχείριση Περιουσιακών Στοιχείων
ΔΠ	Διαχείριση Πληροφοριών
ΔΝΟ	Διεθνής Ναυτιλιακός Οργανισμός
ΕΣΠ	Ενοποιημένο Σύστημα Πλοήγησης
ΔΙΤ	Διαδίκτυο των Πραγμάτων
ΣΠΑΠ	Συνεχής Παρακολούθηση Ασφάλειας Πληροφοριών
ΔΚΑΔ	Διεθνής Κώδικας Ασφαλούς Διαχείρισης
ΔΟΤ	Διεθνής Οργανισμός Τυποποίησης
ΙΤ	Τεχνολογία Πληροφοριών
ΑΣΜ	Άνθρωπος-Στη-Μέση
ΝΑΝΜ	Νόμος για την Ασφάλεια Ναυτιλιακών Μεταφορών
ΕΙΠΤ	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας
ΟΤ	Λειτουργική Τεχνολογία
ΥΔΚ	Υποδομή Δημόσιου Κλειδιού
Π	Προστασία
ΕΠ	Έλεγχος Πρόσβασης
ΡΕΕ	Ραδιοεντοπισμός και Εύρεση
ΠΔΚ	Πλαίσιο Διαχείρισης Κινδύνων
ΡΣ	Ραδιοσυχνότητα
ΜΜΔ	Μπλοκ Μηνυμάτων Διακομιστή
ΥΣΜ	Υπηρεσία Σύντομων Μηνυμάτων
ΕΕ	Ειδική Έκδοση
ΤΤΔ	Τακτικές, Τεχνικές και Διαδικασίες

Βιβλιογραφία

1.1 Πηγές:

[1] https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

[2] https://www.nist.gov/pao/nist-100-foundations-progress/founding-overview

[3] NIST Timeline - Significant Achievements

[4] https://www.nist.gov/cyberframework

[5] National Bureau of Standards και η ιστορική του εξέλιξη

[6] NIST Guidelines: a methodological underpinning for cyberSecurity analysts https://www.tarlogic.com/blog/nist-guidelines-cyberSecurity/

[7] What are the NIST Special Publications (SPs) 800 Series? October24, 2023: https://ipkeys.com/blog/nist-special-publications/

[8] NICCS:National Initiativefor CyberSecurity Careersand Studies https://niccs.cisa.gov/workforce-development/nice-framework

[9] Zero trust Architecturedesign principles https://www.ncsc.gov.uk/collection/zero-trust-architecture

[10] DigitalIdentityStandards https://www.enisa.europa.eu/publications/digital-identity-standards

[11] Cloud Computing https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[12] Comparison between NIST CyberSecurity Framework (CSF) and NIST SP 800-53 : https://www.6clicks.com/resources/comparisons/nist-cyberSecurity-framework-csf-vs-nist-sp-800- 53

1.2 Πηγές:

[13] Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls https://apps.dtic.mil/sti/trecms/pdf/AD1107339.pdf

[14] NIST Computer Security Resource Center. https://csrc.nist.gov/search?keywords=

[15] CyberSecurity Framework https://www.nist.gov/cyberframework

1.3 Πηγές:

[16] Dourmas, G., NikITakos, N., & Lambrou, M. (2005). The concept of Digitalbusiness ecosystems applied to the shipping industry. Proceedings international association of Marinetime economists 2005 conference, Cyprus.

[17] 2020 IEEE Symposium on Security and Privacy. A Tale of Sea and Sky On the Security

ofMarinetimeVSATCommunications
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152624

[18] ICS Security in Marinetime Transportation A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure July 2013 DOT-VNTSC-MARAD-13- 01 Prepared for: Office of Security Marinetime Administration U.S. Department of Transportation Washington, D.C. https://rosap.ntl.bts.gov/view/dOT/10057

[19] Ship to Shore https://www.borderlesshub.com/ship-to-shore

[20] wireless communications on automated charging systems in marine industry April 2020 : https://urn.fi/URN:NBN:fi:tuni-202004273954

[21] Ships infectedwith ransomware, USB malware, worms https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/

[22] S. Sethi, “Types of Governors for Engines Used On Ships,” 25 September 2020. https://www.marineinsight.com/tech/types-of-governors-for-engines-used-on-ships/

[23] B. Hyra, “Analyzing the Attack Surface of Ships,” Denmark, 2019.
https://orbit.dtu.dk/files/218483747/190401_Analyzing_the_Attack_Surface_of_Ships.pdf

[24] Priyanga Rajaram et al 2022 J. Phys.: Conf. Ser. 2311 012002DOI 10.1088/1742-6596/2311/1/012002

[25] Ship Automation & Control System https://www.shippipedia.com/ship-automation-control-system/

[26] Marine Heavy Fuel Oil (HFO) For Ships – Properties, Challenges and Treatment Methods https://www.marineinsight.com/tech/marine-heavy-fuel-oil-hfo-for-ships-properties-challenges-and-treatment-methods/

[27] Anish, “Different Types of Alarms on Ships,” 14 January2021 https://www.marineinsight.com/marine-safety/different-types-of-alarms-on-ship/.

[28] Karkosi ´nski, D.; Rosi ´nski, W.A.; Deinrych, P.; POTrykus, S. Onboard Energy Storage and Power Management Systems for All-Electric Cargo Vessel Concept. Energies 2021, 14, 1048. https://doi.org/10.3390/ en14041048

[29] Raising Awareness on Cyber Security of ECDIS. TRANSNAV, the International Journal on Marine Navigation and Safety of Sea Transportation Volume 13 Number 1 March 2019 DOI: 10.12716/1001.13.01.24

[30] Applications of high-frequency radar J. M. Headrick, J. F. Thomason First published: 01 July 1998 https://doi.org/10.1029/98RS01013

[31] M. B. M. K. DimITrios Dalaklis, “Vulnerabilities of the Automatic Identification System in the Era of Marinetime Autonomous Surface Ships,” in 9th NMIOTC Annual Conference (Fostering Projection of Stability through Marinetime Security: Achieving

Enhanced Capabilities and Operational Effectiveness), 2018
DOI: 10.13140/RG.2.2.14478.46408

[32] https://www.gps.gov/applications/marine/

[33] Mehrzadi, M.; Terriche, Y.; Su, C.-L.; OThman, M.B.; Vasquez, J.C.; Guerrero, J.M. Review of Dynamic Positioning Control in Marine time Microgrid Systems. Energies 2020, 13, 3188. https://doi.org/10.3390/en13123188

[34] Valčić, S.; Škrobonja, A.; Maglić, L.; Sviličić, B. GMDSS Equipment Usage: Seafarers' Experience. J. Mar. Sci. Eng. 2021, 9, 476. https://doi.org/10.3390/jmse9050476

[35] Svilicic, B.; Rudan, I.; Jugović, A.; Zec, D. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. J. Mar. Sci. Eng. 2019, 7, 364. https://doi.org/10.3390/jmse7100364

[36] Wikipedia, "Cargo control room," https://en.wikipedia.org/wiki/Cargo_control_room

[37] S. Lagouvardou, "Marinetime Cyber Security: concepts, problems and models," 2018. https://orbIT.dtu.dk/

1.4 Πηγές:

[38] IT vs. OT: Safeguarding Marine Terminals from Cyber Threats in the Age of Industry 4.0 https://tideworks.com/safeguarding-marine-terminals/

[39] IT vs OT Security: Key Differences In CyberSecurityhttps://claroty.com/blog/IT-and- OT-cyberSecurity-key-differences

[40] M. Wingrove, "Secure VSAT to prevent cyber attacks," 16 April 2020. https://www.rivieramm.com/news-content-hub/news-content-hub/secure-vsat-to- preventcyber-attacksnbsp-58986.

[41] M. Wingrove, "How to ensure VSAT modems cannot be hacked," 05 December 2019. https://www.rivieramm.com/news-content-hub/news-content-hub/ensurevsat-modems- cannot-be-hacked-57065

[42] R. Foggia, "CVE-2019-15652: SatLink VSAT Vulnerabilities," 21 November 2019. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cve-2019-15652- satlink-vsat-Vulnerabilities/.

[43] E. Robinson, "Hacked – a real life story of exploITing vessel VSAT," 25 May 2020 https://smartMarinetimenetwork.com/2020/05/25/hacked-a-real-life-story-ofexploITing-vessel-vsat/.

[44] C. McCraw, "12 VoIP Security Vulnerabilities and How to Fix Them," 06 May 2020 https://getvoip.com/blog/2020/05/06/voip-Security/.

[45] WebTITan, "Most Common Wireless Network Attacks," 19 April 2018 https://www.webtITan.com/blog/most-common-wireless-network-attacks/.

[46]M. Wingrove, "'Impregnable' radar breached in simulated cyber attack," 2018. [Online]. Available: https://www.rivieramm.com/news-content-hub/news-content-hub/impregnableradar-breached-in-simulated-cyber-attack-25158.

[47] Guidelines for cyber risk management in shipboard operational technology systems Priyanga Rajaram, Mark Goh, Jianying Zhou ITrust, Centre for Research in Cyber Security Singapore UniversITy of Technology and Design (SUTD) https://arxiv.org/pdf/2203.04072

[48] “Automatic Identification Systems (AIS), ITs BenefITs and Threats,” 2016 https://www.trendmicro.com/vinfo/us/Security/news/cybercrime-and-digITal-threats/faqautomatic- identification-systems-ais-benefITs-and-threats.

[49] D. G. S. R. Joseph DiRenzo, “The LITtle-known Challenge of Marinetime Cyber Security,” http://archive.dimacs.rutgers.edu/People/Staff/froberts/MarinetimeCyberSecurityCorfu7-5-15.pptx.pdf

[50] Connectivity, “Understanding GPS Spoofing in shipping: How to stay protected,” 2020. https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/

[51] D. A. Grant, “GPS Jamming and ITs impact on Marinetime navigation,” 10 May 2010. https://www.researchgate.net/publication/228897052_GPS_Jamming_and_the_Impact_on_Marineti me_Navigation#:~:text=The%20result%20of%20such%20interference,reacts%20to%20the%20jam ming%20incident.

[52] Hacking the Ship Scenario: An Offshore Supply Vessel's Dynamic Positioning System https://www.abs-group.com/Knowledge-Center/Insights/Hacking-the-Ship-Scenario-An-Offshore- Supply-Vessels-Dynamic-Positioning-System/

[53] Nettitude, “Marine and Offshore Cyber Briefing: Cyber Risks in Communication Systems,” https://cdn2.hubspOT.net/hubfs/3021880/Ebook%20PDFs/NETT_2019_M&O_CRCS_2019.pdf

[54] “STRIDE (Security),” 2021 https://en.wikipedia.org/wiki/STRIDE_(Security)

[55] Cyber Security Onboard Ships https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

[56] Exposed and vulnerable: Recent attacks highlight Critical need to protect internet-exposed OT devices https://www.microsoft.com/en-us/Security/blog/2024/05/30/exposed-and-vulnerable- recent-attacks-highlight-Critical-need-to-prOTect-internet-exposed-OT-devices/
1

2.1 Πηγές:

[57] Complete Guide to ΗλεκτρονΙκό ψάρεμα: Techniques & MITigations https://www.valimail.com/resources/guides/guide-to-phishing/#:~:text=Implement%20email%20Security%20software%20to,to%20test%20their%20phishing%20knowledge.

[58] D. C. M. P. C. D. David Maguire, “S/MIME for message signing and encryption,” 23 March 2021. https://docs.microsoft.com/en-us/exchange/policy-andcompliance/smime/smime?view=exchserver-2019.

[59] VSAsTer: Uncovering Inherent Security Issues in Current VSAT System Practices

https://mschloegel.me/paper/willbold2024vsaster.pdf

[60] “Cross-site scripting https://portswigger.net/web-Security/cross-sITescripting.

[61] VoIP Info, “What Is Telephony Denial of Service and How to Prevent IT,” 15 July 2019. [http://www.voipinfo.net/telephony-denial-of-service-and-how-to-preventIT/.

[62] J. Karasek, “Security 101: Protecting Wi-Fi Networks Against Hacking and Eavesdropping,” https://www.trendmicro.com/vinfo/fr/Security/news/cybercrime-and-digITal-threats/Security-101- prOTecting-wi-fi-networks-against-hacking-and-eavesdropping

[63] Managing Cyber Risk Supportfor Vessel Operators https://www.sperrymarine.com/media/jeilslgy/sperry-marine-cyber-risk-management-whITe-paper- issue-april-2021.pdf
[64] K. Munro, “Hacking Serial Networks on Ships,” 25 June 2018 https://www.pentestpartners.com/Security-blog/hacking-serial-networks-on-ships/.

[65] o. Developer, “How to Mitigate DoS Attacks https://developer.okta.com/books/api-Security/dos/how/.
[66] G. Weadock, “SMB Signing and Security,” 31 Jan 2010. https://www.networkworld.com/article/2229737/smb-signing-and-Security.html.
[67] “Overview of Server Message Block signing https://learn.microsoft.com/en- us/troubleshoOT/windows-server/networking/overview-server-message-block-signing

[68] “AIS Spoofing Detection with TDOA,” CRFS, https://www.crfs.com/blog/ais-Spoofing-detection-with-tdoa/.

[69] Kaspersky, “What Is a Replay Attack?,” https://www.kaspersky.com/resource- center/definITions/replay-attack.
[70] P. Marco Balduzzi and Kyle Wilhoite, “A Security Evaluation of AIS,” https://www.researchgate.net/publication/299466963_A_Security_evaluation_of_AIS_automated_i dentification_system

[71] M. A. F. S. A. K. S. M. A. U. A. Mukhtar Ahmad, “Impact and Detection of GPS Spoofing and Countermeasures against Spoofing,” 2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019 , 2019.
[72] “How to deal with GPS jamming and Spoofing,” CRFS, July 2020. https://www.crfs.com/blog/how-to-deal-with-gps-jamming-and-Spoofing/

[73] B. Martens, “What Is a Backdoor & How to Prevent Backdoor Virus Attacks in 2021,” SafetyDetectives, 31 May 2021. https://www.safetydetectives.com/blog/what-is-a-backdoor-and- how-to-prOTect-against-IT/.
[74] “Set up DKIM to prevent email Spoofing,” [https://support.google.com/a/answer/174124?hl=en

[75] R. Santamarta, “Marine time Security: Hacking into a Voyage Data Recorder (VDR),” IOActive, 9 December 2015 https://ioactive.com/Marinetime-Security-hacking-into-a-voyage-data- recorder-vdr/
[76] Dimakopoulou, A.; Rantos, K. Comprehensive Analysis of Marine time Cybersecurity

Landscape Based on the NIST CSF v2.0. J. Mar. Sci. Eng. 2024, 12, 919. https://doi.org/10.3390/jmse12060919
[77] IMO. Guidelines on Marine time Cyber Risk Management. MSC-FAL.1/Circ.3/Rev.2. https://www.imo.org/en/ OurWork/Security/Pages/Cyber-Security.aspx
[78] International Marinetime Organization. Marine time Cyber Risk Management in Safety ManagementSystems—ResolutionMSC.428(98).: https://www.imo.org/en/OurWork/Security/Pages/Cyber-Security.aspx
[79] International Association of Classification Societies. IACS Adopts New Requirements on Cyber Safety. https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

2.2 Πηγές:

[80] CSF 2.0 For industry, government, and organizations to reduce cyberSecurity risks https://doi.org/10.6028/NIST.CSWP.29
[81] National Instituteof Standards and Technology CyberSecurity Framework – NIST CSF Explained https://www.radiflow.com/OT-cyber-knowledge/national-instITute-of-standards- and-technology-cyberSecurity-framework/
[82] What is NIST CyberSecurity Framework 2.0? How Businesses Can Use NIST CSF? Author: SangforTechnologies Published Date : 27 Mar 2024 https://www.sangfor.com/glossary/cyberSecurity/what-is-nist-cyberSecurity-framework- csf-2-0

2.3 Πηγές:

[83] msc medITerranean shipping company s.a. -v- glencore international ag [2017] ewca civ 365 : https://www.hilldickinson.com/insights/articles/msc-medITerranean- shipping-company-sa-v-glencore-international-ag-2017-ewca-civ
[84] Maersk incident response : https://red-goat.com/why-you-should-test-your-incident-response-a-review-of-the-maersk-incident/
[85] Shipping: BW Group's computer systems hacked; steps up cyber Security : https://www.spglobal.com/commodITyinsights/en/market-insights/latest-news/shipping/101317-shipping-bw-groups-computer-systems-hacked-steps-up-cyber-Security
[86] CLARKSON PLC (“Clarksons” “the Company”) NOTice of cyber Security incident : https://infoSecuritymagazine.be/files/784d57ce2fe4ee3f0c5d765d274fe890.pdf
[87] Clarkson Plc Reveals Details of 2017 Cyber Security Incident: https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-Security-incident/

[88] COSCO US operations disrupted by cyber attack : https://www.rivieramm.com/news-content-hub/news-content-hub/cosco-us-operations-disrupted-by-cyber-attack-23881

3.3 Πηγές:

[89] Guidelines on Marinetime Cyber Risk Management https://www.imo.org/en/OurWork/Security/Pages/Guidance-home.aspx

[90] Introduction to MTSA: The Marinetime Transportation Security Act U. S. Coast Guard Ms. April Tribeck, PSS, D8 : https://www.cisa.gov/sites/default/files/publications/2019- CSSS-USCG-MTSA-101-508.pdf

[91] 2023 cyber trends and insights in the marine environment Coast Guard Cyber Command, UnITed States Coast Guard https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf

[92] Code of Practice Cyber Security for Ships: https://www.steamshipmutual.com/sites/default/files/downloads/loss-prevention/UK- Cyber-Security-Code-of-Practice-for-ships-201709.pdf

[93] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) http://data.europa.eu/eli/reg/2016/679/oi