Κεφάλαιο 4: Πλαίσιο Ναυτιλιακής Κυβερνοασφάλειας

Επισκόπηση

Το Θαλάσσιο Διαδίκτυο των Πραγμάτων (MIoT) είναι η σύνδεση συστημάτων Επιχειρηματικής Τεχνολογίας (BT) και Πληροφορικής (IT) για τη δημιουργία περίπλοκων και έξυπνων δικτύων στη ναυτιλιακή βιομηχανία. Ο ψηφιακός μετασχηματισμός βελτιώνει την απόδοση των πλοίων και το διεθνές εμπόριο, αλλά δημιουργεί νέες κυβερνοαπειλές. Αυτό το κεφάλαιο εξετάζει τα έξι θεμελιώδη στοιχεία που απαιτούν οι οντότητες για να αναπτύξουν ένα ισχυρό πλαίσιο θαλάσσιας ασφάλειας. Αυτά τα στοιχεία είναι η πλήρης ασφάλεια των πλοίων στην Επιχειρησιακή Τεχνολογία (OT), η αξιολόγηση απειλών από πλοίο σε ακτή, η εφαρμογή Αρχιτεκτονικής Μηδενικής Εμπιστοσύνης, η σημαντική προστασία των θαλάσσιων υποδομών, η ασφάλεια της εφοδιαστικής αλυσίδας με blockchain και τα προηγμένα συστήματα ανίχνευσης εισβολών (IDS).

Η ασφάλεια στον κυβερνοχώρο στη θάλασσα είναι ανάλογη, αλλά έχει μια σειρά από βασικές έννοιες που δεν είναι ίδιες. Η ασφάλεια OT προστατεύει το βασικό επίπεδο ενός πλοίου, το υλικό και τα προγράμματα που εκτελούν τα βασικά συστήματα. Συζητά επίσης τις μεθόδους που χρησιμοποιούνται για την επίθεση στις επικοινωνίες πλοίου-ξηράς. Χρησιμοποιείται Αρχιτεκτονική Μηδενικής Εμπιστοσύνης για την υποβολή ερωτημάτων. Προστατεύονται επίσης κρίσιμες υποδομές, όπως λιμάνια και ναυτιλιακές οδοί. Δύο που ενισχύουν την εμπιστοσύνη και την προστασία είναι το blockchain και τα Συστήματα Ανίχνευσης Εισβολών. Οι πυλώνες συνδυάζονται για να έχουν μια πλήρη εικόνα της ασφάλειας στη θάλασσα και αυτό δεν είναι η ασφάλεια των συνόρων, αλλά πολλαπλά επίπεδα προστασίας από οποιαδήποτε απειλή ανά πάσα στιγμή.

Αυτό το κεφάλαιο καταδεικνύει πώς τα στοιχεία συνεργάζονται για την προστασία της διεθνούς ναυτιλίας από τον αυξανόμενο αριθμό κυβερνοαπειλών που θέτουν σε κίνδυνο την αξιοπιστία της. Το κεφάλαιο βασίζεται στη συνδεσιμότητα που περιγράφεται από το Κεφάλαιο 2 και στα συστήματα ανίχνευσης από το Κεφάλαιο 3 για να δημιουργήσει το απαραίτητο πλαίσιο εμπιστοσύνης για προηγμένα αυτόνομα και βασισμένα σε δεδομένα συστήματα των επόμενων κεφαλαίων.

4.1 Ασφάλεια Ναυτιλιακής Επιχειρησιακής Τεχνολογίας (OT)

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Οι επιθέσεις στον κυβερνοχώρο σε συστήματα Επιχειρησιακής Τεχνολογίας (OT) πλοίων θα οδηγήσουν σε καθυστερήσεις στις αποστολές και κινδύνους για την ασφάλεια. Η αυξημένη αυτοματοποίηση των πλοίων θα καταστήσει πιο σημαντική από ποτέ την προστασία των OT. Η ενότητα στοχεύει να δείξει πώς η κατάσταση ασφάλειας των OT των λιμένων επηρεάζει ολόκληρο το σύστημα IoT. BIMCO et al., 2024; Διεθνής Ναυτιλιακός Οργανισμός, 2022. Τα συστήματα Επιχειρησιακής Τεχνολογίας (OT) που είναι εγκατεστημένα σε ένα πλοίο διευκολύνουν την εκτέλεση βασικών δραστηριοτήτων όπως η πλοήγηση και η λειτουργία της μηχανής. Είναι επίσης σημαντικά για τη διασφάλιση της ασφάλειας των λειτουργιών των πλοίων.

Θεωρητικό Υπόβαθρο

Η επιχειρησιακή τεχνολογία ή OT περιλαμβάνει συστήματα SCADA που χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο των συστημάτων των πλοίων. Τα παλιά συστήματα OT λειτουργούσαν ξεχωριστά και εφάρμοζαν μοναδικά πρωτόκολλα επικοινωνίας για την επίτευξη ασφάλειας μέσω περιορισμένης πρόσβασης. Τα συστήματα ενσωματώθηκαν περισσότερο με τα δίκτυα πληροφορικής για την ενίσχυση των δυνατοτήτων κοινής χρήσης δεδομένων. Η μελέτη καταδεικνύει ότι αυτή η εξέλιξη έχει εισαγάγει περισσότερες κυβερνοαπειλές, καθώς τα συστήματα OT δεν είχαν σχεδιαστεί για να χειρίζονται κυβερνοεπιθέσεις. Τα βασικά ευρήματα δείχνουν ότι τα παλιά συστήματα OT δεν λαμβάνουν ενημερώσεις

ασφαλείας και αυτό τα καθιστά ευάλωτα σε κυβερνοαπειλές. Η Ναυτιλιακή Επιχειρησιακή Τεχνολογία έχει εξελιχθεί από απλά συστήματα ελέγχου σε ολοκληρωμένα ψηφιακά συστήματα, αλλά τα επίπεδα ασφάλειας που εφαρμόζονται δεν έχουν αυξηθεί ως σημαντικές βελτιώσεις (Stouffer et al., 2023; BIMCO et al., 2024).

Πίνακας 4.1: *Σύγκριση Χαρακτηριστικών Τεχνολογίας Πληροφοριών (IT) και Επιχειρησιακής Τεχνολογίας (OT)*

Χαρακτηριστικό	Τεχνολογία Πληροφοριών (IT)	Επιχειρησιακή Τεχνολογία (OT)
Κύριος Στόχος Ασφάλειας	Εμπιστευτικότητα & Ακεραιότητα (Προστασία Δεδομένων)	Διαθεσιμότητα & Ασφάλεια (Συνεχής Λειτουργία)
Απαίτηση Πραγματικού Χρόνου	Μη κρίσιμη (καθυστερήσεις αποδεκτές)	Κρίσιμη (αυστηρές απαιτήσεις σε ms)
Κύκλος Ζωής Συστήματος	Μικρός (3-5 έτη)	Μεγάλος (10-20+ έτη)
Διαχείριση Ενημερώσεων (Patching)	Τακτικές, προγραμματισμένες ενημερώσεις	Δύσκολη; απαιτείται διακοπή λειτουργίας ή δεξαμενισμός
Συνδεσιμότητα	Υψηλό εύρος ζώνης, τυπικά πρωτόκολλα (TCP/IP)	Χαμηλό εύρος ζώνης, ιδιόκτητα πρωτόκολλα (NMEA, Modbus)
Τυπικά Συστήματα	Servers, PCs, Wi-Fi Πληρώματος, ERP	SCADA, PLC, ECDIS, Έλεγχος Μηχανής
Κύριος Κυβερνοκίνδυνος	Υποκλοπή δεδομένων, Ransomware, Phishing	Φυσική ζημιά, Περιστατικά ασφαλείας, GPS Spoofing

Τεχνικές Προκλήσεις και Προβληματισμοί

Το Ναυτικό Οργάνωση (ΟΟ) λειτουργεί υπό ειδικές συνθήκες, καθώς η θάλασσα είναι ταραγμένη και τα συστήματα απομακρυσμένα. Τα παλιά συστήματα διαθέτουν παλιό λογισμικό, το οποίο είναι γνωστό και μπορεί να αξιοποιηθεί από χάκερ. Η σύνδεση μεταξύ των συστημάτων πληροφορικής του γραφείου και των συστημάτων ελέγχου παρέχει πρόσβαση σε χάκερ που μπορούν να χρησιμοποιήσουν τα δίκτυα του γραφείου για επιθέσεις. Τα πληρώματα πρέπει να εκτελούν τόσο την εργασία πληροφορικής όσο και την εργασία ΟΟ με έλλειψη εμπειρογνωμοσύνης. Μερικά από τα σφάλματα που εντοπίστηκαν είναι οι ανεπαρκείς ρυθμίσεις δικτύου που επιτρέπουν την κυκλοφορία του κακόβουλου λογισμικού και οι ανεπαρκείς έλεγχοι πρόσβασης που επιτρέπουν στους επιτιθέμενους. Αυτά τα προβλήματα είναι ακόμη χειρότερα σε απομονωμένες τοποθεσίες όπου δεν είναι δυνατή η πρόσβαση σε βοήθεια σε πραγματικό χρόνο (Διεθνής Ναυτιλιακός Οργανισμός, 2022; BIMCO et al., 2024).

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Επί του παρόντος, τα δίκτυα OT και IT μπορούν να διαχωριστούν χρησιμοποιώντας τμηματοποίηση. Τα τείχη προστασίας και τα εργαλεία παρακολούθησης είναι τα εργαλεία που μπορούν να χρησιμοποιηθούν για την ανίχνευση απειλών σε πρώιμο στάδιο. Το μοντέλο μηδενικής εμπιστοσύνης χρησιμοποιείται από ορισμένες προσεγγίσεις για να διασφαλιστεί ότι η πρόσβαση ελέγχεται. Τα συστήματα ανίχνευσης εισβολών χρησιμοποιούνται για την παρακολούθηση των δεδομένων του OT για την ανίχνευση ασυνήθιστων μοτίβων. Οι κίνδυνοι μπορούν να μειωθούν όταν αυτά τα εργαλεία χρησιμοποιούνται μαζί με την κανονική ενημέρωση (Stouffer et al., 2023; International Maritime Organization, 2022). Διατάξεις με κενό αέρα χρησιμοποιούνται σε κρίσιμα συστήματα για την αποτροπή απομακρυσμένων επιθέσεων σύμφωνα με τις τρέχουσες αρχιτεκτονικές.

Εφαρμογές και Σενάρια Χρήσης

Η ασφάλεια της επιχειρησιακής τεχνολογίας (OT) βοηθά στην προστασία των συστημάτων πλοήγησης των πλοίων κατά τη διάρκεια των πραγματικών λειτουργιών. Τα δεξαμενόπλοια εφαρμόζουν μεθόδους διαμέρισης για την προστασία των συστημάτων ελέγχου πρόωσης, γεγονός που έχει ως αποτέλεσμα τη μείωση των λειτουργικών διακοπών. Τα δεδομένα απόδοσης της μελέτης περίπτωσης καταδεικνύουν βελτιωμένους χρόνους απόκρισης του συστήματος σε καταστάσεις απειλής. Τα εργαλεία παρακολούθησης επιτρέπουν στα λιμάνια να αποτρέπουν επιθέσεις ransomware, γεγονός που οδηγεί σε εξοικονόμηση χρόνου και μείωση κόστους. (BIMCO et al., 2024; Stouffer et al., 2023).

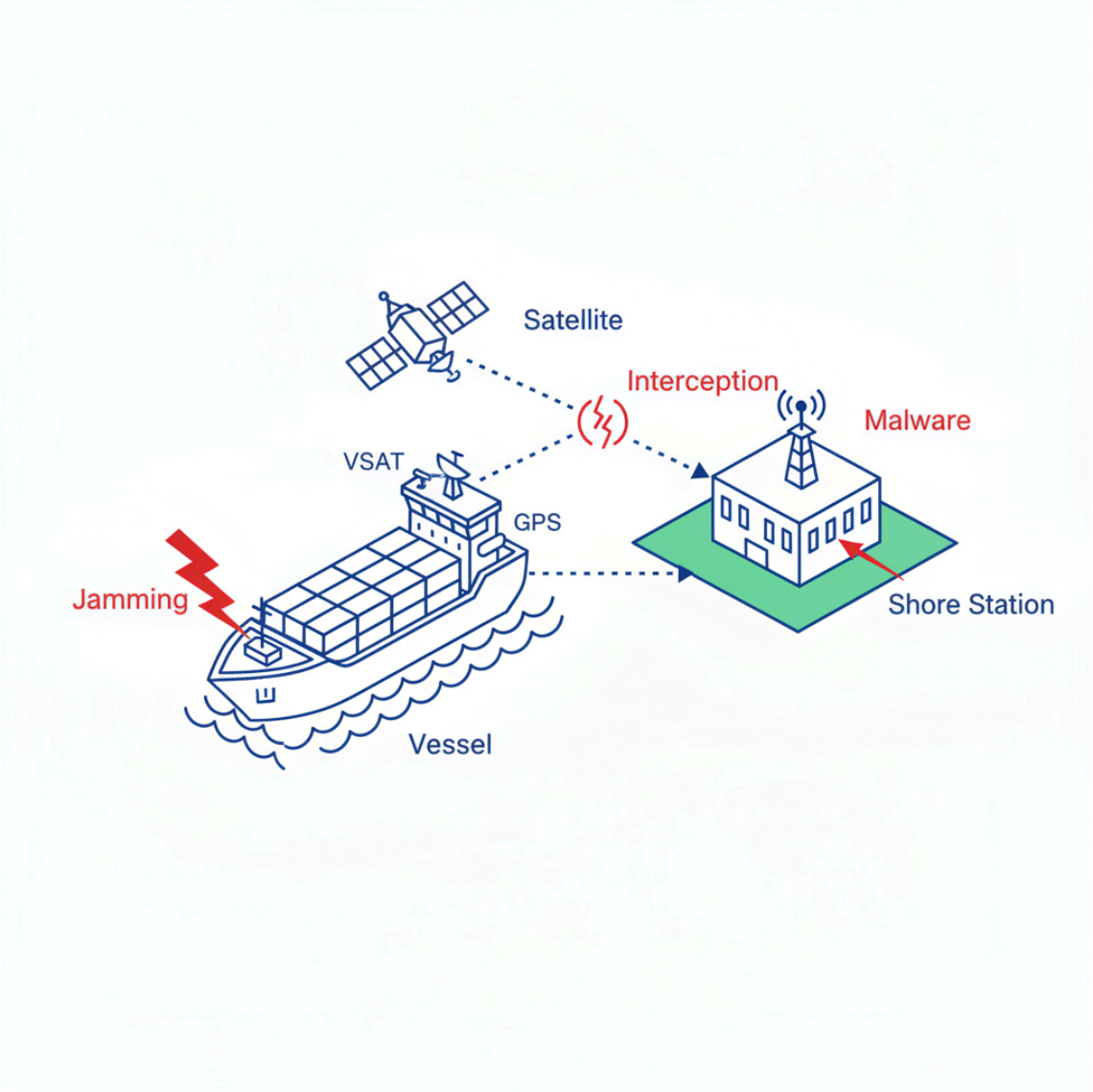
Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Στο μέλλον, οι έρευνες θα πρέπει να επικεντρωθούν σε εφαρμογές που βασίζονται στην Τεχνητή Νοημοσύνη (ΤΝ) για την πρόβλεψη των απειλών στην ΟΤ. Υπάρχουν ελλείψεις στον τρόπο διαχείρισης των κατανεμημένων συστημάτων σε πλοία και λιμάνια. Μερικές από τις νέες τάσεις που αναδύονται είναι η χρήση της αλυσίδας μπλοκ για ασφαλή μεταφορά δεδομένων. Τα σημαντικά ζητήματα που παραμένουν ανεπίλυτα είναι το πώς να καταστεί η ΟΤ ανθεκτική στις νέες επιθέσεις, όπως αυτές που προκαλούνται από την ΤΝ. Οι άλλες έρευνες θα πρέπει να κατευθύνονται προς την ανάπτυξη βελτιωμένων τεχνικών εκπαίδευσης από τους σχεδιαστές για την εκπαίδευση των πληρωμάτων στην ασφάλεια της ΟΤ (Διεθνής Ναυτιλιακός Οργανισμός, 2022; BIMCO et al., 2024).

4.2 Μοντέλα Κυβερνοαπειλών Πλοίου-Ξηράς

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Η ψηφιακή επικοινωνία μεταξύ πλοίων και λιμενικών αρχών επιτρέπει στις ναυτιλιακές επιχειρήσεις να λειτουργούν αποτελεσματικά. Η ψηφιακή σύνδεση μεταξύ πλοίων και λιμενικών αρχών επιτρέπει στα πλοία να επικοινωνούν με τις λιμενικές αρχές, τα εταιρικά back offices τους και τα άλλα βασικά συστήματα logistics. Η ψηφιακή σύνδεση πλοίου-ξηράς έχει γίνει σημαντικός στόχος κυβερνοεπιθέσεων, επειδή τα πλοία χρησιμοποιούν ολοένα και περισσότερο ένα ενιαίο δίκτυο που διασυνδέει τα συστήματα πληροφορικής τους με συστήματα ΟΤ. Η δυσλειτουργία των ψηφιακών συνδέσεων πλοίου-ξηράς θα αναστείλει τις λιμενικές λειτουργίες και θα υποβαθμίσει την αποτελεσματικότητα του παγκόσμιου εμπορίου, και θα δημιουργήσει σοβαρούς κινδύνους για την ασφάλεια και το περιβάλλον που πρέπει να μετριαστούν από ισχυρά συστήματα μοντελοποίησης απειλών σε θαλάσσια συστήματα IoT (US Coast Guard, 2024; BIMCO et al., 2024).



Εικόνα 4.2: *Τοπίο Κυβερνοαπειλών Πλοίου-Προς-Ξηρά, που απεικονίζει κρίσιμα τρωτά σημεία σε δορυφορικές συνδέσεις επικοινωνίας (VSAT) και συστήματα εντοπισμού θέσης (GPS/AIS).*

Θεωρητικό Υπόβαθρο

Η βιβλιογραφία δείχνει ότι οι κυβερνοαπειλές στις επικοινωνίες πλοίου-ξηράς συνεχίζουν να αυξάνονται σε πολυπλοκότητα και κλίμακα. Οι ερευνητές αρχικά εντόπισαν κινδύνους σε συστήματα πλοήγησης και γεφυρών, αλλά η τρέχουσα επιφάνεια επίθεσης περιλαμβάνει πλέον ευπάθειες σε συστήματα φορτίου και συστήματα πρόωσης, καθώς και σε πλατφόρμες διοίκησης. Εθνικές και διεθνείς αναφορές δείχνουν ότι οι εισβολείς μπορούν να εκμεταλλευτούν τόσο τις απομακρυσμένες απειλές όσο και τα φυσικά σημεία πρόσβασης. Τα σύγχρονα πλαίσια αξιολόγησης κινδύνου, συμπεριλαμβανομένων των NIST CSF και MaCRA, επιτρέπουν στους ναυτιλιακούς οργανισμούς να εκτελούν διακυβέρνηση σε ολόκληρη τη θάλασσα, διαχείριση περιουσιακών στοιχείων και ανάλυση ευπάθειας (Li et al., 2024; Hopcraft et al., 2024; Ακτοφυλακή των ΗΠΑ, 2024).

Τεχνικές Προκλήσεις και Προβληματισμοί

Τα ναυτιλιακά συστήματα αντιμετωπίζουν συγκεκριμένα τεχνικά προβλήματα με τη μορφή παρωχημένου εξοπλισμού και πολλαπλών εκδόσεων λογισμικού, καθώς και έλλειψης γνώσεων για την κυβερνοασφάλεια επί του πλοίου. Η ενσωμάτωση παρέχει πρόσθετα σημεία επίθεσης, όπως κακόβουλο λογισμικό σε χερσαία εταιρικά δίκτυα και επιθέσεις στην εφοδιαστική αλυσίδα μέσω τρίτων προμηθευτών. Το ανθρώπινο λάθος και η κοινωνική μηχανική αποτελούν έναν συνεχή κίνδυνο, ενώ οι κανόνες είναι ασυνεπείς και οι αργοί κύκλοι ενημέρωσης κώδικα επιδεινώνουν τα προβλήματα. Το προσωπικό των πλοίων δεν διαθέτει υποστήριξη κυβερνοασφάλειας σε πραγματικό χρόνο ή δυνατότητες αντιμετώπισης περιστατικών (US Coast Guard, 2024; Li et al., 2024).

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Εξελιγμένα πλαίσια όπως τα STRIDE, STPA-Sec, CORAS και MaCRA χρησιμοποιούνται στη μοντελοποίηση απειλών στον ναυτιλιακό τομέα για την αξιολόγηση των κινδύνων από τεχνικής αλλά και επιχειρησιακής άποψης. Τέτοια μοντέλα εφαρμόζονται στην αναγνώριση απειλών και στην προτεραιότητα μετριασμού τους με τη βοήθεια εργαλείων χαρτογράφησης περιουσιακών στοιχείων, ανακάλυψης διαδρομής επίθεσης και ποσοτικοποίησης κινδύνου. Υπάρχει μεγαλύτερη χρήση της ανίχνευσης απειλών που βασίζεται στην Τεχνητή Νοημοσύνη, της τμηματοποίησης δικτύου και της συνεχούς παρακολούθησης. Τα τυποποιημένα πρωτόκολλα για τη διαχείριση κινδύνου και την αξιολόγηση τρωτότητας παρέχονται από τις κυβερνητικές και βιομηχανικές οδηγίες, όπως αυτές του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) και του BIMCO, 2024, Hopcraft et al., 2024, Maritime Artificial Intelligence-based Intrusion Detection Sahay et al., 2022).

Εφαρμογές και Σενάρια Χρήσης

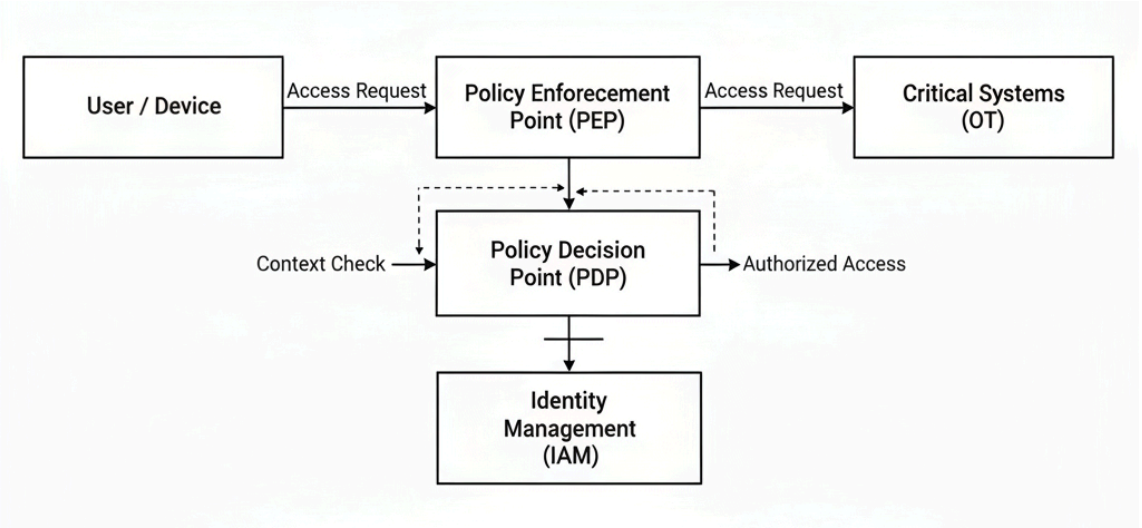
Τα μοντέλα απειλών χρησιμοποιούνται από επαγγελματίες ασφαλείας για την αναζήτηση τρωτών σημείων, την προσποίηση επιθέσεων και την αντιμετώπιση πραγματικών επιθέσεων. Μπορούν επίσης να διαδραματίσουν ρόλο στις ασκήσεις εκπαίδευσης, στην εκπαίδευση πληρωμάτων για την ανίχνευση ηλεκτρονικού "ψαρέματος" (phishing) και στον τακτικό σχεδιασμό σε περίπτωση επίθεσης ransomware σε γερανούς ή συστήματα ελέγχου γεφυρών. Αυτά τα μοντέλα χρησιμοποιούνται από την Ακτοφυλακή των ΗΠΑ και διεθνείς εταίρους σε ετήσια βάση για τη διεξαγωγή ελέγχων ασφαλείας και την υποβολή εκθέσεων σχετικά με το πώς αλλάζουν οι επιθέσεις, όπως η στόχευση της διαχείρισης πλοίων που βασίζεται στο cloud.

Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Τα μελλοντικά μοντέλα θαλάσσιων κυβερνοκινδύνων θα πρέπει να περιλαμβάνουν την εξάπλωση των αυτόνομων πλοίων, τη ζήτηση για κβαντικά ασφαλείς επικοινωνίες και νέους τύπους υποδομών cloud. Οι ερευνητές πρέπει να ανακαλύψουν πώς να προσαρμόζονται γρήγορα στους εξελισσόμενους κινδύνους. Απαιτούν μοντέλα που συνδυάζουν ταυτόχρονα τις προοπτικές της Πληροφορικής (IT) και της Επιχειρησιακής Τεχνολογίας (OT). Ο κόσμος απαιτεί ενοποιημένους κανονισμούς και βελτιωμένη εκπαίδευση του προσωπικού ως τομείς όπου οι καινοτόμοι μπορούν να δημιουργήσουν νέες λύσεις, σύμφωνα με τους Li et al. (2024) και Hopcraft et al. (2024).

4.3: Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust) για Ναυτιλιακά Συστήματα

Η Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust Architecture) εφαρμόζει το δόγμα «ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις» (never trust, always verify) στο IT/OT πλοίων και λιμένων, χρησιμοποιώντας ελέγχους με επίκεντρο την ταυτότητα, συνεχή επαλήθευση και μικρο-κατάτμηση (micro-segmentation) που δεν βασίζονται στην τοποθεσία δικτύου για εμπιστοσύνη (π.χ. πλοίο έναντι ξηράς) (Rose et al., 2020). Σε ναυτιλιακά πλαίσια, η υιοθέτηση του Zero Trust μειώνει το εύρος των επιπτώσεων των παραβιάσεων και περιορίζει την πλευρική μετακίνηση (lateral movement) στα δίκτυα πλοήγησης, ελέγχου και ευημερίας υπό μικτή δορυφορική και επίγεια συνδεσιμότητα (Li et al., 2024).



Εικόνα 4.1: *Λογικό Μοντέλο Ναυτιλιακής Αρχιτεκτονικής Μηδενικής Εμπιστοσύνης (Zero Trust Architecture - ZTA) που δείχνει τον διαχωρισμό των Σημείων Λήψης Αποφάσεων Πολιτικής (PDP) και των Σημείων Επιβολής Πολιτικής (PEP) για την ασφάλεια κρίσιμων συστημάτων OT επί του πλοίου. (Πηγή: Προσαρμογή από το NIST SP 800-207)*

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Η εγκατάσταση πολυάριθμων απομακρυσμένων συστημάτων τρίτων και ψηφιακών συστημάτων στα σύγχρονα πλοία έχει αυξήσει τις πιθανότητες επίθεσης. Η μηδενική εμπιστοσύνη επιβάλλει ελάχιστη πρόσβαση ανά αίτημα και πολλαπλές διαδικασίες επαλήθευσης που είναι καλές για απομακρυσμένους στόλους και λιμάνια (Rose et al., 2020). Η εμπειρική έρευνα δείχνει ότι τα AIS, ECDIS, VSAT και port OT διατρέχουν αυξανόμενο κίνδυνο κυβερνοαπειλής. Ενθαρρύνει τη συνεχή επαλήθευση χρηστών και συσκευών και την τμηματοποίηση σημαντικών περιουσιακών στοιχείων για τη μείωση των λειτουργικών διαταραχών (Li et al., 2024).

Θεωρητικό Υπόβαθρο

Το NIST SP 800-207 καθορίζει βασικές έννοιες και στοιχεία της Μηδενικής Εμπιστοσύνης, οι οποίες περιλαμβάνουν τα σημεία επιβολής και λήψης αποφάσεων πολιτικής, την ελάχιστη πρόσβαση, τη συνεχή επαλήθευση/εξουσιοδότηση και την πολιτική που βασίζεται στην τηλεμετρία (Rose et al., 2020). Αργότερα, οι πρακτικές Μηδενικής Εμπιστοσύνης, όπως συζητούνται στη βιβλιογραφία, περιλαμβάνουν τη δυναμική εμπιστοσύνη, τη μικροτμηματοποίηση και την πρόσβαση βάσει ταυτότητας, οι οποίες στοχεύουν στη μείωση της πλευρικής κίνησης σε ετερογενή δίκτυα που σχετίζονται με την ψηφιοποίηση της ναυτιλίας (Azad et al., 2024).

Τεχνικές Προκλήσεις και Προβληματισμοί

Οι μετατοπισμένες και καθυστερημένες συνδέσεις (όπως το VSAT) εμποδίζουν τη διαδικασία συνεχούς επαλήθευσης και κεντρικής χάραξης πολιτικής. Θα πρέπει να υπάρχει τοπική συμμόρφωση στις αρχιτεκτονικές, με προσωρινή αποθήκευση πολιτικής για την υποστήριξη της ασφάλειας και των λειτουργιών σε περίπτωση απώλειας σύνδεσης (Li et al., 2024). Τα συστήματα ασφαλείας ναυτιλιακών OT πρέπει να είναι ανεξάρτητα. Η μικροτμηματοποίηση μηδενικής εμπιστοσύνης σε ζώνες και αγωγούς IEC 62443 θα πρέπει να διατηρεί την ακεραιότητα της ασφάλειας, αλλά να επιτρέπει τη συντήρηση και την παρακολούθηση ελεγχόμενων, ελεγχόμενων αγωγών (Rødseth et al., 2022).

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Αυτό το σύστημα έχει σχεδιαστεί με χειριστήρια τοποθετημένα κοντά στις κρίσιμες περιοχές του πλοίου, π.χ. πλοήγηση, πρόωση και φορτίο. Η επαλήθευση και η εξουσιοδότηση συνεδρίας, σε συνδυασμό με την κρυπτογράφηση, προστατεύουν τις επικοινωνίες πλοίου-ξηράς και πλοίου-cloud, Rose et al., 2020. Η μικροτμηματοποίηση ορίζει λίστες επιτρεπόμενων για τις επικοινωνίες συσκευής-προς-συσκευή, ευθυγραμμιζόμενη με τις ζώνες/αγωγούς IEC 62443 για να διατηρήσει την αυτονομία ασφάλειας OT και να επιτρέψει την απομακρυσμένη πρόσβαση με τα λιγότερα δικαιώματα (Rödseth et al., 2022).

Εφαρμογές και Σενάρια Χρήσης

Πρόσβαση σε συντήρηση την κατάλληλη στιγμή: Οι OEM του τμήματος Propulsion ή ECDIS μπορούν να έχουν πρόσβαση στο σύστημα για ένα ορισμένο χρονικό διάστημα, ανάλογα με τον ρόλο εργασίας τους, αφού πρώτα επαληθεύσουν τη στάση της συσκευής και την ταυτότητα του χρήστη (Rose et al., 2020).

Διαχωρισμός λιμενικών λειτουργιών: Ο σαφής διαχωρισμός των συστημάτων ελέγχου γερανών, διαχείρισης αυλής και πύλης με βάση πολιτικές που βασίζονται στην ταυτότητα μειώνει τη ζημιά μεταξύ τομέων που προκαλείται από επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing) ή κακόβουλου λογισμικού (Azad et al., 2024).

Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Η μηδενική εμπιστοσύνη απαιτεί κατανεμημένη επιβολή αποφάσεων με ισχυρό σύστημα προσωρινής μνήμης μέχρι να υπάρξουν διακοπές λειτουργίας δορυφόρων, και στη συνέχεια θα πρέπει να επιβεβαιωθεί σε δοκιμές αποστολής (Rose et al., 2020). Δεν έχουν ακόμη λυθεί οι πρακτικές προσεγγίσεις της προσθήκης ταυτότητας και τηλεμετρίας στο παλιό λειτουργικό σύστημα (όπως proxies ή sidecars) και οι φιλικές προς τον χειριστή ροές εργασίας που διατηρούν την ασφάλεια και εξηγούν τις αποφάσεις (Li et al., 2024).

4.4 Προστασία Κρίσιμων Ναυτιλιακών Υποδομών

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Τα λιμάνια, τα υποθαλάσσια καλώδια, οι υπεράκτιες πλατφόρμες και οι ναυτιλιακές οδοί είναι ζωτικής σημασίας εμπορικές οδοί που επιτρέπουν την ομαλή λειτουργία του παγκόσμιου εμπορικού συστήματος, επιτρέποντας τη μεταφορά αγαθών και ενέργειας και τη μετάδοση δεδομένων (MARSEC-COE, 2023). Όταν τέτοιες υποδομές παραβιάζονται ή υποβαθμίζονται από κυβερνοεπιθέσεις ή φυσικές επιθέσεις, επηρεάζουν τις αλυσίδες εφοδιασμού, την οικονομία και την ασφάλεια στη θάλασσα (Liebetrau, 2023). Η ναυτιλιακή βιομηχανία γίνεται όλο και πιο προσανατολισμένη στα δεδομένα, επομένως η προστασία αυτών των συστημάτων αποτελεί εθνική ανησυχία για την ασφάλεια και είναι ζωτικής σημασίας για τη διατήρηση του διεθνούς εμπορίου σε έναν ψηφιακά διασυνδεδεμένο κόσμο (MARSEC-COE, 2023; Liebetrau, 2023).

Θεωρητικό Υπόβαθρο

Η έρευνα για την Προστασία των Θαλάσσιων Κρίσιμων Υποδομών έχει αυξηθεί λόγω του γεγονότος ότι υπάρχουν νέες απειλές που δημιουργούνται από τις ψηφιακές τεχνολογίες και τις παγκόσμιες πολιτικές εντάσεις. Η βασική έρευνα καταδεικνύει ότι τα θαλάσσια περιουσιακά στοιχεία είναι ευάλωτα σε κυβερνοεπιθέσεις και φυσικές επιθέσεις, με τα λιμάνια και τα υποθαλάσσια καλώδια να επικεντρώνονται ολοένα και περισσότερο σε εξελιγμένους εισβολείς, στους οποίους περιλαμβάνονται έθνη-κράτη και εγκληματικές ομάδες (Cyble, 2025). Το NATO και ο Διεθνής Ναυτιλιακός Οργανισμός είναι μεταξύ των σημαντικότερων διεθνών οργανισμών που έχουν ξεκινήσει κατευθυντήριες γραμμές και ομάδες εργασίας, καθώς και συνεργατικές ασκήσεις για την ενίσχυση της ανθεκτικότητας (O' Dwyer, 2023). Η κυβερνοεπίθεση της Maersk και τα περιστατικά στις υπηρεσίες GPS έχουν προκαλέσει αύξηση της ευαισθητοποίησης, των κανονισμών και της διεθνούς συνεργασίας (MARSEC-COE, 2023).

Τεχνικές Προκλήσεις και Προβληματισμοί

Η προστασία κρίσιμων θαλάσσιων υποδομών αντιμετωπίζει συγκεκριμένες δυσκολίες, όπως εκτεταμένες αλυσίδες εφοδιασμού και απομακρυσμένες μη επανδρωμένες υποδομές, απαρχαιωμένα συστήματα και πολλαπλές ομάδες ενδιαφερομένων (BIMCO et al., 2024). Η σύγκλιση της επιχειρησιακής τεχνολογίας (OT) και της τεχνολογίας πληροφοριών (IT) αξιοποιείται από τους κυβερνοεγκληματίες, οι οποίοι εκμεταλλεύονται επίσης την αδύναμη τμηματοποίηση του δικτύου και τις κακές πρακτικές συντήρησης, καθώς και το ανθρώπινο στοιχείο της ανεπαρκούς εκπαίδευσης του πληρώματος στην κυβερνοασφάλεια (MARSEC-COE, 2023). Σύμφωνα με τον Liebetrau (2023), η πρόκληση της παρακολούθησης των υποβρύχιων περιουσιακών στοιχείων είναι περίπλοκη λόγω της ευρείας κατανομής τους. Σύμφωνα με τον Liebetrau (2023), η έλλειψη συντονισμού στα συστήματα απόκρισης και τα ανεπαρκή κανάλια ανταλλαγής πληροφοριών οδηγούν σε αργές αντιδράσεις ελέγχου ζημιών, ειδικά όταν εμπλέκονται πολλαπλές δικαιοδοσίες.

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Οι σύγχρονες προσεγγίσεις του MCIP χρησιμοποιούν εργαλεία αξιολόγησης κινδύνου, πρότυπα κυβερνοασφάλειας (συμπεριλαμβανομένου του κώδικα ISM του IMO) και εξελιγμένα σχέδια αντιμετώπισης περιστατικών, τα οποία αποτελούνται από φάσεις προετοιμασίας, ανίχνευσης, περιορισμού, απομάκρυνσης και ανάκτησης (IASME, 2025). Η εφαρμογή μη επανδρωμένων οχημάτων (USV/UUV) βελτιώνει τις επιχειρήσεις επιτήρησης και ασφάλειας, ιδιαίτερα σε περιοχές υψηλού κινδύνου ή απομακρυσμένες τοποθεσίες (EEAS, 2025). Οι πλατφόρμες των ψηφιακών διδύμων και των συστημάτων επίγνωσης κατάστασης υποστηρίζουν την παρακολούθηση του περιβάλλοντος, και τα συνεργατικά οικοσυστήματα όπως η πλατφόρμα του PRECINCT επιτρέπουν τη διατομεακή συνεργασία σε συστήματα κυβερνοφυσικής ασφάλειας (PRECINCT, 2024). Πολυεθνικές ασκήσεις, όπως η MARSEC EU 25, ενισχύουν τις δυνατότητες συντονισμένης αντιμετώπισης και τη χρήση βέλτιστων πρακτικών (EEAS, 2025).

Εφαρμογές και Σενάρια Χρήσης

Τα πλαίσια MCIP αποδεικνύονται επίσης αποτελεσματικά στις λειτουργίες ασφάλειας λιμένων και στην ανθεκτικότητα των υποβρυχίων καλωδίων, καθώς και στην προστασία των γραμμών εφοδιασμού ενέργειας, όπως οι τερματικοί σταθμοί LNG (MARSEC-COE, 2023). Η εμπειρία του περιστατικού με την Maersk έχει οδηγήσει στην εφαρμογή ισχυρών συστημάτων δημιουργίας αντιγράφων ασφαλείας και διατομεακών ασκήσεων στον κυβερνοχώρο (PRECINCT, 2024). Τα αυτοματοποιημένα συστήματα ανίχνευσης απειλών και χαρτογράφησης κινδύνου βάσει δεδομένων είναι ικανά να επιτρέψουν στους οργανισμούς να ανταποκρίνονται προληπτικά στις μεταβαλλόμενες απειλές (O'Dwyer, 2023). Οι μελέτες περιπτώσεων καταδεικνύουν τα πλεονεκτήματα της συνεργασίας μεταξύ οργανισμών του δημόσιου τομέα και ιδιωτικών φορέων εκμετάλλευσης και διεθνών οργανισμών για την έγκαιρη αντιμετώπιση καταστάσεων έκτακτης ανάγκης και την προστασία του διεθνούς εμπορίου (Liebetrau, 2023).

Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Οι επιστήμονες αναπτύσσουν επί του παρόντος πιο ευέλικτες προσεγγίσεις ανθεκτικότητας βασισμένες στον κίνδυνο, καλύτερες προσεγγίσεις ενσωμάτωσης OT/IT και προγράμματα εκπαίδευσης για την ενίσχυση της κυβερνοεπίγνωσης των πληρωμάτων (BIMCO et al., 2024). Η τεχνητή νοημοσύνη μπορεί επίσης να χρησιμοποιηθεί για την αυτόματη ανίχνευση ανωμαλιών και μπορούν να αναπτυχθούν πλαίσια απόκρισης ΕΕ-ΝΑΤΟ για τον συντονισμό της ταχείας αντίδρασης πέρα από τα γεωπολιτικά σύνορα (EEAS, 2025). Το κενό εξακολουθεί να υπάρχει στον τομέα της συλλογής πληροφοριών για απειλές και της ανταλλαγής πληροφοριών με τις υβριδικές ναυτιλιακές και διασυνοριακές απειλές, ιδίως όσον αφορά τις ενεργειακές υποδομές και τα καλώδια δεδομένων (Liebetrau, 2023).

4.5: Εφαρμογές Blockchain στις Ναυτιλιακές Εφοδιαστικές Αλυσίδες

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Οι αλυσίδες εφοδιασμού ναυτιλιακών μεταφορών διευκολύνουν το μεγαλύτερο μέρος του παγκόσμιου εμπορίου, καθώς μεταφέρουν περισσότερο από το ενενήντα τοις εκατό των παγκόσμιων εμπορευμάτων (Liu et al., 2023). Οι αλυσίδες εφοδιασμού ναυτιλιακών μεταφορών πρέπει να διαχειριστούν διάφορα εμπόδια, όπως τα ασύνδετα συστήματα γραφειοκρατίας και την απουσία ορατότητας και τις υποβαθμισμένες σχέσεις μεταξύ των διαφόρων μερών (Farah et al., 2024). Οι βασικές λειτουργίες της τεχνολογίας blockchain είναι τριπλές, οι οποίες περιλαμβάνουν τη δημιουργία μόνιμων αρχείων και την αυτόματη εκτέλεση έξυπνων συμβολαίων και την παροχή ορατών και κοινόχρηστων πληροφοριών. Ο κλάδος υιοθετεί τον ψηφιακό μετασχηματισμό και η τεχνολογία blockchain αποτελεί βασικό πυλώνα που υποστηρίζει την επιχειρησιακή αποτελεσματικότητα, την πλήρη αξιοπιστία και τη μακροπρόθεσμη βιωσιμότητα (Farah et al., 2024; Liu et al., 2023).

Θεωρητικό Υπόβαθρο

Η ναυτιλιακή εφοδιαστική απολαμβάνει επί του παρόντος πολυάριθμων ερευνητικών ευρημάτων σχετικά με τον τρόπο χρήσης του blockchain. Αρκετές μελέτες έχουν καταδείξει και αξιολογήσει εφαρμογές blockchain για την ασφαλή μετάδοση εγγράφων και την παρακολούθηση αποστολών, καθώς και για την ενίσχυση της συνεργασίας μεταξύ λιμένων, ναυτιλιακών εταιρειών και ρυθμιστικών φορέων (Farah et al., 2024). Μερικά από τα σημαντικά πιλοτικά προγράμματα είναι το TradeLens από την IBM/Maersk, το Global Shipping Business Network (GSBN) από την CargoSmart και το Silsal από τα Abu Dhabi Ports, τα οποία δείχνουν πώς το blockchain μπορεί να χρησιμοποιηθεί σε ψηφιακή γραφειοκρατία από άκρο σε άκρο και στην ασφαλή ανταλλαγή πληροφοριών στη ναυτιλία (Irannezhad, 2020; Abu Dhabi Ports, 2018).

Τεχνικές Προκλήσεις και Προβληματισμοί

Η υιοθέτηση του blockchain σε ολόκληρη την αλυσίδα εφοδιασμού της ναυτιλίας αντιμετωπίζει σημαντικά εμπόδια. Τα τεχνικά προβλήματα αφορούν τον συνδυασμό με τα υπάρχοντα παλιά λιμενικά συστήματα, την ικανότητα διαχείρισης μεγάλου όγκου συναλλαγών και την ανάγκη για ισχυρή κυβερνοασφάλεια (Surucu-Balci et al., 2024). Μια άλλη πρόκληση για την υιοθέτηση είναι η αντίσταση των οργανισμών στην αλλαγή, το υψηλό αρχικό κόστος, τα ασυνεπή πρότυπα δεδομένων και οι περίπλοκοι κανονισμοί (Η ναυτιλιακή βιομηχανία επιταχύνει..., 2025). Οι παγκόσμιες αλυσίδες εφοδιασμού είναι κατακερματισμένες και επομένως είναι δύσκολο να διασφαλιστεί ότι όλα τα μέρη λειτουργούν στις ίδιες διαλειτουργικές πλατφόρμες blockchain, αν και η DCSA και η BIMCO έχουν ξεκινήσει πρωτοβουλίες τυποποίησης (Farah et al., 2024).

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Η εφοδιαστική αλυσίδα της ναυτιλίας χρησιμοποιεί τρεις κύριες εφαρμογές της τεχνολογίας blockchain σύμφωνα με τους Liu et al. (2023). Το σύστημα επιτρέπει στις επιχειρήσεις να δημιουργούν ψηφιακά έγγραφα, όπως ηλεκτρονικές φορτωτικές και πιστοποιητικά προέλευσης, μέσω αυτοματοποίησης επιχειρηματικών διαδικασιών που βασίζονται σε έξυπνες συμβάσεις και βελτιωμένου συντονισμού και ιχνηλασιμότητας της εφοδιαστικής αλυσίδας. Η πλατφόρμα TradeLens παρέχει ασφαλή ψηφιακή διαχείριση εγγράφων μαζί με άμεση παρακολούθηση φορτίου, σύμφωνα με τον Irannezhad (2020). Η πλατφόρμα Silsal στα λιμάνια του Άμπου Ντάμπι επιτρέπει την ασφαλή επαλήθευση ταυτότητας και τη διαχείριση εγγράφων για όλους τους συμμετέχοντες στην εφοδιαστική αλυσίδα, σύμφωνα με τον Irannezhad (2020). Το Παγκόσμιο Δίκτυο Επιχειρήσεων Ναυτιλίας (GSBN) συνεργάζεται για την ανάπτυξη ψηφιακών πλατφορμών ναυτιλίας σύμφωνα με τα ευρήματά τους για μειωμένες διοικητικές διαδικασίες και ταχύτερες συναλλαγές, σύμφωνα με τους Λιμένες του Άμπου Ντάμπι (2018) και τους Farah et.al (2024).

Εφαρμογές και Σενάρια Χρήσης

Ορισμένες εφαρμογές του blockchain στην πραγματική ζωή στον ναυτιλιακό τομέα περιλαμβάνουν ασφαλή και εύχρηστα συστήματα παρακολούθησης εμπορευματοκιβωτίων και αυτοματοποιημένες τελωνειακές

διαδικασίες, καθώς και απομακρυσμένη παρακολούθηση εμπορευματοκιβωτίων-ψυγείων. Σύμφωνα με τους Farah et al. (2024), το σύστημα μπορεί επίσης να χρησιμοποιηθεί για τη διαχείριση ψηφιακών φορτωτικών. Η επιχείρηση αποτελείται πλέον από περισσότερους από εκατό οργανισμούς που μπορούν να παρακολουθούν τις αποστολές τους μέσω του συστήματος TradeLens ή να εκτελωνίζουν αυτόματα τα τελωνεία τους και να μειώνουν αυτές τις χρονοβόρες διαφωνίες, όπως εξηγείται από τους Liu et al. (2023). Στα λιμάνια του Άμπου Ντάμπι, η Silsal συνδέει τους χρήστες χρησιμοποιώντας ψηφιακές ταυτότητες, κρυπτογράφηση ευαίσθητων εγγράφων και απλώς παρακολούθηση της ροής των αγαθών, AbuDhabiPorts (2018). Σύμφωνα με τον Irannezhad (2020), αυτές οι μελέτες δείχνουν ότι η εφαρμογή του blockchain στην εφοδιαστική αλυσίδα της ναυτιλίας ενισχύει την ταχύτητα, την ασφάλεια και την εμπιστοσύνη.

Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Εξακολουθούν να υπάρχουν σημαντικά κενά στην αποδοχή του blockchain, στην ενσωμάτωση συστημάτων και στην ορθή αξιολόγηση του κόστους και του οφέλους της εφαρμογής σε μεγάλη κλίμακα (Surucu-Balci et al, 2024). Υπάρχει ανάγκη για έρευνα στην ενοποίηση των διεθνών προτύπων δεδομένων (όπως τα DCSA και BIMCO), στην προστασία της ιδιωτικής ζωής της τεχνολογίας blockchain και σε μελέτες πραγματικού κόσμου για ολόκληρες εφαρμογές της αλυσίδας εφοδιασμού (Farah et al., 2024). Η ενσωμάτωση του blockchain με το Διαδίκτυο των Πραγμάτων και την τεχνητή νοημοσύνη θα μπορούσε να καταστήσει το σύστημα ακόμη ισχυρότερο και πιο αποτελεσματικό, και μέσω της συνεργασίας πολλαπλών ενδιαφερομένων μερών μπορεί να υιοθετηθεί σε ολόκληρο τον κλάδο (Η ναυτιλιακή βιομηχανία επιταχύνει..., 2025).

4.6: Συστήματα Ανίχνευσης Εισβολών (IDS) στη Ναυτιλία

Σπουδαιότητα και Σκοπιμότητα της Έρευνας

Η εκτεταμένη ψηφιοποίηση των ναυτιλιακών δραστηριοτήτων, σε συνδυασμό με τη βελτιωμένη διασυνδεσιμότητά τους, τις έχει καταστήσει πιο ευάλωτες σε διαδικτυακές απειλές. Το Σύστημα Ανίχνευσης Εισβολών (IDS) είναι ένα κρίσιμο εργαλείο για την προστασία των δικτύων πλοίων και λιμένων από τις εξελισσόμενες κυβερνοεπιθέσεις που θέτουν σε κίνδυνο τα ψηφιακά τους περιουσιακά στοιχεία και τις κρίσιμες για την ασφάλεια λειτουργίες τους (Indian Register of Shipping, 2024; Melnyk et al., 2025).

Θεωρητικό Υπόβαθρο

Η βιβλιογραφία σχετικά με τα Συστήματα Ανίχνευσης Ναυτιλιακών Εισβολών συζητά τις απειλές που επηρεάζουν τη ναυτιλιακή βιομηχανία και την τεχνολογία αιχμής που χρησιμοποιεί τεχνικές Τεχνητής Νοημοσύνης και μηχανικής μάθησης. Οι μελέτες δείχνουν ότι οι κυβερνοεπιθέσεις στη ναυτιλιακή βιομηχανία (σε λιμάνια ή σε πλοία) μπορούν να οδηγήσουν σε σοβαρές λειτουργικές διαταραχές, οικονομικές ζημίες και κινδύνους για την ασφάλεια. Το περιστατικό της Maersk και οι επιθέσεις στο λιμάνι της Βαρκελώνης και στην DP World Australia χρησιμεύουν ως παραδείγματα σημαντικών περιπτώσεων που καταδεικνύουν πώς οι κυβερνοαπειλές επηρεάζουν ολοένα και περισσότερο τις θαλάσσιες υποδομές. Οι προηγούμενες και οι τρέχουσες κυβερνοεπιθέσεις έχουν οδηγήσει σε έρευνα για τα IDS που βασίζονται σε δίκτυα και τα IDS που βασίζονται σε κεντρικούς υπολογιστές, και η τελευταία έρευνα καταδεικνύει πώς τα μοντέλα μηχανικής μάθησης μπορούν να εντοπίσουν ασυνήθιστη συμπεριφορά σε ναυτιλιακά δίκτυα (Melnyk et al., 2025 Vaarandi et al., 2025).

Τεχνικές Προκλήσεις και Προβληματισμοί

Τα Συστήματα Ανίχνευσης Ναυτιλιακών Εισβολών (IDS) αντιμετωπίζουν σαφή εμπόδια, καθώς λειτουργούν σε απομακρυσμένες τοποθεσίες με ασταθείς συνδέσεις χαμηλού εύρους ζώνης που συνδέουν παλιά και νέα συστήματα υπολογιστών, ενώ παράλληλα αντιμετωπίζουν δύσκολες θαλάσσιες συνθήκες. Τα τυπικά συστήματα IDS χρειάζονται συχνές ενημερώσεις και καθιερωμένα όρια δικτύου που δεν ταιριάζουν με την προσαρμόσιμη δομή περιορισμένων πόρων των πλοίων και των λιμενικών εγκαταστάσεων. Το μεγάλο

πρόβλημα με τα ψευδώς θετικά αποτελέσματα μεταξύ των προγραμμάτων αναζήτησης είναι ότι δημιουργούν περιττές προειδοποιήσεις που διακόπτουν σοβαρά τις ναυτιλιακές δραστηριότητες όπου η ανθρώπινη παρέμβαση έχει υψηλό κόστος και λίγους διαθέσιμους εργαζόμενους (Indian Register of Shipping, 2024; Melnyk et al., 2025).

Υφιστάμενες Τεχνολογίες και Μεθοδολογικές Προσεγγίσεις

Το Ναυτιλιακό Σύστημα Πληροφοριών (IDS) βασίζεται επί του παρόντος στην ανίχνευση βάσει υπογραφών για την ανίχνευση γνωστών απειλών και χρησιμοποιεί μοντέλα ανίχνευσης βασισμένα σε ανωμαλίες για τον εντοπισμό άγνωστων επιθέσεων. Τα τελευταία ερευνητικά ευρήματα δείχνουν ότι οι περισσότεροι ερευνητές έχουν υιοθετήσει προσεγγίσεις που βασίζονται στην Τεχνητή Νοημοσύνη (AI), οι οποίες χρησιμοποιούν τόσο εποπτευόμενα όσο και μη εποπτευόμενα μοντέλα μηχανικής μάθησης, μαζί με τεχνικές συνόλων και μοντέλα βαθιάς μάθησης για την αύξηση της ακρίβειας ανίχνευσης. Τα δεδομένα φυσικής ασφάλειας που περιλαμβάνουν συστήματα ελέγχου πρόσβασης και περιβαλλοντικούς αισθητήρες συνδυάζονται όλο και περισσότερο με δεδομένα τηλεμετρίας δικτύου στα Υβριδικά συστήματα IDS. Μια ολοκληρωμένη αξιολόγηση διαφόρων πηγών ναυτιλιακών δεδομένων μπορεί να επιτευχθεί μέσω εξελιγμένων συστημάτων ασφαλείας που ενσωματώνουν συστήματα Πληροφοριών Ασφάλειας και Διαχείρισης Συμβάντων (SIEM). Η τεχνολογία Blockchain ενσωματώνεται στις περισσότερες λύσεις IDS ως τρόπος δημιουργίας αμετάβλητων εγκληματολογικών αρχείων. Το Ινδικό Μητρώο Ναυτιλίας έχει εκδώσει σύσταση ότι η ανάπτυξη ενός IDS αποτελεί καλή πρακτική (Indian Register of Shipping, 2024), (Melnyk et al., 2025), (Jahan et al., 2024).

Εφαρμογές και Σενάρια Χρήσης

Τα λειτουργικά IDS που είναι εγκατεστημένα σε έξυπνα λιμάνια και προηγμένα πλοία είναι σε θέση να εντοπίζουν και να ανταποκρίνονται σε στοχευμένες επιθέσεις, επιθέσεις DDoS και απόπειρες μη εξουσιοδοτημένης πρόσβασης στο δίκτυο. Σύμφωνα με μελέτες περιπτώσεων, τα προσαρμοστικά IDS μηχανικής μάθησης, που αναπτύσσονται στην άκρη του δικτύου με τη βοήθεια του Multi-Access Edge Computing (MEC), παρέχουν υψηλό επίπεδο ανίχνευσης και χαμηλό αριθμό ψευδών συναγερμών. Οι πρακτικές εφαρμογές περιλαμβάνουν την ασφάλεια των λιμένων, τα δίκτυα ελέγχου πλοίων και τις υποδομές πλοίων, δείχνοντας ότι τα IDS δεν είναι μόνο τεχνολογικά εφικτά αλλά και απαραίτητα στις καθημερινές λειτουργίες (Jahan et al., 2024; Melnyk et al., 2025).

Μελλοντικές Κατευθύνσεις και Ερευνητικά Κενά

Οι επόμενες μελέτες πρέπει να βελτιώσουν τα IDS ώστε να παραμένουν αποτελεσματικά στο συνεχώς μεταβαλλόμενο τοπίο απειλών, καθώς και να τα διατηρήσουν στο συνεχώς μεταβαλλόμενο τοπίο απειλών, και να ενσωματώσουν τα συστήματα cloud.edge για την εκτέλεση ανάλυσης σε πραγματικό χρόνο και να τυποποιήσουν τις πηγές ναυτιλιακών πληροφοριών για την καθολική καθιέρωση του συστήματος. Οι τομείς ευκαιρίας είναι η ενσωμάτωση των μοντέλων IDS υπογραφών και συμπεριφοράς, η βελτιωμένη επικοινωνία μεταξύ των συστημάτων και η προσθήκη blockchain για την ενίσχυση της ακεραιότητας των δεδομένων. Υπάρχει ακόμη ερευνητική εργασία που πρέπει να γίνει για την ανάπτυξη παγκοσμίως τυποποιημένων πρωτοκόλλων και μεγάλων, αντιπροσωπευτικών συνόλων δεδομένων ναυτιλιακού κυβερνοχώρου για την ανάπτυξη ανώτερων και καθολικά εφαρμόσιμων IDS (Melnyk et al., 2025; Jahan et al., 2024).

Συμπέρασμα

Αυτό το κεφάλαιο παρείχε μια δομημένη επισκόπηση ενός πολυεπίπεδου πλαισίου κυβερνοασφάλειας, απαραίτητου για τη σύγχρονη ναυτιλιακή βιομηχανία. Εξετάζοντας συστηματικά έξι κρίσιμους πυλώνες — ασφάλεια Επιχειρησιακής Τεχνολογίας (OT), μοντελοποίηση απειλών πλοίου-ξηράς, Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust), προστασία κρίσιμων υποδομών, εφαρμογές blockchain και Συστήματα Ανίχνευσης Εισβολών (IDS)— καθίσταται προφανές ότι μια ισχυρή άμυνα δεν είναι μια μεμονωμένη λύση αλλά μια βαθιά ολοκληρωμένη στρατηγική. Η συζήτηση ανέδειξε τις μοναδικές προκλήσεις που θέτει το

ναυτιλιακό περιβάλλον, συμπεριλαμβανομένης της σύγκλισης παλαιών και σύγχρονων συστημάτων, των περιορισμών της διακοπτόμενης συνδεσιμότητας και της τεράστιας γεωγραφικής κλίμακας των λειτουργιών. Το κεφάλαιο συνέθεσε τρέχουσες τεχνολογίες και προσεγγίσεις, καταδεικνύοντας μια σαφή τάση προς πιο δυναμικά, ευφυή και επικεντρωμένα στα δεδομένα μέτρα ασφαλείας, απομακρυνόμενα από στατικές άμυνες βασισμένες στην περίμετρο.

Κύρια Συμπεράσματα:

- **Η άμυνα σε βάθος είναι υποχρεωτική:** Μια ανθεκτική στάση ναυτιλιακής κυβερνοασφάλειας δεν μπορεί να βασίζεται σε ένα μόνο σημείο αποτυχίας. Απαιτεί αλληλεπικαλυπτόμενα επίπεδα ασφάλειας, από τη σκλήρυνση φυσικών συστημάτων OT και τη μοντελοποίηση απειλών έως την εφαρμογή ελέγχων πρόσβασης με επίκεντρο την ταυτότητα και την παρακολούθηση σε πραγματικό χρόνο.
- **Ο ανθρώπινος παράγοντας είναι μια κρίσιμη ευπάθεια και περιουσιακό στοιχείο:** Σε πολλαπλές ενότητες, η έλλειψη τεχνογνωσίας κυβερνοασφάλειας επί του σκάφους και ο κίνδυνος ανθρώπινου λάθους εντοπίστηκαν ως σημαντικές προκλήσεις. Αντίθετα, η αποτελεσματική εκπαίδευση και ευαισθητοποίηση του πληρώματος αναφέρονται σταθερά ως κρίσιμα συστατικά οποιασδήποτε επιτυχημένης στρατηγικής ασφάλειας.
- **Η ακεραιότητα των δεδομένων και η εμπιστοσύνη είναι υψίστης σημασίας:** Η διερεύνηση του Zero Trust και του blockchain αποκαλύπτει μια θεμελιώδη στροφή προς συστήματα που δεν εμπιστεύονται σιωπηρά κανέναν χρήστη ή συσκευή. Αντίθετα, η συνεχής επαλήθευση και τα αμετάβλητα αρχεία γίνονται το νέο πρότυπο για τη διασφάλιση της ακεραιότητας των δεδομένων και τη διευκόλυνση της εμπιστοσύνης σε ένα κατακερματισμένο οικοσύστημα πολλών ενδιαφερομένων.
- **Η προληπτική και προσαρμοστική ασφάλεια είναι το μέλλον:** Η αυξανόμενη εξάρτηση από IDS που βασίζονται στην TN και η ανάγκη για δυναμικά μοντέλα απειλών σηματοδοτούν μια μετάβαση από την αντιδραστική στην προληπτική ασφάλεια. Τα μελλοντικά συστήματα πρέπει να είναι σε θέση να προβλέπουν και να προσαρμόζονται σε αναδυόμενες απειλές σε πραγματικό χρόνο.

Περιορισμοί και Ερευνητικά Κενά:

- *Τρέχοντες Τεχνικοί Περιορισμοί:* Ένας πρωταρχικός περιορισμός είναι η δυσκολία εκ των υστέρων εφαρμογής (retrofitting) σύγχρονων λύσεων ασφαλείας σε παλαιά συστήματα OT χωρίς τη διακοπή των λειτουργιών. Επιπλέον, η υψηλή καθυστέρηση και το χαμηλό εύρος ζώνης των δορυφορικών επικοινωνιών εμποδίζουν την αποτελεσματικότητα κεντρικών αρχιτεκτονικών ασφαλείας σε πραγματικό χρόνο όπως το Zero Trust.
- *Εντοπισμένα Ερευνητικά Κενά:* Ένα επαναλαμβανόμενο κενό σε όλους τους πυλώνες είναι η ανάγκη για μεγάλης κλίμακας, ειδικά για τη ναυτιλία σύνολα δεδομένων για την εκπαίδευση και την επικύρωση μοντέλων ασφαλείας που βασίζονται στην TN. Απαιτείται επίσης περαιτέρω έρευνα για την ανάπτυξη και τη δοκιμή κατανεμημένων μηχανισμών επιβολής πολιτικής ασφαλείας που μπορούν να λειτουργούν αξιόπιστα κατά τη διάρκεια περιόδων αποσύνδεσης δικτύου. Τέλος, υπάρχει έλλειψη εμπειρικών, διαχρονικών μελετών σχετικά με την ανάλυση κόστους-οφέλους της εφαρμογής αυτών των προηγμένων μέτρων ασφαλείας σε έναν στόλο.
- *Εμπόδια Εφαρμογής:* Τα πιο σημαντικά εμπόδια στην εφαρμογή είναι το υψηλό αρχικό κόστος, η σπανιότητα εξειδικευμένων επαγγελματιών ναυτιλιακής κυβερνοασφάλειας και η έλλειψη παγκοσμίως εναρμονισμένων κανονισμών και προτύπων, γεγονός που δημιουργεί ένα πολύπλοκο και συχνά αντιφατικό τοπίο συμμόρφωσης.

Ερευνητικές Συνεισφορές:

Το παρόν κεφάλαιο θεμελιώνει την κρίσιμη βάση κυβερνοασφάλειας που είναι απαραίτητη για το Ναυτιλιακό Διαδίκτυο των Πραγμάτων. Συνθέτοντας την τελευταία λέξη της τεχνολογίας σε αυτούς τους έξι πυλώνες, παρέχει ένα ολιστικό πλαίσιο που ενημερώνει την ανάπτυξη και την ανάπτυξη των πιο

προηγμένων αυτόνομων συστημάτων και πλατφορμών ανάλυσης δεδομένων που συζητούνται στα επόμενα κεφάλαια. Γεφυρώνει το χάσμα μεταξύ του φυσικού επιπέδου και του επιπέδου επικοινωνίας του MIoT και των ευφυών εφαρμογών που βασίζονται σε δεδομένα, οι οποίες εξαρτώνται από μια ασφαλή και αξιόπιστη υποδομή. Αυτό το πλαίσιο χρησιμεύει ως ζωτική προϋπόθεση για την πραγματοποίηση του πλήρους δυναμικού ενός συνδεδεμένου και αυτόνομου ναυτιλιακού μέλλοντος.

Βιβλιογραφία

Abu Dhabi Ports. (2018, June 2). *Abu Dhabi Ports launches blockchain technology for trade community*. https://www.adports.ae/abu-dhabi-ports-launches-blockchain-technology-for-trade-community/

Azad, M. A., et al. (2024). Verify and trust: A multidimensional survey of zero-trust. *Journal of Information Security and Applications, 82*, 103791.

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, & IUMI. (2024). *The guidelines on cyber security onboard ships* (5th ed.). BIMCO.

Cyble. (2025). *Hacktivists, nation-state hackers target global maritime infrastructure as cyberattacks, GPS spoofing surge*.

EEAS, European External Action Service. (2025). *EU maritime security exercise strengthens protection of critical maritime infrastructure*.

Farah, M. B., Iris, Ç., Hassani, H., & Pazienza, P. (2024). A survey on blockchain technology in the maritime industry. *Future Generation Computer Systems, 157*, 618–637.

Hopcraft, T., Oruc, B., & Kapalidis, E. (2024). Comprehensive analysis of maritime cybersecurity landscape—The role of frameworks and risk assessment. *Journal of Marine Science and Engineering, 12*(5), 919.

IASME. (2025). *Overcoming Threats and Building Resilience: A Maritime Cyber Risk Strategy*.

Indian Register of Shipping. (2024). *Guidelines on Maritime Cyber Safety* (Revision 1).

International Maritime Organization. (2022). *Maritime cyber risk management in safety management systems* (IMO Resolution MSC.428(98)). IMO.

Irannezhad, E. (2020). The architectural design requirements of a blockchain-based port community system. *Logistics, 4*(4), 30.

Jahan, T., Islam, M. S., & Rahman, R. (2024). Mitigating maritime cybersecurity risks using AI-based intrusion detection systems and network automation during extreme environmental conditions. *International Journal of Scientific Research in Multidisciplinary Techniques, 3*(10), Article 73.

Li, M., Zhou, J., Chattopadhyay, S., & Goh, M. (2024). Maritime cybersecurity: A comprehensive review. *arXiv preprint arXiv:2409.11417*.

Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy, 155*, 105772.

Liu, J., Chen, X., Wang, Y., & Lam, J. S. L. (2023). Blockchain technology in maritime supply chains. *International Journal of Production Research, 61*(11), 3543–3559.

MARSEC-COE, Maritime Security Centre of Excellence. (2023). *Maritime Critical Infrastructure Protection (MCIP)*.

Maritime industry accelerates shift toward digital trade. (2025, January 30). *Offshore Energy*.

Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cybersecurity in maritime transport: An international perspective on regulatory frameworks and countermeasures. *Lex Portus, 11*(1), 7–19.

O'Dwyer, G. (2023). *Maritime Cyber Attack Database (MCAD)*.

PRECINCT Project. (2024). *The PRECINCT Ecosystem Platform for Critical Infrastructure Protection*.

Rødseth, H., Nesheim, H. I., & Stenumgård, P. (2022). Security and independence of process safety and control systems in offshore facilities. *Journal of Cybersecurity and Privacy, 2*(1), 1–38.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST SP 800-207). National Institute of Standards and Technology.

Sahay, R., Sepulveda Estay, D. A., Meng, W., Jensen, C. D., & Barfod, M. B. (2022). A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS frameworks. *arXiv preprint arXiv:2212.10830*.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82r3). National Institute of Standards and Technology.

Surucu-Balci, E., Iris, Ç., & Balci, G. (2024). Digital information in maritime supply chains with blockchain and cloud platforms: Supply chain capabilities, barriers, and research opportunities. *Technological Forecasting and Social Change, 198*, 122978.

US Coast Guard. (2024). *Cyber Trends and Insights in the Marine Environment (CTIME Report)*.

Vaarandi, R., Tsiopoulos, L., Visky, G., Rehman, M. U., & Bahsi, H. (2025). Literature review: Cyber security monitoring in maritime. *arXiv*.