ΑΚΑΔΗΜΙΑ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΙΩΑΝΝΙΔΗΣ ΑΡΓΥΡΗΣ

ΘΕΜΑ

MARITIME CYBER RISKS
Ποιούς κινδύνους συντρέχει και ποιές προφυλάξεις και εκπαίδευση πρέπει να πάρει η ναυτιλιακή κοινότητα

ΤΟΥ ΣΠΟΥΔΑΣΤΗ: ΤΡΑΓΑΚΗ ΚΩΝΣΤΑΝΤΙΝΟΥ
Α.Γ.Μ:4253

Ημερομηνία ανάληψης της εργασίας: ***18/05/2020***

Ημερομηνία παράδοσης της εργασίας:

Ο ΔΙΕΥΘΥΝΤΗΣ ΣΧΟΛΗΣ : ΤΣΟΥΛΗΣ ΝΙΚΟΛΑΟΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αναφέρεται στην σημασία των όρων Maritime Cyber Risks και Maritime Cyber Security, πώς και γιατί αυτοί οι όροι εδραιώθηκαν μαζί με την άφιξη της τεχνολογίας στη ναυτιλία. Θα γίνει επίσης αναφορά στην πρόληψη, την αντιμετώπιση και στον ρόλο του IMO σε αυτήν την προσπάθεια εξασφάλισης της ομαλής λειτουργίας της παγκόσμιας εμπορικής ναυτιλίας και κατ' επέκταση του παγκόσμιου στόλου.

ΕΙΣΑΓΩΓΗ

Με την ταχύτητα και τους ρυθμούς που εξελίσσεται η τεχνολογία ήταν θέμα χρόνου να εισέλθει και να ριζώσει στον τομέα της ναυτιλίας. Παρόλες τις διευκολύνσεις που επέφερε η τεχνολογία και το διαδίκτυο, μαζί του έφερε κινδύνους και την ανάγκη για προφύλαξη από αυτούς. Έτσι έχουμε τους όρους «cyber risks» και «cyber security» να αποκτούν και αυτοί μια θέση στη ναυτιλία η οποία αποτελεί βασικό πυλώνα στην παγκόσμια οικονομία. Πράγματι, ακόμα και σήμερα η πλειονότητα των αγαθών μεταφέρεται μέσω της θάλασσας και των εμπορικών πλοίων. Είναι λοιπόν αυτονόητο ότι μια αναστάτωση ή δολιοφθορά στην παγκόσμια αλυσίδα μεταφοράς πετρελαιοειδών, φαγητών ή άλλων πρώτων υλών θα προκαλούσε αξιοσημείωτη ζημιά στην παγκόσμια οικονομία. Η χρήση των ηλεκτρονικών, καθώς και των δορυφορικών συστημάτων δημιουργούν επίσης σοβαρούς κινδύνους στην ασφάλεια τόσο του πλοίου και του φορτίου του, όσο και του πληρώματος. Είχαν σημειωθεί το 2019 πάνω από 310 παραβιάσεις ηλεκτρονικών συστημάτων και εκτιμάται ότι με το τέλος του 2020 θα έχουμε πάνω από 500 επίσημα καταγεγραμμένες παραβιάσεις σύμφωνα με τον Robert Rizika, επικεφαλή της Naval Dome's Boston-based of North American Operations.

ΚΕΦΑΛΑΙΟ 1: CYBER RISKS

1.1 Σύγχρονα ναυτιλιακά όργανα και κίνδυνοι

Στην σύγχρονη ναυτιλία τα πλοία εξαρτούνται από τεχνολογίες, όπως το ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), Radar/ARPA(Radio Direction and Ranging) / (Automatic Radar Plotting Aid), Compass (Gyro, Fluxgate, GPS and others), Steering (Computerized Automatic Steering System), VDR (Voyage Data Recorder), GMDSS (Global Maritime Distress and Safety System) και πολλές άλλες προηγμένες μονάδες και συστήματα. Όλα αυτά αποτελούν συστήματα εκτεθειμένα σε πιθανή επίθεση στον κυβερνοχώρο. Ας πάρουμε για παράδειγμα το σύστημα ECDIS το οποίο είναι στην ουσία ένας υπολογιστής που χρησιμοποιείται για την προβολή χαρτών σαν εναλλακτική των χάρτινων χαρτών. Αυτό το σύστημα όμως σου δίνει κι άλλες δυνατότητες πέρα από την απλή προβολή του εκάστοτε χάρτη. Έτσι έχουμε ένα πλήθος πληροφοριών σε «ζωντανό» χρόνο και συμβάλλει στην σημαντικά στην λήψη αποφάσεων, προβάλει συνεχώς την θέση του πλοίου σε σχέση με την στεριά, χαρτογραφημένα αντικείμενα, προειδοποιήσεων που έχουν σχέση με την πλοήγηση και γενικών κινδύνων. Συνδέεται με το GPS για την υπόδειξη της θέσεως και άλλα ναυτιλιακά όργανα όπως το ραντάρ, το βυθόμετρο, το AIS. Η χρήση τέτοιων συστημάτων έχει συμβάλλει σημαντικά στην μείωση του πληρώματος σήμερα, σε σημείο που η τήρηση φυλακής οριακά είναι δυνατόν να εκτελεστεί από ένα άτομο.

Έχοντας λοιπόν υπόψη την σημασία του ECDIS όσον αφορά την πλοήγηση είναι ξεκάθαρο το ότι σε μία ενδεχόμενη επίθεση εάν αποκτούσαν πρόσβαση και άλλαζαν δεδομένα στο σύστημα αυτό θα οδηγούσε σε αναξιόπιστα δεδομένα και πιθανότατα σε επικίνδυνες πληροφορίες και καταστάσεις. Τα αποτελέσματα θα ήταν σοβαρά καθώς θα προκαλούνταν σοβαρές περιβαλλοντικές και οικονομικές φθορές.

Τον Ιανουάριο του 2013, η ομάδα του NCC (εταιρεία παροχής πληροφοριών που εδρεύει στο Μάντσεστερ του Ηνωμένου Βασιλείου) προσπάθησε να εισχωρήσει σε ένα σύστημα ECDIS γνωστού κατασκευαστή. Βρέθηκαν συγκεκριμένες αδυναμίες στην ασφάλεια του, όπως η δυνατότητα ανάγνωσης, λήψης, αντικατάστασης ή διαγραφής οποιουδήποτε αρχείου στον υπολογιστή που υποστηρίζει το ECDIS. Μια τέτοια πρόσβαση μπορεί να οδηγήσει στην εισχώρηση του δικτύου στο πλοίο και όλων των συστημάτων που είναι συνδεδεμένα σε αυτό και να προκαλέσει χάος. Αυτό είναι δυνατόν να γίνει με τη χρήση ενός απλού USB ή μέσω ίντερνετ.

Το σύστημα AIS έχει οριστεί από τον IMO (International Maritime Organization), ως υποχρεωτικό όργανο τόσο σε επιβατηγά όσο και σε εμπορικά (εκτός από ασχολούμενα με αλιεία) πλοία που ξεπερνούν τους 300 μετρικούς τόνους. Το AIS εντοπίζει αυτόματα το πλοίο συνδέοντας δεδομένα με άλλα πλοία, βάσεις δεδομένων του AIS και δορυφόρους. Το σύστημα

αυτό επιτρέπουν στα πλοία να ανταλλάζουν δεδομένα με άλλα πλοία. Σε περίπτωση cyber attack θα μπορούσαν να παραποιηθούν οι πληροφορίες που παρέχει το AIS και να δοθούν εσφαλμένα δεδομένα όπως ταυτότητα ή μέγεθος πλοίου καθώς και θέση, πορεία και ταχύτητα. Θα μπορούσε ακόμα να χρησιμοποιηθεί για να αναγκάσει ένα πλοίο να αλλάξει πορεία είτε κάνοντας το να νομίζει πως αποφεύγει ένα άλλο πλοίο το οποίο στην πραγματικότητα δεν υπάρχει είτε στέλνοντας ψεύτικο δελτίο καιρού. Ένας ακόμα τρόπος είναι να χρησιμοποιηθεί ώστε να παραστήσει ο επιτιθέμενος τις αρχές και να αναγκάσει το πλοίο να κλείσει το AIS του ώστε οι πραγματικές αρχές να μην το εντοπίζουν παρά μόνο ο ίδιος. Ένα παράδειγμα τέτοιας επίθεσης που ονομάζεται «frequency hopping attack» είναι η εκμετάλλευση της δυνατότητας των σταθμών και των αρχών να δίνουν οδηγίες για αλλαγή σε συγκεκριμένη συχνότητα χρήσης του AIS. Με αυτόν τον τρόπο το πλοίο θα σταματούσε να στέλνει και να λαμβάνει δεδομένα σε σωστή συχνότητα με αποτέλεσμα να «εξαφανιστεί» και να μην μπορεί να επικοινωνήσει. Έχουν καταγγελθεί επίσης στη Σομαλία περιπτώσεις όπου προτρέπουν τα πλοία να κλείσουν τις συσκευές πλοήγησης τους ή να βάλουν εσφαλμένα δεδομένα κάνοντας τα να φαίνονται πως βρίσκονται αλλού.

Ένα ακόμα πολύ χρήσιμο εργαλείο για την ναυτιλία, και όχι μόνο, είναι το GPS (Global Positioning System) το οποίο είναι εξίσου ευάλωτο σε πιθανή επίθεση. Μάλιστα το GPS συνδέεται με πληθώρα συσκευών σε μία γέφυρα καθώς στέλνει και λαμβάνει πληροφορίες. Συμπεραίνουμε λοιπόν ότι μια επιτυχημένη επίθεση που θα έδινε πρόσβαση στο GPS θα επηρέαζε όλα τα όργανα όπου συνδέεται. Το 2013 μια επίδειξη από την ερευνητική ομάδα του Πανεπιστημίου του Texas-Austin έδειξε πως ένας πιθανός «αντίπαλος» θα μπορούσε να αποκτήσει εξ αποστάσεως τον έλεγχο ενός πλοίου χρησιμοποιώντας το Παγκόσμιο Σύστημα Εντοπισμού Θέσης(Global Positioning System). Το σκάφος «White Rose of Drax» ενώ έπλεε στην Μεσόγειο Θάλασσα, χρησιμοποιήθηκε από την ερευνητική ομάδα και στέλνοντας ψεύτικα σήματα GPS από την στεριά κατάφεραν σιγά-σιγά να υπερισχύσουν του πραγματικού σήματος GPS και να αποκτήσουν τον έλεγχο του συστήματος πλοήγησης του σκάφους. Σύμφωνα με τον καθηγητή Todd Humphreys, συγγραφέα της μελέτης, «Το σκάφος πραγματικά γύριζε και μπορούσαμε να το αισθανθούμε όλοι, αλλά η οπτική ένδειξη του χάρτη και το πλήρωμα είδε μια ευθεία γραμμή». Να σημειωθεί πως το GPS και τα συστήματα πλοήγησης ήταν αυτά που χρησιμοποιούνται κανονικά στα πλοία κάνοντας το «White Rose of Drax» δύσκολο «θήραμα».

1.2 Κίνδυνοι των φορτίων

Με τον τρόπο που λειτουργούν τα λιμάνια σήμερα σε όλο τον κόσμο, καθίστανται εξαρτημένα από ένα σύνθετο σύστημα το οποίο επιτρέπει την παρακολούθηση και τον εντοπισμό του φορτίου καθ'όλη τη διάρκεια μεταφοράς του ώσπου αυτό να φτάσει στον τελικό παραλήπτη. Όσο χρήσιμο και να είναι αυτό δεν παύει να είναι ευάλωτο σε ανάλογες επιθέσεις όπου θα προκαλούσαν εν δυνάμει σημαντικά προβλήματα. Ας δούμε για παράδειγμα, το λιμάνι της Αμβέρσας στο Βέλγιο, το οποίο αποτελεί ένα από τα μεγαλύτερα λιμάνια της Ευρώπης και του κόσμου. Όπως όλα τα σύγχρονα συστήματα διαχείρισης φορτίου έτσι και τα containers έχουν έναν αριθμό αναφοράς ώστε να παρακολουθούνται από τους ενδιαφερόμενους, δίνοντας έτσι πληροφορίες για την άφιξη, τη θέση και την προγραμματισμένη παραλαβή του από το λιμάνι. Κατά την περίοδο 2011 με 2013 hackers οι οποίοι κατάφεραν να εισβάλουν στο σύστημα του λιμανιού, είχαν πλέον πρόσβαση σε αυτές τις πληροφορίες και τις εκμεταλλεύτηκαν βάζοντας ναρκωτικά σε συγκεκριμένα containers πριν την προγραμματισμένη παραλαβή-

φόρτωση. Έτσι με αυτόν τον τρόπο μπορούσαν να ξέρουν τα πάντα για τα containers που τους ενδιέφεραν και να ενημερώσουν τους δικούς τους παραλήπτες για την παραλαβή των ναρκωτικών χωρίς να γνωρίζει τίποτα, ούτε τα λιμάνια φόρτωσης και εκφόρτωσης αλλά ούτε και το πλοίο που τα μετέφερε. Μάλιστα μπορούσαν να διαγράψουν πληροφορίες για την ίδια την ύπαρξη του container. Όλο αυτό ξεκίνησε με μερικά απλά e-mail που έστειλαν οι hackers στις εγκαταστάσεις του λιμανιού ή στις ναυτιλιακές εταιρίες. Μετά την ανακάλυψη αυτής της επίθεσης, εγκαταστάθηκαν τοίχοι προστασίας(firewalls) ώστε να αποφευχθούν παρόμοιες επιθέσεις. Το 2012, έλαβαν χώρα διαφορετικού είδους επιθέσεις στην Αυστραλία όπου εισχώρησαν στα συστήματα φόρτωσης που χειρίζονταν οι Αυστραλιανές Αρχές. Έτσι οι δράστες μπορούσαν να ελέγξουν ποια containers θεωρούνταν ύποπτα από τις αρχές και να εστιάσουν στα υπόλοιπα τα οποία δεν παρακολουθούσαν. Ένα ακόμα παράδειγμα αφορά την IRISL (Islamic Republic of Iran Shipping Line). Συγκεκριμένα το 2011 έπειτα από μια επιτυχημένη επίθεση αλλοιώθηκαν πληροφορίες σε σχέση με την φόρτωση, τον αριθμό φορτίου, την ημερομηνία και την τοποθεσία. Για να καταλάβουμε καλύτερα τη σημασία της επίθεσης, πράγματι ήταν αδύνατο να γνωρίζουν την τοποθεσία του φορτίου, ούτε αν ήταν στο λιμάνι ούτε αν είχαν φορτωθεί στο πλοίο. Αυτό προκάλεσε σε απώλειες φορτίων, αποστολή του σε λάθος προορισμούς και άλλα μείζονα προβλήματα και επιπλοκές. Το FBI(Federal Bureau of Investigation) των Η.Π.Α. ενημέρωσε την ιδιωτική βιομηχανία πως οι επιπλοκές στα GPS είναι κοινό εργαλείο για την κλοπή φορτίων από το οργανωμένο έγκλημα. Μάλιστα στην ενημέρωση του Ιουλίου του 2014 ανέφεραν πως είχαν σημειωθεί 46 τέτοια περιστατικά και μεταφέρθηκαν κλεμμένα αυτοκίνητα στην Κίνα, καθώς και μία περίπτωση κλοπής κατεψυγμένων φαρμάκων.

1.3 Λειτουργίες στο Λιμάνι (Port Operations)

Η διαχείριση του φορτίου αποτελεί την «καρδία» των λειτουργιών στα λιμάνια, αλλά το σύστημα εντόπισης του φορτίου δεν είναι το μοναδικό σύστημα που είναι ευάλωτο σε επίθεση. Σήμερα τα λιμάνια βασίζονται τόσο στα υπολογιστικά συστήματα όσο και σε μηχανήματα ανύψωσης και καθαίρεσης φορτίων τα οποία εκτελούν την φόρτωση και την εκφόρτωση των πλοίων. Τέτοιου είδους γερανοί χρησιμοποιούν τεχνολογίες όπως οπτική αναγνώριση για την διαχείριση των λειτουργιών του λιμένα, καθώς και τον εντοπισμό φορτίου, την μεταφορά και την επιθεώρηση. Εμπορευματοκιβώτια τοποθετούνται αυτόματα με την χρήση GPS και φορτηγά που τραβούν το φορτίο από το λιμάνι εξαρτώνται και αυτά από το GPS. Έτσι, ο σύγχρονος τρόπος λειτουργίας των λιμανιών καθίσταται ευάλωτος καθώς σε περίπτωση επίθεσης, θα μπορούσε εν δυνάμει να σταματήσει η λειτουργία όλου του λιμανιού, από την διαχείριση φορτίων μέχρι και την κίνηση των γερανών και των φορτηγών. Σε αυτό το σημείο αξίζει να επισημανθεί πως το κόστος διακοπής λειτουργίας ενός λιμανιού για μία μόνο ημέρα έχει υπολογιστεί περίπου στο ένα με δύο εκατομμύρια δολάρια. Το καλό είναι πως έχει σημειωθεί μόνο μια επίθεση αυτού του είδους. Το 2014 δύο γερανοί σε ένα μεγάλο λιμένα της ανατολικής ακτής των Ηνωμένων Πολιτειών, προκαλώντας μια επτάωρη αδράνεια, καθώς ήταν αδύνατη η λήψη σημάτων GPS.

1.4 Τύποι των cyber threats (απειλές κυβερνοχώρου)

Γενικά υπάρχουν δύο κατηγορίες cyber threats οι οποίες μπορεί να επηρεάσουν τις εταιρίες και τα πλοία:

Α) Μη στοχευόμενες επιθέσεις, όπου μια εταιρία ή το σύστημα και τα δεδομένα ενός πλοίου αποτελούν ένα από τους πολλούς εν δυνάμει στόχους.
Β) Στοχευόμενη επίθεση, όπου η εταιρία ή το σύστημα και τα δεδομένα ενός πλοίου είναι συγκεκριμένα ο στόχος ή ένας από αυτούς.

Στην πρώτη κατηγορία, είναι πιθανόν να χρησιμοποιηθούν εργαλεία και τεχνικές που είναι διαθέσιμες στο διαδίκτυο και χρησιμοποιούνται για να εντοπίσουν, να ανακαλύψουν και να εκμεταλλευτούν διαδεδομένα τρωτά σημεία της εταιρίας ή του πλοίου. Μερικά παραδείγματα των παρακάτω εργαλείων και τεχνικών είναι:

- Malware (Κακόβουλο λογισμικό) το οποίο είναι σχεδιασμένο να εισχωρήσει ή να κάνει ζημιά στον υπολογιστή χωρίς την επίγνωση του ιδιοκτήτη του. Υπάρχουν ποικίλοι τύποι τέτοιων λογισμικών όπως τα λεγόμενα Trojans, Ransom ware (κρυπτογραφεί δεδομένα μέχρι να πληρωθούν λύτρα), Spyware, Viruses και Worms. Τα κακόβουλα λογισμικά μπορούν επίσης να εκμεταλλευτούν γνωστά προβλήματα σε απαρχαιωμένα λογισμικά. Ο όρος «εκμετάλλευση» αναφέρεται στην χρήση ενός κώδικα ή λογισμικού που είναι σχεδιασμένος για να υπερνικήσει και να χειραγωγήσει ένα πρόβλημα στο software ή το hardware ενός άλλου υπολογιστή. Για παράδειγμα τέτοιο πρόβλημα μπορεί να είναι ένα bug του κώδικα ή ένα τρωτό software ή ακόμα και μια εσφαλμένη σχεδίαση του.
- Water holing (Τρύπες Νερού), εγκατάσταση μιας ψευδούς ιστοσελίδας ή παραβίαση μίας γνήσιας ιστοσελίδας προφανώς χωρίς την επίγνωση του επισκέπτη.
- Scanning (Έρευνα), σάρωση δηλαδή σε ένα μεγάλο μέρος του διαδικτύου τυχαία με σκοπό την εύρεση αδυναμιών και τρωτών σημείων που θα ήταν εν δυνάμει εκμεταλλεύσιμα.
- Typo squatting (Δακτυλογράφηση), επίσης γνωστό όπως πειρατεία URL ή ψευδής URL. Βασίζεται σε λάθη τυπογραφικά που γίνονται από χρήστες του διαδικτύου κατά την πληκτρολόγηση μιας διεύθυνσης ιστοσελίδας. Το λάθος αυτό μπορεί να οδηγήσει τον χρήστη σε εναλλακτική, συχνά κακόβουλη, ιστοσελίδα.

Τώρα όσον αφορά για τις στοχευόμενες επιθέσεις διακρίνουμε πως μπορεί να είναι πιο εξειδικευμένες και τα εργαλεία και οι τεχνικές που χρησιμοποιούνται να είναι ειδικά κατασκευασμένες προκειμένου να επιτεθούν σε μία εταιρία ή πλοίο. Σε αυτήν την περίπτωση έχουμε τα εξής εργαλεία και τεχνικές:

- Social engineering (Κοινωνική μηχανική), η οποία δεν αποτελεί τεχνολογική τεχνική άλλα στην ουσία χρησιμοποιείται για να χειραγωγηθούν άτομα εκ των έσω στο να παραβούν διαδικασίες ασφάλειας, συνήθως αλλά όχι αποκλειστικά, μέσω των social media (μέσα κοινωνικής δικτύωσης).
- Brute force («Ωμή Βία»), είναι η προσπάθεια του επιτεθέντος να εισχωρήσει σε ένα σύστημα χρησιμοποιώντας τυχαίους κωδικούς ελπίζοντας ότι θα μαντέψει σωστά εν τέλει και ελέγχει συστηματικά για όλους τους πιθανούς κωδικούς εωσότου να βρεθεί ο σωστός.
- Credential stuffing, η χρήση δηλαδή προηγούμενων παραβιασμένων πιστοποιητικών/διαπιστευτηρίων ή συγκεκριμένων κωδικών που χρησιμοποιούνται συχνά, με σκοπό την μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή μια εφαρμογή.
- Denial of Service (DoS- Άρνηση υπηρεσίας), παρεμποδίζει τους εξουσιοδοτημένους χρήστες από την πρόσβαση τους σε πληροφορίας, συνήθως γεμίζοντας το δίκτυο με

δεδομένα. Αυτό έχει ως αποτέλεσμα την απόκτηση του ελέγχου από αυτόν που επιτίθεται σε πολλούς υπολογιστές και/ή servers με την εφαρμογή της επίθεσης DoS.

- Phishing (Ηλεκτρονικό ψάρεμα), το οποίο αποτελεί μία πολύ συχνή μορφή εξαπάτησης όπου με την αποστολή e-mail σε πολλούς παραλήπτες και συνεπώς πιθανούς στόχους, ζητούνται ευαίσθητα και εμπιστευτικά δεδομένα. Το e-mail μπορεί επίσης να έχει κακόβουλα συνημμένα ή να προτρέπει κάποιον να επισκεφτεί μια ψεύτικη ιστοσελίδα με την χρήση ενός υπερσυνδέσμου (hyperlink) που υπάρχει στο ηλεκτρονικό μήνυμα.
- Spear-Phishing, όπως και στο phishing, όμως με την διαφορά πως πλέον οι χρήστες έχουν στοχοποιηθεί με τα προσωπικά τους e-mail, και περιέχουν κακόβουλο λογισμικό ή σύνδεσμο που κατεβαίνει αυτόματα.
- Subverting the supply chain (Ανατροπή αλυσίδας εφοδιασμού), είναι η επίθεση σε μια εταιρία ή ένα πλοίο παραβιάζοντας τον εξοπλισμό, το λογισμικό ή τις υπηρεσίες υποστήριξης.

Τα παραπάνω παραδείγματα δεν είναι τα μοναδικά που χρησιμοποιούνται καθώς οι τεχνικές είναι ανεξάντλητες και εξελίσσονται ανάλογα με την ευφυΐα των οργανώσεων και των ατόμων που τις δημιουργούν.

1.5 Στάδια ενός cyber incident

Το 2019, απαιτούνταν 279 μέρες κατά μέσο όρο μεταξύ της στιγμής όπου το δίκτυο του θύματος παραβιαζόταν μέχρι την δράση της παραβίασης. Παρόλα αυτά η παραβίαση μπορεί να μείνει απαρατήρητη για χρόνια. Ο χρόνος για την προετοιμασία ενός cyber attack καθορίζεται από τα κίνητρα και τους στόχους του θύτη, καθώς και την ελαστικότητα των τεχνικών και των διαδικασιών ελέγχου του cyber risk που εφαρμόζει η εταιρία και το πλήρωμα σε ένα πλοίο. Σε περίπτωση που θεωρηθεί ότι ένα πλοίο ή μία εταιρία έγινε στόχος cyber attack, τα γενικά στάδια που παρατηρούμε στο περιστατικό είναι τα εξής:

- Survey/Reconnaissance (Έρευνα/ Αναγνώριση). Ανοιχτές/Δημόσιες πηγές όπως τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται για να παρθούν πληροφορίες για έναν πιθανό στόχο (εταιρία, πλοίο ή ναυτικό) κατά την προετοιμασία ενός cyber attack. Τα μέσα κοινωνικής δικτύωσης, τα τεχνικά φόρουμ και οι κρυφές ιδιότητες σε μια ιστοσελίδα, τα αρχεία και διάφορες εκδόσεις μπορεί να χρησιμοποιηθούν προκειμένου να αναγνωριστούν τεχνικά, διαδικαστικά και φυσικά τρωτά σημεία. Κατά τη χρήση δημοσίων πηγών θα πρέπει να παρακολουθούνται τα πραγματικά δεδομένα που ανταλλάσσονται από μια εταιρία ή ένα πλοίο.
- Delivery (Παράδοση). Οι δράστες μπορεί να προσπαθήσουν να αποκτήσουν πρόσβαση στα δεδομένα και τα συστήματα της εταιρίας και του πλοίου. Αυτό μπορεί να γίνει είτε από την εταιρία είτε από το πλοίο ή και μέσω σύνδεσης στο διαδίκτυο. Παραδείγματα των μεθόδων που χρησιμοποιούνται για να αποκτηθεί η πρόσβαση είναι: α) οι online υπηρεσίας της εταιρίας που περιλαμβάνουν τα συστήματα παρακολούθησης (tracking) φορτίου ή container, β) αποστολή e-mail που περιέχουν κακόβουλα αρχεία ή συνδέσμους που οδηγούν σε κακόβουλες ιστοσελίδες στο προσωπικό, γ) παροχή «μολυσμένων» removable media για παράδειγμα σαν μία αναβάθμιση λογισμικού σε ένα σύστημα πάνω στο πλοίο και δ) δημιουργία ψευδών ή παραπλανητικών ιστοσελίδων οι οποίες ενθαρρύνουν το προσωπικό να αποκαλύψουν και να εκθέσουν δεδομένα.

- Breach (Παραβίαση). Η έκταση της παραβίασης στην οποία μπορεί να εκτεθούν τα συστήματα του πλοίου και της εταιρίας εξαρτάται από το πόσο σημαντικά είναι τα αδύναμα σημεία που θα βρει ο δράστης καθώς και η μέθοδος που θα επιλέξει να επιτεθεί. Να σημειώσουμε πως η παραβίαση δεν σημαίνει απαραίτητα πως θα παρατηρήσουμε προφανές αλλαγές στην κατάσταση του εξοπλισμού. Ανάλογα με το μέγεθος της παραβίασης ο δράστης μπορεί να έχει την ικανότητα: α) να κάνει αλλαγές που θα επηρεάσουν την λειτουργία του συστήματος, για παράδειγμα να διακόψει ή να χειραγωγήσει πληροφορίες που χρησιμοποιεί ο εξοπλισμός ναυσιπλοΐας, β) να αποκτήσει πρόσβαση που θα του επιτρέψουν να πάρει αντίγραφα ή να αλλάξει λειτουργικά σημαντικές πληροφορίες όπως loading lists ή εμπορικά ευαίσθητα δεδομένα, πχ. Cargo manifests, crew lists, passenger/visitor lists, και γ) να αποκτήσει τον πλήρη έλεγχο ενός συστήματος όπως για παράδειγμα το σύστημα διαχείρισης μηχανημάτων.
- Pivot. Το pivoting είναι η τεχνική που χρησιμοποιείτε σε ένα ήδη εκτεθειμένο σύστημα για να γίνει επίθεση σε άλλα συστήματα που βρίσκονται στο ίδιο δίκτυο. Σε αυτή τη φάση της επίθεσης ο δράστης χρησιμοποιεί το εκτεθειμένο σύστημα προκειμένου να αποκτήσει πρόσβαση σε άλλα απροσπέλαστα συστήματα. Συνήθως ο δράστης θα επιλέξει το πιο εύκολο και ευάλωτο σύστημα και μετά θα προσπαθήσει να αποκτήσει πρόσβαση στα υπόλοιπα που βρίσκονται στο δίκτυο. Πολύ πιθανόν για κατά την φάση του pivoting, ο δράστης θα προσπαθήσει: α) να ανεβάσει εργαλεία και διάφορα αρχεία που θα τον βοηθήσουν να ξεκινήσει την επόμενη φάση της επίθεσης, β) να ανακαλύψει τα υπόλοιπα συστήματα του δικτύου χρησιμοποιώντας εργαλεία scanning ή network mapping, γ) να εγκαταστήσει μόνιμα εργαλεία ή κλειδιά για να κρατήσει και να διατηρήσει πρόσβαση στο σύστημα και δ) να επιτεθεί σε άλλα συστήματα του δικτύου.

Τα κίνητρα και οι στόχοι του δράστη είναι αυτά που θα καθορίσουν το αντίκτυπο που θα έχει η επίθεση στα συστήματα και τα δεδομένα της εταιρίας ή του πλοίου. Ο δράστης μπορεί να εξερευνήσει συστήματα, να επεκτείνει ή να εξασφαλίσει ότι θα διατηρήσει την πρόσβαση του σε ένα σύστημα με σκοπό :

- Να έχει πρόσβαση σε εμπιστευτικά και ευαίσθητα δεδομένα που αφορούν το φορτίο, το πλήρωμα, τους επιβάτες και τους επισκέπτες.
- Να χειραγωγήσει τις λίστες πληρώματος, επιβατών ή επισκεπτών, τα loading lists, τα stow plans ή τα cargo manifests. Αυτό μπορεί να αποσκοπεί στην μεταφορά παράνομου φορτίου ή σε κλοπή.
- Να κάνει τελείως μη λειτουργικά τα συστήματα.
- Να προβεί σε άλλης μορφής εγκλήματα όπως πειρατεία, κλοπή ή απάτη.
- Να εμποδίσει την ομαλή λειτουργία των συστημάτων της εταιρίας και του πλοίου, για παράδειγμα διαγράφοντας σημαντικά αρχεία ή δεδομένα ή ακόμα και να υπερφορτώσουν τα συστήματα της εταιρίας.
- Να απαιτήσει λύτρα

ΚΕΦΑΛΑΙΟ 2: CYBER SECURITY

2.1 Ο ρόλος του IMO στην πρόληψη και την αντιμετώπιση των κινδύνων

Το 2017 ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) και πιο συγκεκριμένα η Επιτροπή Ναυτιλιακής Ασφάλειας (Maritime Safety Committee – MSC) υιοθέτησε κατευθυντήριες γραμμές (guidelines) σύμφωνα με την ανάλυση MSC.428 (98) που αφορά τη διαχείριση των ναυτιλιακών κινδύνων στον κυβερνοχώρο (Maritime Cyber Risk Management). Για να θεωρηθεί, λοιπόν αποδεκτός ο ISM Code (International Safety Management) και ο SMS (Safety Management System) μίας ναυτιλιακής εταιρίας και κατ' επέκταση του εκάστοτε στόλου, θα πρέπει να συμμορφωθεί και να λάβει υπόψη το cyber risk management σύμφωνα με τους στόχους και τους λειτουργικές απαιτήσεις που ορίζει. Επίσης καλεί τις διοικήσεις να εξασφαλίσουν πως τα cyber risks αναφέρονται στον SMS κατάλληλα, όχι αργότερα από την πρώτη ετήσια επαλήθευση συμμόρφωσης του DoC (Document of Compliance) της εταιρίας μετά την 1η Ιανουαρίου 2021. Τον ίδιο χρόνο αναπτύχθηκαν guidelines τα οποία παρέχουν υψηλού επιπέδου προτάσεις στην διαχείριση κινδύνων στον κυβερνοχώρο που υπάρχουν στην ναυτιλία, με σκοπό να την προστατεύσει από τις υπάρχοντες απειλές και αδυναμίες που την καθιστούν ευάλωτη. Τόνισε επίσης πως θα πρέπει να τεθεί μια κουλτούρα cyber risk management σε όλα τα επίπεδα και τμήματα ενός οργανισμού για να εξασφαλισθεί ένα ολιστικό και παράλληλα εύκαμπτο καθεστώς όπου θα λειτουργεί και θα αξιολογείται διαρκώς. Από την 1η Ιανουαρίου 2021 αυτές οι κατευθυντήριες γραμμές έγιναν υποχρεωτικές και θα πρέπει όλα τα πλοία να συμμορφωθούν κατάλληλα.

2.2 Διαχείριση ασφάλειας και ρίσκου στον κυβερνοχώρο

Με βάση τα ρίσκα που αναφέρθηκαν παραπάνω(βλ. Κεφάλαιο 1) θα πρέπει να ληφθούν μέτρα τόσο από τις εταιρίες όσο και από τα πληρώματα των πλοίων για την διαχείριση τους. Πιο συγκεκριμένα:

- Αναγνώριση των ρόλων και των υποχρεώσεων των χρηστών, βασικών προσώπων και διαχείριση σε στεριά και στο πλοίο.
- Αναγνώριση των συστημάτων, των δεδομένων και των δυνατοτήτων, που αν υποστούν δολιοφθορά, θα τεθεί σε κίνδυνο την λειτουργία και την ασφάλεια του πλοίου.
- Εφαρμογή τεχνικών και διαδικαστικών μέτρων για την προστασία περιστατικών(cyber incidents) και εξασφάλιση διαρκούς λειτουργίας.
- Ενδεχόμενο πλάνο και τακτική εξάσκηση του.

Επίσης, μερικές πτυχές του cyber risk management ενδέχεται να περιέχουν ευαίσθητες και εμπιστευτικές πληροφορίες. Οι εταιρίες, επομένως, θα πρέπει να προστατέψουν κατάλληλα αυτές τις πληροφορίες όσο το δυνατόν καλύτερα και να μην τις εμπεριέχουν στον SMS τους.

Εικόνα 1: *Διαχείριση κινδύνων στον κυβερνοχώρο όπως παρουσιάζονται στα guidelines.*

Η ανάπτυξη, η υλοποίηση καθώς και η συντήρηση ενός προγράμματος διαχείρισης κινδύνων στον κυβερνοχώρο σύμφωνα με τον τρόπο που προσεγγίζεται στο παραπάνω σχεδιάγραμμα (Εικόνα 1) δεν είναι τόσο απλό. Συνεπώς απαιτείται ιδιαίτερη προσοχή κατά τη διαδικασία ώστε να εξασφαλισθεί ότι η προστασία και το ενδεχόμενο πλάνο είναι ισορροπημένο για να διαχειριστεί κινδύνους σε αποδεκτά πλαίσια. Παράγοντες όπως το αντίκτυπο, η πιθανότητα, η τρωτότητα, οι απειλές, η δυνατότητα, η ευκαιρία και η πρόθεση των κακοηθών δραστών συνδέονται μεταξύ τους και συνυπολογίζονται στην αξιολόγηση του ρίσκου. Επομένως σε περίπτωση που οι προαναφερθέντες παράγοντες είναι χαμηλοί σαν πιθανότητα ή και μηδενικοί αυτό σημαίνει πως το ίδιο χαμηλό ή ακόμα και μηδενικό θα είναι το ρίσκο. Σε αυτό το σημείο καλό είναι να γίνει αναφορά στις φόρμες όπου συμπληρώνονται στα πλοία που αφορούν την αξιολόγηση κινδύνου (risk assessment) και τα μέτρα που μπορούν και πρέπει να ληφθούν προκειμένου να μειωθεί το ρίσκο και ο κίνδυνος. Αυτές οι φόρμες συμπληρώνονται για

διάφορες εργασίες και καταστάσεις, καθώς μια από αυτές αποτελεί και το cyber risk και το cyber security. Ο IMO τονίζει πως η συμπλήρωση τους δεν αποτελεί μια ενέργεια που θα γίνει μια φορά αλλά θα πρέπει να είναι επαναλαμβανόμενη και να διαπιστώνει αν οι παράγοντες που αναφέραμε έχουν αλλάξει και αν τα μέτρα αντιμετώπισης που έχουμε είναι επαρκή.

2.3 Ρόλοι, Υποχρεώσεις και καθήκοντα

Για την επίτευξη ενός αποτελεσματικού cyber risk management απαραίτητη προϋπόθεση είναι ο ξεκάθαρος καταμερισμός και καθορισμός των καθηκόντων και των υποχρεώσεων μέσα στην εταιρία. Το cyber risk management αποτελεί αναπόσπαστο κομμάτι της διαχείρισης των πλοίων και των λειτουργιών του. Οι υποχρεώσεις και τα καθήκοντα θα πρέπει να περιγράφονται και να βρίσκονται στον SMS. Καθότι το πλάνο για το cyber risk management αφορά ολόκληρη την εταιρία θα πρέπει να είναι ξεκάθαρο το ποιος είναι υπεύθυνος και ποιος οφείλει να παραχωρεί υποστήριξη. Για παράδειγμα , ένας IT manager είναι αρμόδιος και υπεύθυνος για το cyber risk management, παρόλα αυτά βασίζεται στην στήριξη από άλλα department της εταιρίας. Τέλος είναι αποτελεσματικότερο οι υποχρεώσεις και τα καθήκοντα να απευθύνονται στα άτομα τα οποία είναι ψηλά ιεραρχικά. Έτσι όσον αφορά την συμμόρφωση με τις διαδικασίες του cyber risk management στο πλοίο, είναι επακόλουθο πως θα απευθυνθούμε στον Καπετάνιο ή τον Α' Μηχανικό. Παρακάτω βλέπουμε έναν πίνακα καταμερισμού εργασιών και αρμοδιοτήτων.

Task Role/person	Cyber input to safety/security policy	Cyber risk assessment on ship OT systems	Cyber risk assessment on ship IT systems	Ship IT infrastructure management	Crew cyber risk management training
Managing director	Responsible				
Company IT manager	Supporting		Supporting		
Ship IT manager	Supporting	Responsible	Responsible	Responsible	
Safety manager	Supporting	Supporting	Supporting	Supporting	Supporting
Procurement manager	Supporting			Supporting	
Fleet manager		Supporting	Supporting	Supporting	Supporting
Training manager			Supporting		Supporting
Marine HR manager			Supporting		Responsible

Πίνακας 1: *Πίνακας καταμερισμού καθηκόντων.*

2.4 Προσδιορισμός αδυναμιών/τρωτών σημείων

Τα παρακάτω αποτελούν κοινές αδυναμίες στον κυβερνοχώρο, που μπορεί να βρεθούν σε υπάρχοντα πλοία ή σε νεόκτιστα:

- Απαρχαιωμένα ή χωρίς στήριξη λειτουργικά συστήματα
- Μη συμβατό λογισμικό συστήματος
- Ανενημέρωτο ή καθόλου λογισμικό antivirus και προστασία από κακόβουλα λογισμικά
- Ανεπαρκής διαμόρφωση ασφάλειας και καλής πρακτικής, συμπεριλαμβανομένου αναποτελεσματικής διαχείρισης δικτύου και χρήση προεπιλεγμένου λογαριασμού διαχείρισης και κωδικών
- Δίκτυα υπολογιστών στο πλοίο που υστερούν σε οριακά μέτρα προστασίας και κατάτμηση των δικτύων
- Κρίσιμα συστήματα ή εξοπλισμός που σχετίζονται με την ασφάλεια είναι μονίμως συνδεδεμένα με την στεριά
- Ανεπαρκής έλεγχος πρόσβασης στον κυβερνοχώρο, δίκτυα κλπ για τρίτους συμπεριλαμβανομένων των εργολάβων και των παρόχων υπηρεσιών
- Ανεπαρκής εκπαίδευση και/ή ικανοτήτων του προσωπικού στην διαχείριση του cyber risk
- Ανύπαρκτο, ανεπαρκή ή αδοκίμαστο πλάνο έκτακτης ανάγκης και διαδικασιών

Για να βοηθήσουμε κάθε βήμα της αξιολόγησης κινδύνου (risk assessment), το IT και OT σύστημα πρέπει να είναι ξεκάθαρα προσδιορισμένο με τεκμηριωμένες τις ευθύνες της διακυβέρνησης και της ιδιοκτησίας εντός ενός μητρώου περιουσιακών στοιχείων, το οποίο θα πρέπει να διατηρείται ενημερωμένο σωστά. Το μητρώο περιουσιακού στοιχείου θα πρέπει να περιλαμβάνει την αποτίμηση του στοιχείου καθώς και το κόστος διατήρησης του. Σύμφωνα με την πρόταση no. 166 του IACS (International Association of Classification Societies- Διεθνής Ένωση Νηογνωμόνων) πάνω στο Cyber Resilience (Κυβερνο-ανθεκτικότητα), παρόλο που εφαρμόζεται μόνο στα νεόχτιστα πλοία, μπορεί να εξυπηρετήσει ο οδηγός για την ανάπτυξη αρχείου που μπορεί να περιέχει:

- Απογραφή των συσκευών επικοινωνίας
- Απογραφή των συσκευών επικοινωνίας του δικτύου
- Λογικός χάρτης των δικτύων:
    1. Διευθύνσεις IP
    2. Διευθύνσεις non-IP
    3. Σημεία πρόσβασης non-Ethernet
    4. Διακομιστές και υπολογιστές
    5. Συνδέσμους και συσκευές πεδίων επικοινωνίας
- Απογραφή λογισμικού (σε μερικές περιπτώσεις αυτή η απογραφή είναι μέρος ενός Shop Software Logging System)
- Απογραφή των υπηρεσιών δικτύου για κάθε εξοπλισμό

Υπάρχουν διαθέσιμα εργαλεία για την διαχείριση της απογραφής ενός συστήματος IT αλλά δεν συνίσταται για συστήματα OT καθώς μπορεί να επηρεαστεί η ακεραιότητα του συστήματος (εκτός εάν γίνει από έναν εξειδικευμένο τεχνικό σε στενή επικοινωνία με τον Καπετάνιο, τον Α' Μηχανικό κλπ) .

Ο προσδιορισμός των αδυναμιών περιλαμβάνει την ανάλυση των εφαρμογών, των συστημάτων και των διαδικασιών για να τρωτά σημεία που θα μπορούσαν να μοχλευθούν από πιθανές απειλές. Αυτό μπορεί να γίνει από εσωτερικούς εμπειρογνώμονες και/ή να υποστηριχθεί από εξωτερικούς εμπειρογνώμονες με γνώσεις της ναυτιλιακής βιομηχανίας και των βασικών διαδικασιών.

INCIDENT: Crush of integrated navigation bridge system at sea

Πλοίο με ενσωματωμένο σύστημα πλοήγησης υπέστη ζημιά σχεδόν όλων των συστημάτων ναυσιπλοΐας στη θάλασσα, σε μία περιοχή με υψηλή κίνηση και μειωμένη ορατότητα. Το πλοίο αναγκάστηκε να πλοηγήσει με ένα ραντάρ και έναν εφεδρικό χάρτινο χάρτη για δύο μέρες πριν την άφιξη του σε λιμένα για επισκευές. Η αιτία της δυσλειτουργίας όλων των υπολογιστών ECDIS αποδόθηκε στα απαρχαιωμένα λειτουργικά συστήματα. Στο τελευταίο λιμάνι που ήταν το πλοίο, ένας τεχνικός αντιπρόσωπος κατασκευαστή, έκανε ενημέρωση λογισμικού στο navigation και τους navigation υπολογιστές του πλοίου. Παρόλα αυτά τα απαρχαιωμένα λειτουργικά συστήματα ήταν ανίκανα να τρέξουν το λογισμικό και κράσαραν. Το πλοίο αναγκάστηκε να κάτσει στο λιμάνι μέχρι να εγκατασταθούν νέοι υπολογιστές ECDIS, να παρευρεθούν επιθεωρητές κλάσης, και όπως προβλέπεται από την εταιρία να εκδοθεί near-miss notification. Το κόστος της καθυστέρησης ήταν μεγάλο και καλύφθηκε από τον πλοιοκτήτη.

Το περιστατικό αυτό δίνεται ως παράδειγμα, για να τονιστεί πως δεν είναι όλες οι ζημιές σε έναν υπολογιστή αποτέλεσμα μίας επίθεσης και πως ένα απαρχαιωμένο λειτουργικό σύστημα μπορεί να δημιουργήσει πρόβλημα. Περισσότερες δοκιμές και προληπτική συντήρηση του λογισμικού μπορεί να είχαν αποτρέψει αυτό το συμβάν.

Ο στόχος της αξιολόγησης του δικτύου ενός πλοίου και των συστημάτων και των συσκευών του είναι για να προσδιοριστούν οποιεσδήποτε αδυναμίες που μπορεί να παραβιαστούν ή να οδηγήσουν σε απώλεια της εμπιστευτικότητας, ακεραιότητας ή της διαθεσιμότητας των δεδομένων και των συστημάτων που είναι απαραίτητα για την λειτουργία του εξοπλισμού, του δικτύου, του συστήματος ή ακόμη και του πλοίου. Αυτές οι αδυναμίες θα μπορούσαν να ενταχθούν σε μία από τις παρακάτω κατηγορίες:

- Προσωρινές εκθέσεις όπως ελάττωμα λειτουργικού συστήματος, ξεπερασμένο ή μη προσαρμοσμένο σύστημα
- Σφάλματα εφαρμογής όπως για παράδειγμα λάθος διαμορφωμένα firewalls
- Διαδικαστικά ή άλλα σφάλματα χρήστη
- Σχεδιασμού όπως η διαχείριση πρόσβασης ή μη διαχειριζόμενη διασύνδεση δικτύου

Τα αυτόνομα συστήματα είναι λιγότερο ευάλωτα σε εκτεταμένα cyber incidents σε σύγκριση με αυτά που είναι συνδεδεμένα σε ανεξέλεγκτα δίκτυα ή συνδεδεμένα κατευθείαν στο διαδίκτυο. Πρέπει να κατανοήσουμε την σημασία και την κρισιμότητα της κατάστασης όταν συστήματα του πλοίου είναι συνδεδεμένα σε μη ελεγχόμενα δίκτυα. Ο ανθρώπινος παράγοντας θα πρέπει να ληφθεί υπόψη καθότι πολλά περιστατικά ξεκίνησαν από ενέργειες του προσωπικού. Σε αυτά τα συστήματα του πλοίου περιλαμβάνονται:

- **Cargo and loading management systems:** Τα ψηφιακά συστήματα που χρησιμοποιούνται για την φόρτωση, την διαχείριση και τον έλεγχο του φορτίου, συμπεριλαμβανομένου επικίνδυνου φορτίου, μπορεί να έχουν επαφή με ποικίλα συστήματα στη στεριά όπως λιμάνια, τερματικούς, στοιβαδόρους. Τέτοια συστήματα μπορεί να περιέχουν εργαλεία παρακολούθησης αποστολών διαθέσιμα για τους αποστολείς μέσω ίντερνετ. Διασυνδέσεις σαν αυτές καθιστούν τα συστήματα διαχείρισης φορτίο, τα δεδομένα του cargo manifest και της λίστας φόρτωσης, ευάλωτα σε cyber incidents.
- **Bridge systems:** Η αυξημένη χρήση δικτύων και ψηφιακών συστημάτων ναυσιπλοΐας με σύνδεση σε επίγεια δίκτυα για ενημερώσεις και παροχή υπηρεσιών, καθιστά αυτά τα συστήματα ευάλωτα σε cyber incidents. Τα συστήματα της γέφυρας που δεν είναι συνδεδεμένα σε άλλα δίκτυα μπορεί να είναι εξίσου ευάλωτα, καθώς χρησιμοποιούνται συχνά αφαιρούμενα μέσα για την ενημέρωση τέτοιων συστημάτων από άλλα ελεγχόμενα ή μη δίκτυα. Ένα cyber incident μπορεί να επεκταθεί σε service denial ή σε χειραγώγηση, και συνεπώς να επηρεάσει όλα τα συστήματα που σχετίζονται με την ναυσιπλοΐα, όπως το ECDIS, GNSS, AIS, VDR και Radar/ARPA.
- **Propulsion and machinery management and power control systems:** Η χρήση ψηφιακών συστημάτων για την παρακολούθηση και τον έλεγχο των μηχανημάτων στο πλοίο, των συστημάτων πρόωσης και πηδαλιουχίας αποτελεί την αιτία που είναι ευάλωτα σε cyber incidents. Τα συστήματα αυτά γίνονται ακόμα πιο ευάλωτα όταν χρησιμοποιούνται σε σύνδεση για απομακρυσμένη παρακολούθηση (remote condition-based monitoring) και/ή είναι ενσωματωμένα σε εξοπλισμό επικοινωνίας και ναυσιπλοΐας στα πλοία που χρησιμοποιούν ενσωματωμένα συστήματα γέφυρας.
- **Access control systems:** Τα ψηφιακά συστήματα που χρησιμοποιούνται την υποστήριξη της πρόσβασης ελέγχου για να διασφαλίσουν την φυσική ασφάλεια και την ασφάλεια του πλοίου και του φορτίου του, που περιλαμβάνει συστήματα επιτήρησης, security alarm, και ηλεκτρονικά συστήματα πληρώματος είναι και αυτά ευάλωτα σε cyber incidents.
- **Passenger servicing and management systems:** Τα ψηφιακά συστήματα για την διαχείριση ιδιοκτησίας, επιβίβασης και πρόσβασης ελέγχου μπορεί να περιέχουν πολύτιμα δεδομένα των επιβατών. Έξυπνες συσκευές (tablets, φορητοί σαρωτές κλπ) είναι τα ίδια θύματα επίθεσης καθώς τελικά τα συλλεγόμενα δεδομένα περνάνε σε άλλα συστήματα.
- **Passenger facing public networks:** Σταθερά ή ασύρματα δίκτυα που συνδέονται στο ίντερνετ, εγκαθίστανται στο πλοίο προς όφελος των επιβατών. Για παράδειγμα τα συστήματα guest entertainment, θα πρέπει να θεωρούνται μη ελεγχόμενα και δεν θα πρέπει να συνδέονται σε κανένα κρίσιμο σύστημα που αφορά την ασφάλεια του πλοίου.

- **Administrative and crew welfare systems:** Τα δίκτυα των υπολογιστών στο πλοίο που χρησιμοποιούνται για την διαχείριση του πλοίου ή για την ευημερία του πληρώματος είναι ιδιαίτερα ευάλωτα όταν έχουν πρόσβαση στο διαδίκτυο και στα e-mail. Αυτό μπορεί να το εκμεταλλευτούν οι «cyber attackers» για να αποκτήσουν πρόσβαση στα δεδομένα και στα συστήματα του πλοίου. Αυτά τα συστήματα θα πρέπει να τα θεωρούμε μη ελεγχόμενα και δεν θα πρέπει να είναι συνδεδεμένα με συστήματα που είναι κρίσιμα για την ασφάλεια στο πλοίο. Στην ίδια κατηγορία περιλαμβάνεται και το λογισμικό που παρέχεται από τις ναυτιλιακές εταιρίες ή τους πλοιοκτήτες.
- **Communication systems:** Η διαθεσιμότητα της σύνδεσης στο διαδίκτυο μέσω δορυφόρου και/ή άλλων ασύρματων επικοινωνιών αυξάνουν την τρωτότητα των πλοίων, και πρόσφατες εξελίξεις δείχνουν πως για παράδειγμα τα σήματα VSAT είναι ευάλωτα σε εκμετάλλευση χρησιμοποιώντας προϊόντα χαμηλού κόστους. Θα πρέπει να ληφθούν υπόψη συστήματα επικοινωνίας με κρυπτογράφηση καθώς και οι μηχανισμοί cyber defense που είναι ενσωματωμένοι από τους παρόχους υπηρεσιών αλλά δεν θα πρέπει να βασιζόμαστε αποκλειστικά σε αυτούς για την ασφάλιση κάθε συστήματος ή δεδομένων του πλοίου. Μέσα σε αυτά τα συστήματα συμπεριλαμβάνονται σύνδεσμοι επικοινωνίας με δημόσιες αρχές που χρησιμοποιούνται για την αποστολή απαιτούμενων πληροφοριών σχετικά με το πλοίο και το φορτίο. Στις απαιτήσεις από αυτές τις αρχές σχετικά με τον ισχύον έλεγχο ταυτότητας και την διαχείριση του ελέγχου πρόσβασης τα πλοία θα πρέπει να συμμορφώνονται αυστηρά. Επίσης συμπεριλαμβάνονται οι ικανότητες του πλοίου να συλλέγει δεδομένα από συσκευές ανάκρισης και καταγραφείς δεδομένων που είναι τοποθετημένοι σε εμπορευματοκιβώτια για μετέπειτα μετάδοση σε σχεδιασμένους παραλήπτες στη στεριά.

  Όλα τα παραπάνω συστήματα του πλοίου που αναφέραμε αποτελούν εν δυνάμει ευάλωτα συστήματα, τα οποία θα πρέπει να αναφέρονται κατά τη διάρκεια της αξιολόγησης. Κατά αξιολόγηση της τρωτότητας μπορεί να βοηθήσει εάν απαντήσουμε τις εξής ερωτήσεις:
  - Είναι το σύστημα αυτόνομο ή συνδεδεμένο με άλλα συστήματα;
  - Είναι το σύστημα εκτενώς συνδεδεμένο, είτε απευθείας είτε μέσω άλλων συστημάτων;
  - Έχει το σύστημα αποτελεσματικό ενσωματωμένα μέτρα μετριασμού κινδύνου όπως για παράδειγμα κρυπτογράφηση;
  - Απαιτεί το σύστημα τακτικές ενημερώσεις λογισμικού;
  - Συμπεριλαμβάνει η λειτουργία του συστήματος σύνδεση αφαιρούμενων μέσων ,για παράδειγμα για την λήψη διαγνωστικών πληροφοριών;
  - Είναι το σύστημα εύκολα προσβάσιμο φυσικά;

Τα πλοία ενσωματώνονται ολοένα και περισσότερο με τις λειτουργίες της στεριάς εξαιτίας της χρήσης ψηφιακών επικοινωνιών για την διεξαγωγή των επιχειρήσεων, την διαχείριση των λειτουργιών και για την διατήρηση της επικοινωνίας με τα κεντρικά γραφεία. Αποτέλεσμα των παραπάνω είναι πως κρίσιμα συστήματα του πλοίου που είναι απαραίτητα για την ασφάλεια της ναυσιπλοΐας, την διαχείριση της ενέργειας και του

φορτίου έχουν γίνει ψηφιακά και συνδέονται στο ίντερνετ για να διεξάγουν μια ποικιλία θεμιτών λειτουργιών όπως:

- Παρακολούθηση απόδοσης μηχανής
- Απομακρυσμένες διαγνώσεις
- Διαχείριση συντήρησης και ανταλλακτικών
- Διαχείριση και παρακολούθηση φορτίου και εμπορευματοκιβωτίων, φόρτωσης και εκφόρτωσης, και πλάνου στοιβασίας
- Διαχείριση γερανών και αντλιών
- Παρακολούθηση των συστημάτων για την συμμόρφωση με τους περιβαλλοντικούς κανονισμούς και για αναφορές
- Παρακολούθηση απόδοσης ταξιδιού

Η παραπάνω λίστα παρέχει παραδείγματα της διεπαφής των πλοίων και είναι ανεξάντλητη. Τα παραπάνω συστήματα περιέχουν δεδομένα, τα επεξεργάζονται και τα ανταλλάζουν, κάτι το οποίο μπορεί να αποτελέσει ενδιαφέρον για εκμετάλλευση από τους εγκληματίες στον κυβερνοχώρο. Οι μοντέρνες τεχνολογίες μπορεί να προσθέσουν κι άλλα ευάλωτα σημεία στα πλοία ειδικά αν είναι μη ασφαλή σχεδιασμένα δίκτυα και ανεξέλεγκτες προσβάσεις στο διαδίκτυο. Επιπλέον, το προσωπικό τόσο στη στεριά όσο και στο πλοίο μπορεί να μην γνωρίζουν πως μερικοί κατασκευαστές εξοπλισμού και παρόχοι λογισμικών διατηρούν απομακρυσμένη πρόσβαση σε εξοπλισμό του πλοίου και στα συστήματα δικτύου του. Η άγνωστη και ασυντόνιστη απομακρυσμένη πρόσβαση σε ένα λειτουργικό πλοίο θα πρέπει να ληφθεί υπόψη ως σημαντικό κομμάτι κατά την αξιολόγηση κινδύνου. Προτείνεται στις εταιρίας να είναι πλήρως ενημερωμένοι και να καταγράφουν ,όπως προβλέπεται, τα συστήματα IT και OT του πλοίου και πώς αυτά τα συστήματα συνδέονται και ενσωματώνονται με την στεριά, συμπεριλαμβανομένων και των δημοσίων αρχών, των λιμανιών και των στοιβαδόρων. Αυτό απαιτεί κατανόηση όλων των συστημάτων του πλοίου που βασίζονται σε υπολογιστή και το πώς η ασφάλεια, η λειτουργία και η επιχείριση, συμπεριλαμβανομένης της διαχείρισης φορτίου και της φόρτωσης, μπορεί να εκτεθούν από ένα cyber incident.

Κατά την επίσκεψη τρίτων στο πλοίο πολλές φορές απαιτείται η σύνδεση σε έναν ή παραπάνω υπολογιστή του πλοίου και αυτό μπορεί επίσης να θεωρηθεί σύνδεση πλοίου-στεριάς. Είναι συνηθισμένο οι τεχνικοί, οι προμηθευτές, αρχές του λιμανιού και άλλοι, εκπρόσωποι των λιμανιών, διεκπεραιωτές, πιλότοι και άλλοι που θα μπουν στο πλοίο να συνδέσουν τις συσκευές τους, για παράδειγμα λάπτοπ ή τάμπλετ. Μερικοί τεχνικοί μπορεί ακόμα και να χρησιμοποιήσουν αφαιρούμενα μέσα για να ενημερώσουν υπολογιστές, να κατεβάσουν δεδομένα και/ή να διεξάγουν άλλες εργασίες. Επίσης είναι γνωστό πως οι αρχές και το Port State Control που επισκέπτονται το πλοίο ζητούν να χρησιμοποιήσουν υπολογιστή για να εκτυπώσουν επίσημα έγγραφα μετά αφού εισάγουν ένα άγνωστο αφαιρούμενο μέσο (πχ USB). Κάποιες φορές είναι αδύνατον να ελεγχθεί το ποιος έχει πρόσβαση στα συστήματα πάνω στο πλοίο, για παράδειγμα κατά την διάρκεια του drydocking ή όταν παίρνουμε ένα καινούργιο ή ήδη υπάρχον πλοίο. Σε τέτοιες περιπτώσεις είναι δύσκολο να γνωρίζουμε εάν υπάρχει κάποιο κακόβουλο λογισμικό πάνω στο πλοίο και τα συστήματα του. Έτσι λοιπόν προτείνεται η διαγραφή των ευαίσθητων δεδομένων από το πλοίο και η επανεγκατάσταση τους και θα πρέπει τουλάχιστον να υπάρχει ένα back-up των δεδομένων. Όπου είναι δυνατόν, τα συστήματα

θα πρέπει να ελέγχονται για κακόβουλα λογισμικά πριν την χρήση. Τα συστήματα ΟΤ θα πρέπει να εξετάζονται για να ελέγχεται ότι λειτουργούν σωστά.

Κάποια IT και ΟΤ συστήματα έχουν τη δυνατότητα της απομακρυσμένης πρόσβασης και μπορεί να λειτουργούν συνεχώς με σύνδεση στο διαδίκτυο για απομακρυσμένη παρακολούθηση, συλλογή δεδομένων, λειτουργίες συντήρησης και ασφάλειας. Αυτά τα συστήματα μπορεί να είναι «συστήματα τρίτων» όπου ο εργολάβος μπορεί να παρακολουθεί και να συντηρεί από απόσταση τα συστήματα. Αυτά τα συστήματα μπορεί να περιλαμβάνουν διπλής κατεύθυνσης ροή δεδομένων και/ή μεταφόρτωσης. Τα συστήματα και οι σταθμοί εργασίας με απομακρυσμένο έλεγχο, πρόσβαση ή λειτουργίες διαμόρφωσης μπορεί για παράδειγμα να είναι:

- Υπολογιστές και σταθμοί εργασίας στη γέφυρα ή το engine room στο διοικητικό δίκτυο
- Φορτίο όπως εμπορευματοκιβώτια με συστήματα ελέγχου θερμοκρασίας ή ειδικό φορτίο που παρακολουθείται από απόσταση
- Βοηθητικά συστήματα καθορισμού ευστάθειας
- Συστήματα παρακολούθησης hull-stress
- Συστήματα ναυσιπλοΐας συμπεριλαμβανομένων των ENC (Electronic Navigation Chart), VDR (Voyage Data Recorder), DP (Dynamic Position)
- Συστήματα σχεδιασμού φόρτωσης, στοιβασίας και διαχείρισης φορτίου
- Συστήματα ελέγχου και παρακολούθησης μηχανής
- Δίκτυα ασφαλείας όπως πχ CCTV (Closed Circuit TeleVision)
- Ειδικά συστήματα σε πλοία όπως λειτουργίες γεώτρησης, συστήματα υποθαλάσσιας εγκατάστασης, προφυλακτήρες έκρηξης, ESD (Emergency Shut Down) για τα gas tankers, υποβρύχιες εγκαταστάσεις και επισκευές καλωδίων

Η έκταση και η φύση της συνδεσιμότητας του εξοπλισμού θα πρέπει να είναι γνωστή στον πλοιοκτήτη ή αυτόν που το λειτουργεί και να αποτελεί σημαντικό κομμάτι στην αξιολόγηση κινδύνου.

2.5 Αξιολόγηση της πιθανότητας με βάση την απειλή και την τρωτότητα

Υπάρχει μία τάση να εκτιμούμε το ρίσκο στηριζόμενοι μόνο στα πιθανά αποτελέσματα και στα υπάρχοντα ευάλωτα σημεία. Παρόλα αυτά η πιθανότητα ενός cyber security γεγονότος να συμβεί είναι το «προϊόν» της απειλής και της τρωτότητας. Αυτό σημαίνει πως στην περίπτωση όπου ένας από αυτούς τους δύο παράγοντες είναι σχεδόν ανύπαρκτος τότε και οι πιθανότητες να συμβεί κάτι θα είναι εξίσου ανύπαρκτες, και αυτό θα πρέπει να λαμβάνεται υπόψη κατά την ποσοτικοποίηση της πιθανότητας. Στον SMS μιας εταιρίας περιλαμβάνονται τα risk assessments (εκτίμηση κινδύνου), όπου η πιθανότητα (likelihood) μετριέται σε μια five-step κλίμακα. Η χρήση της υπάρχουσας κλίμακας πιθανοτήτων αποτελεί πλεονέκτημα καθώς χρησιμοποιείται υπάρχουσα γλώσσα και σενάρια για να περιγραφούν όλα τα ρίσκα που σχετίζονται με τα cyber attack και διευκολύνουν την κατανόηση στην εταιρία. Μια ευθυγραμμισμένη επιχειρησιακή στρατηγική στην διαχείριση του ρίσκου και την κατανόηση είναι κρίσιμη στην εξασφάλιση της υποστήριξης στην ανώτερη ηγεσία για αποτελεσματική αντιμετώπιση βασιζόμενη στα αποτελέσματα του risk assessment. Ακολουθεί πίνακας ως παράδειγμα της κλίμακας:

LEVEL	LIKELIHOOD DESCRIPTION
1	Never heard of in industry. Close to being something unimaginable.
2	Heard of in industry, but only extremely rarely and as the result of a chain of many unfortunate events.
3	Incident has probably occurred in own company, but in the context of faulty equipment or by surprising mistakes made by people involved.
4	Happens occasionally in own company, typically in the context of faulty equipment or by mistakes by people involved (the kind of mistakes that tend to happen on board from time to time).
5	Happens frequently when undertaking the work in question.

Πίνακας 2: *Πίνακας παράδειγμα της κλίμακας πιθανοτήτων του SMS.*

2.6 Εκτίμηση αντίκτυπου

Όπως και κατά την εκτίμηση της πιθανότητας έτσι και στην εκτίμηση του αντίκτυπου-αποτελέσματος, το risk assessment του SMS αποτελείται από μια five-step κλίμακα. Η κλίμακα αυτή ταξινομείται σε αύξουσα σειρά με βάση την σοβαρότητα του αποτελέσματος για παράδειγμα την ασφάλεια του προσωπικού, του περιβάλλοντος, του φορτίου, των περιουσιακών στοιχείων, την συνέχεια της εταιρίας, το οικονομικό αντίκτυπο και την φήμη της εταιρίας. Ακολουθεί πίνακας ως παράδειγμα της κλίμακας:

LEVEL	IMPACT DESCRIPTION
1	No health effect/injuries. No damage to environment, assets, finances, or company's reputation.
2	Very slight health effect/injuries. Very slight damage to environment, assets, finances, or to company's reputation.
3	Some health effect/minor injuries. Minor damage to environment, assets, finances, or to company's reputation.
4	Major health effect/relatively serious injuries. Local but major damage to environment, assets, finances, or to company's reputation.
5	Fatality or permanent disabilities. Widespread, significant damage to

	environment, assets, finances, or company's reputation.

Πίνακας 3: *Πίνακας παράδειγμα της κλίμακας αντίκτυπου του SMS.*

2.7 Διαφορές IT (Information Technology) και OT (Operational Technology) συστημάτων

Ενώ τα συστήματα IT διαχειρίζονται δεδομένα και υποστηρίζουν τις λειτουργίες της εταιρίας, το OT είναι το hardware και το software που παρακολουθεί και ελέγχει φυσικές συσκευές και διαδικασίες οπότε είναι αναπόσπαστο μέρος του πλοίου και πρέπει να λειτουργεί ανεξάρτητα από τα IT συστήματα πάνω στο πλοίο. Τα συστήματα όμως μπορεί να είναι συνδεδεμένα στο IT δίκτυο για παρακολούθηση της απόδοσης, εξ αποστάσεως υποστήριξη κλπ. Το IT καλύπτει ένα φάσμα τεχνολογιών για την επεξεργασία πληροφοριών, συμπεριλαμβάνοντας software, hardware και τεχνολογίες επικοινωνιών. Το OT και το IT ήταν κατεξοχήν διαχωρισμένα αλλά με το διαδίκτυο, από αυτόνομα συστήματα, έχουν αρχίσει πλέον να ενσωματώνονται. Μία αναστάτωση στη λειτουργία του συστήματος OT μπορεί να προκαλέσει σημαντικό ρίσκο στην ασφάλεια του προσωπικού πάνω στο πλοίο, στο φορτίο, να προκαλέσει ζημιά στο θαλάσσιο περιβάλλον και να εμποδίσει τις λειτουργίες του πλοίου. Παρομοίως, ένα σφάλμα σε συγκεκριμένα IT συστήματα όπως για παράδειγμα η έλλειψη άμεσης πρόσβασης στη δήλωση επικίνδυνων αγαθών, μπορεί να προκαλέσει επικίνδυνες καταστάσεις. Για παράδειγμα στην περίπτωση όπου ένα εμπορευματοκιβώτιο στο πλοίο πάρει φωτιά, η πληροφορία για το περιεχόμενο του εμπορευματοκιβωτίου είναι απαραίτητη για την σωστή αντιμετώπιση της φωτιάς και τον τρόπο κατάσβεσης. Υπάρχουν σημαντικές διαφορές μεταξύ αυτών που αγοράζουν και διαχειρίζονται τα συστήματα OT έναντι των IT συστημάτων στο πλοίο. Οι IT managers, συνήθως δεν συμμετέχουν στην αγορά των OT συστημάτων και μπορεί ή μπορεί να μην έχουν πλήρη επίγνωση και κατανόηση του cyber security. Η αγορά τέτοιων συστημάτων θα πρέπει να περιλαμβάνει κάποιον που να γνωρίζει το αντίκτυπο στο πλοίο αλλά πολύ πιθανόν να έχει περιορισμένες γνώσει στα λογισμικά και στη διαχείριση του cyber risk. Είναι λοιπόν πολύ σημαντικό να υπάρχει διάλογος με έναν γνώστη του cyber security για να εξασφαλισθεί ότι τα cyber risks λαμβάνονται υπόψη κατά την αγορά ενός συστήματος OT. Η ενημέρωση και η αναβάθμιση του λογισμικού ενός OT συστήματος απαιτεί εξονυχιστικό έλεγχο συμβατότητας και έγκριση από την κλάση ενώ το IT λογισμικό, ενημερώνεται συστηματικά. Για να αποκτηθεί μία πλήρη εικόνα των πιθανών προκλήσεων και για να εκδοθεί η σωστή και απαραίτητη πολιτική και διαδικασίες για την συντήρηση των λογισμικών, η ομάδα που είναι υπεύθυνη για το cyber security θα πρέπει να έχουν μια λίστα απογραφής των συστημάτων OT.

2.8 Πλάνα και διαδικασίες

Κατά τον IMO και σύμφωνα με το MSC.428(98) resolution, υποδεικνύεται η ανάγκη για ευαισθητοποίηση στις απειλές που υπάρχουν στο cyber risk και στις αδυναμίες για να δημιουργηθεί ένα στήριγμα που θα οδηγήσει στην ασφαλή ναυτιλία, η οποία είναι λειτουργικά ευάλωτη σε cyber risks. Έτσι, όλα τα ενδιαφερόμενα μέρη τα ναυτιλίας θα πρέπει να δουλέψουν προκειμένου να οχυρώσουν και να προστατεύσουν την ναυτιλία από τους κινδύνους του κυβερνοχώρου και τα τρωτά τους σημεία. Επιπροσθέτως ο ΣΜΣ θα πρέπει να αντιμετωπίζει τη διαχείριση του cyber risk σύμφωνα με τoyς στόχους και τις λειτουργικές απαιτήσεις του κώδικα ISM. Στην 101η συνεδρία του IMO MSC (Maritime Safety Committee), συμφωνήθηκε πως πτυχές που αφορούν την διαχείριση του cyber risk, συμπεριλαμβανομένων πτυχών της φυσικής ασφάλειας του cyber security θα πρέπει να απευθύνονται στο Ships Security Plan (SSP) σύμφωνα με τον κώδικα ISPS (International Ship and Port Facility Security Code). Παρόλα αυτά δεν πρέπει να θεωρηθεί πως η εταιρία είναι υποχρεωμένη να εκδώσει ξεχωριστό σύστημα cyber security management λειτουργώντας παράλληλα με τον SMS της εταιρίας.

2.9 Ανάπτυξη μέτρων προστασίας (Defense in depth and in breadth)

Είναι σημαντικό να προστατεύσουμε τα κρίσιμα συστήματα και δεδομένα με πολλά «στρώματα» προστατευτικών μέτρων τα που λαμβάνουν υπόψη το ρόλο του προσωπικού, τις διαδικασίες και την τεχνολογία για να:

- Αυξηθούν οι πιθανότητες εντοπισμού ενός cyber incident
- Γίνεται η όσο το δυνατόν καλύτερη χρήση των πόρων που απαιτούνται για την προστασία την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων τόσο στα IT όσο και στα OT συστήματα.

Τα συνδεδεμένα συστήματα OT στο πλοίο πρέπει να έχουν περισσότερα από ένα τεχνικά και/ή διαδικαστικά μέτρα προστασίας. Οι περιμετρικές άμυνες όπως τα firewalls (τείχος προστασίας) είναι σημαντικά για την απώθηση ανεπιθύμητων εισόδων στα συστήματα αλλά πιθανόν να μην είναι αρκετά για να αντιμετωπίσουν κινδύνους εκ των έσω.

Τέτοιου βάθους άμυνες συνιστούν συνδυασμό:

- Φυσική ασφάλεια στο πλοίο όπως ορίζεται στο Ship Security Plan (SSP)
- Προστασία των δικτύων συμπεριλαμβάνοντας αποτελεσματικές τμηματοποιήσεις
- Εντοπισμό εισβολών
- Χρήση firewall
- Περιοδικά τεστ και σαρώσεις για τυχόν τρωτά σημεία
- Έλεγχος χρηστών και προσβασιμότητας
- Διαχείριση αλλαγών
- Σωστές διαδικασίες σε ότι αφορά αφαιρούμενα μέσα και κωδικούς
- Γνώση και κατανόηση του προσωπικού πάνω στο cyber security

- Κατανόηση κα εξοικείωση με τις σωστές διαδικασίες και την ανταπόκριση σε ένα περιστατικό

Οι πολιτικές και οι διαδικασίες της εταιρίας θα πρέπει να συμβάλλουν και να εξασφαλίζουν ότι το cyber security λαμβάνεται υπόψη μέσα στο γενικό πλαίσιο προσέγγισης της ασφάλειας και της διαχείρισης κινδύνου. Η πολυπλοκότητα και η πιθανή επιμονή μιας απειλής ότι θα πρέπει να υπάρχει μια προσέγγιση εις βάθους άμυνας. Ο εξοπλισμός και τα δεδομένα που προστατεύεται από στρώματα προστασίας είναι πιο ανθεκτικός σε cyber incidents.

Κατά την διαδικασία ενσωμάτωσης μεταξύ συστημάτων, θα πρέπει να υπάρχει ένα μοντέλο έμπιστων συνόρων όπου τα συστήματα θα είναι ομαδοποιημένα σε αυτά όπου η μεταξύ τους εμπιστοσύνη είναι σιωπηρή (π.χ. σταθμός εργασίας χρηστών) και μεταξύ αυτών όπου θα πρέπει να υπάρχουν σαφή όρια (π.χ. μεταξύ υπολογιστών γέφυρας και εταιρικών δικτύων).

Ωστόσο, στα πλοία όπου τα επίπεδα ενσωμάτωσης μεταξύ IT και OT συστημάτων μπορεί να είναι μεγάλα, η άμυνα εις βάθος λειτουργεί μόνο εάν τα τεχνικά και διαδικαστικά μέτρα προστασίας εφαρμόζονται σε στρώματα σε όλα τα τρωτά και ενσωματωμένα συστήματα. Αυτή είναι η άμυνα κατά πλάτος και χρησιμοποιείται για να αποτρέψει κάθε αδυναμία σε ένα σύστημα που χρησιμοποιείται για να παρακάμψει μέτρα προστασίας από άλλο σύστημα. Τόσο η άμυνα εις βάθος όσο και η άμυνα κατά πλάτος αποτελούν συμπληρωματικές προσεγγίσεις, οι οποίες, όταν υλοποιηθούν, παρέχουν την βάση για μία ολιστική απάντηση στη διαχείριση των cyber risks. Η υλοποίηση του cyber security control πρέπει να είναι σε προτεραιότητα, εστιάζοντας πρώτα σε αυτά τα μέτρα ή σε συνδυασμό των μέτρων, όπου προσφέρον το μεγαλύτερο όφελος. Φυσικά, όλα τα συστήματα μπορούν να προστατεύονται αλλά σε μερικές περιπτώσεις, οι δαπάνη σε χρόνο και χρήμα είναι μακράν περισσότερο από το ρίσκο.

2.10 Ανάπτυξη μέτρων εντοπισμού

Ο εντοπισμός μιας εισβολής ή μίας μόλυνσης είναι ένα κεντρικό μέρος της διαχείρισης των cyber risks. Μία βασική γραμμή της λειτουργίας του δικτύου και της ροής δεδομένων των χρηστών και των συστημάτων θα πρέπει να καθιερώνονται και να διαχειρίζονται, έτσι ώστε να υπάρξει συναγερμός με κατώτατα όρια για cyber incident. Το κλειδί σε αυτό αποτελεί ο καθορισμός των ρόλων και των ευθυνών για εντοπισμό ώστε να βοηθήσει να εξασφαλισθούν οι ευθύνες. Επιπροσθέτως η εταιρία μπορεί να επιλέξει να ενσωματώσει ένα Σύστημα Εντοπισμού Εισβολής (Intrusion Detection System-IDS) ή ένα Σύστημα Αποτροπής Εισβολής (Intrusion Prevention System-IPS) μέσα στο δίκτυο ή ως μέρος του firewall. Μερικές από τις βασικές λειτουργίες του περιλαμβάνουν αναγνώριση απειλής/κακόβουλης ενέργειας και κωδικού, και εν συνεχεία συνδέεται, αναφέρει και προσπαθεί να μπλοκάρει αυτήν την ενέργεια. Το πλήρωμα και γενικά το προσωπικό θα πρέπει να είναι ικανό να καταλάβει αυτούς τους συναγερμούς και τις επιπτώσεις. Αφού εντοπιστεί ένα συμβάν και γίνει γνωστό, θα πρέπει να ενημερωθεί ένας πάροχος υπηρεσιών, ο οποίος είναι υπεύθυνος για να δράσει σε τέτοιου είδους συναγερμούς. Ακόμα, το λογισμικό το οποίο σαρώνει και αυτόματα εντοπίζει και προσδιορίζει την ύπαρξη κακόβουλου λογισμικού στα συστήματα του πλοίου θα πρέπει να διαχειρίζεται και να είναι ενημερωμένο. Σαν γενική κατευθυντήρια γραμμή, οι υπολογιστές στο πλοίο θα πρέπει να είναι προστατευμένοι στον ίδιο βαθμό με αυτόν των υπολογιστών στην στεριά. Θα πρέπει δηλαδή να έχουν κατεβασμένο, συντηρημένο antivirus και antimalware λογισμικό σε όλα τα προσωπικά και στα σχετιζόμενα με τις εργασίες κομπιούτερ του πλοίου. Με αυτόν τον τρόπο θα μειωθεί ο

κίνδυνος να χρησιμοποιηθούν ως μέσω επίθεσης στους servers και στους άλλους υπολογιστές στο δίκτυο του πλοίου. Θα πρέπει ακόμα να ληφθεί υπόψη το πόσο συχνά το λογισμικό που σκανάρει πρέπει να ενημερώνεται και να αποφασιστεί εάν θα βασιστούμε σε αυτές τις μεθόδους άμυνας.

2.11 Ανταπόκριση και ανάκτηση από ένα περιστατικό cyber security

Το εναρκτήριο σημείο μιας αποτελεσματικής ανταπόκρισης είναι το πλάνο ανταπόκρισης να καλύπτει τα σχετικά ενδεχόμενα. Παρόλα αυτά είναι απίθανο τα πλάνα ανταπόκρισης να ταιριάξουν στο σενάριο του περιστατικού όπως αυτό εκτυλίσσεται. Γι' αυτό είναι σημαντικό να γίνονται τακτικά γυμνάσια πάνω στο πλάνο ανταπόκρισης και να αναπτύσσουμε ενδεχόμενα σύμφωνα με τα «lessons learned» που αφορούν τις απειλές, τις αδυναμίες και το αντίκτυπο. Για τα περισσότερα πλοία το πλάνο ενδεχομένων είναι ήδη τοποθετημένο στις διαδικασίες έκτακτης ανάγκης όπως απαιτείται από τον κώδικα ISM (ISM Code 1.4.5). Ένα περιστατικό στον κυβερνοχώρο απαιτεί ενεργή ανταπόκριση προκειμένου να γίνει το πλοίο λειτουργικό. Αν για παράδειγμα το σύστημα ECDIS έχει μολυνθεί με ένα κακόβουλο λογισμικό, η εκκίνηση του backup ECDIS μπορεί να προκαλέσει κι άλλο cyber incident. Έτσι λοιπόν συμπεραίνουμε πως θα πρέπει να χτίσουμε και να «προβάρουμε» ένα πλάνο ανταπόκρισης, στο οποίο θα αναλύονται οι ρόλοι και οι ευθύνες, οι τρόποι επικοινωνίας και οι βασικές δραστηριότητες-ενέργειες. Μπορεί να υπάρξουν περιπτώσεις που η ανταπόκριση σε ένα περιστατικό να είναι εκτός συναγωνισμού στο πλοίο ή στα κεντρικά γραφεία εξαιτίας της πολυπλοκότητας ή σοβαρότητας του περιστατικού. Σε αυτές τις περιπτώσεις θα πρέπει να υπάρχουν περαιτέρω βοήθειες από ειδικούς για να βοηθήσουν με πολλαπλές λειτουργίες, όπως ενέργειες δικτύου, ανωμαλίες στη συμπεριφορά συνδεδεμένων συσκευών ή τον εντοπισμό άγνωστων συσκευών, μη εγκεκριμένες ή μη συντονισμένων προσβάσεων προμηθευτών σε κρίσιμα συστήματα, και πτυχές ανταπόκρισης και ανάκτησης όπως ανάλυση και εκκαθάριση μετά από ένα περιστατικό. Τέλος θα πρέπει να χρησιμοποιούμε ως παραδείγματα και να μαθαίνουμε από προηγούμενα περιστατικά τόσο στον στόλο μας όσο και από άλλους στόλους, προκειμένου να βελτιώσουμε τα πλάνα ανταπόκρισης όλων των πλοίων στον στόλο της εταιρίας και θα πρέπει να υπάρχει μια στρατηγική πληροφόρησης για τέτοιου είδους περιστατικά.

2.12 Οι τέσσερεις φάσεις ανταπόκρισης σε περιστατικό

Όπως καθορίστηκε από τον NSIT (Netaji Subhas Institute of Technology), υπάρχουν τέσσερις φάσεις-κλειδιά στην ανταπόκριση ενός περιστατικού:

1. Preparation (Προετοιμασία)
2. Detection and analysis (Εντοπισμός και ανάλυση)
3. Containment and eradication (Περιορισμός και εξάλειψη)
4. Post-incident recovery (Ανάρρωση μετά το περιστατικό)

Ακολουθεί η ανάλυση κάθε φάσης ξεχωριστά:

1Η ΦΑΣΗ-Preparation:

Σε συμφωνία με προηγούμενες συμβουλές των κατευθυντήριων γραμμών:

- Καθορισμός των κρίσιμων εξαρτημάτων του πλοίου, της ιεράρχησης προτεραιότητας και της τοποθεσία τους
- Διασφάλιση τακτικών αντίγραφων ασφαλείας κατάλληλα όλων των σχετικών δεδομένων

- Προσδιορισμός σημείων αποτυχίας και καθορισμός λύσεων
- Δημιουργία πλάνου ανταπόκρισης και εξάσκηση αυτού τακτικά. Το πλάνο θα πρέπει να περιλαμβάνει τους ρόλους και τις ευθύνες του πληρώματος και του προσωπικού στην στεριά καθώς και οδηγίες για την καλή επικοινωνία. Το πλάνο θα πρέπει ακόμα να αναλύει λεπτομερώς τις διαδικασίες ανάκτησης κρίσιμων δικτύων και δεδομένων.

2Η ΦΑΣΗ-Detection and analysis:

Προκειμένου να διασφαλιστεί η κατάλληλη ανταπόκριση, η ομάδα ανταπόκρισης πρέπει να μάθει, όπου αυτό είναι δυνατόν:

- Πώς συνέβη το περιστατικό
- Ποια συστήματα IT ή/και OT επηρεάστηκαν και πως
- Το πόσο επηρεάστηκαν τα εμπορικά ή/και τα λειτουργικά δεδομένα
- Σε τι έκταση παραμένει οποιοσδήποτε κίνδυνος στα IT και OT συστήματα

3Η ΦΑΣΗ-Containment and eradication:

Ο περιορισμός ενός ξεσπάσματος περιστατικού είναι μια πρακτική που βασίζεται στον χρόνο. Όπου αυτό είναι δυνατό, αφαιρούμε την συσκευή από το δίκτυο. Όπου αυτό είναι αδύνατο, τότε είναι σημαντικό να περιοριστεί η συσκευή από το VLAN ή το LAN για να εξασφαλίσουμε ότι τα όρια ελέγχου είναι λειτουργικά ανάμεσα στα δίκτυα. Επιπροσθέτως:

- Έλεγχος των κανόνων του firewall για τυχόν αλλαγές. Ένας εκλεπτυσμένος επιτιθέμενος έχει τη δυνατότητα να ανοίξει τις θύρες του δικτύου. Όπου τα συστήματα λειτουργούν με internet ή VSAT, κλείνουμε την απομακρυσμένη πρόσβαση
- Διασφάλιση πως το anti-virus και το anti-malware είναι ενημερωμένα
- Βγάζουμε φωτογραφία οποιουδήποτε συστήματος επηρεάστηκε. Την αποθηκεύουμε κατάλληλα για να την στείλουμε για έρευνα στην στεριά. Εκεί θα γίνει η αναγνώριση, η τιτλοφόρηση, η καταγραφή, η διαχείριση, η μεταφορά, ο έλεγχος πρόσβασης και η ασφαλής αποθήκευση της εικόνας
- Σκεφτείτε να τραβήξετε φωτογραφίες (RAM images) καθώς βοηθάνε στην διαδικασία ανάλυσης. Σημειώστε πως το κλείσιμο ή η επανεκκίνηση του υπολογιστή θα καταστρέψει τα πτητικά δεδομένα όπως τη RAM οπότε είναι καλό να συμβουλευόμαστε κάποιον ειδικό σε τέτοιες περιπτώσεις.

4Η ΦΑΣΗ-Post-Incident recovery:

- Ανάκτηση συστημάτων και δεδομένων- Ακλουθώντας μια αρχική εκτίμηση του cyber incident, τα συστήματα IT και OT θα πρέπει να εκκαθαριστούν, να ανακτηθούν και να αποκαταστηθούν, όσο αυτό είναι δυνατόν, σε μία λειτουργική κατάσταση αφαιρώντας τους κινδύνους από το σύστημα και ανακτώντας το λογισμικό. Το περιεχόμενο του σχεδίου ανάκτησης θα αναλυθεί παρακάτω στο υποκεφάλαιο 2.12.
- Έρευνα του συμβάντος- Για την κατανόηση των αιτιών και των συνεπειών ενός cyber incident, είναι απαραίτητο να διεξαχθεί μια έρευνα από την εταιρία, με υποστήριξη από ειδικούς, αν κριθεί κατάλληλο. Οι πληροφορίες από την έρευνα, θα παίξουν σημαντικό ρόλο στο να αποτραπεί παρόμοιο συμβάν στο μέλλον. Οι έρευνες ενός cyber incident θα αναλυθούν σε επόμενο κεφάλαιο (2.14).
- Αποτροπή επανάληψης περιστατικού- Μετά το πέρας των ερευνών που αναφερθήκαμε παραπάνω, θα πρέπει να γίνουν ενέργειες ώστε να εντοπίσουμε και να προσδιορίσουμε

τυχόν ανεπάρκειες στα τεχνικά ή διαδικαστικά μέτρα προστασίας και να ληφθούν υπόψη, σύμφωνα με τις διαδικασίες εκτέλεσης διορθωτικών ενεργειών τις εταιρίας.

Όταν ένα cyber incident είναι πολύπλοκο, για παράδειγμα εάν το IT και/ή το OT σύστημα δεν μπορεί να επανέλθει σε κανονική λειτουργία, ίσως είναι απαραίτητο να γίνει έναρξη του πλάνου ανάκτησης μαζί με τα σχέδια έκτακτης ανάγκης στο πλοίο. Σε αυτή την περίπτωση, η ομάδα ανταπόκρισης θα πρέπει να παρέχει συμβουλές στο πλοίο:

- Εάν το IT ή το OT σύστημα θα πρέπει να τερματιστεί ή να συνεχίσει η λειτουργία του με σκοπό την προστασία των δεδομένων
- Εάν συγκεκριμένοι σύνδεσμοι επικοινωνίας στο πλοίο με την στεριά πρέπει να τερματιστούν και ποια βήματα συνεπαγωγής θα πρέπει να υπάρξουν
- Την κατάλληλη χρήση οποιωνδήποτε εργαλείων ανάκτησης διατίθενται στο ήδη εγκατεστημένο λογισμικό ασφαλείας
- Την έκταση την οποία το περιστατικό παραβίασε το σύστημα IT ή OT πέρα από τις δυνατότητες ανάκτησης που υπάρχουν στο πλάνο ανάκτησης

Όπως έχουμε αναφέρει ξανά, η εκπαίδευση και η επίγνωση είναι στοιχεία κλειδιά στην αποτελεσματική προσέγγιση στη διαχείριση του cyber risk. Είναι λοιπόν σημαντικό για το σχετικό προσωπικό στο πλοίο καθώς και στη στεριά να εκτελούν συχνές ασκήσεις στο cyber security.

2.13 Πλάνο ανάκτησης (Recovery plan)

Αντίγραφο του πλάνου ανάκτησης θα πρέπει να είναι διαθέσιμα σε έντυπη μορφή για το προσωπικό που είναι υπεύθυνο για το cyber security και που τους έχει ανατεθεί η να βοηθούν σε cyber incidents. Ο σκοπός του πλάνου είναι να υποστηρίξει την ανάκτηση των συστημάτων και των δεδομένων που είναι απαραίτητα ώστε να είναι σε λειτουργική κατάσταση τα συστήματα IT και OT. Για τνα διασφαλίσουμε την ασφάλεια του πληρώματος στο πλοίο, προτεραιότητα στο πλάνο έχει η ναυσιπλοΐα και η λειτουργικότητα του πλοίου. Η πολυπλοκότητα και η λεπτομέρειες ενός πλάνου ανάκτησης είναι ανάλογη του τύπου του πλοίου, των συστημάτων IT,OT και των υπόλοιπων εγκατεστημένων συστημάτων σε αυτό. Η ομάδα ανταπόκρισης θα πρέπει να αναλογιστεί προσεκτικά τις επιπτώσεις μίας ενέργειας ανάκτησης (όπως για παράδειγμα η εκκαθάριση ενός σκληρού δίσκου), που μπορεί να προκαλέσουν καταστροφή αποδεικτικών στοιχείων τα οποία πιθανόν να παρείχαν πολύτιμες πληροφορίες για τις αιτίες του συμβάντος. Όπου κρίνεται κατάλληλο, υποστήριξη από ειδικούς ανταποκριτές cyber incident θα πρέπει να λαμβάνεται προκειμένου να μας βοηθήσουν να διατηρήσουμε λίστα αποδείξεων ενώ παράλληλα ανακτούμε την λειτουργική ικανότητα. Η δυνατότητα ανάκτησης δεδομένων αποτελεί ένα πολύτιμο τεχνικό μέτρο προστασίας και είναι κανονικά στη μορφή ενός software backup για τα δεδομένα IT. Η διαθεσιμότητα ενός αντιγράφου ασφαλείας λογισμικού (software backup), είτε στο πλοίο είτε στη στεριά , θα ενεργοποιήσει την ανάκτηση του IT σε μία λειτουργική κατάσταση μετά από ένα cyber incident. Επειδή υπάρχουν ιστορικά καταγεγραμμένα περιστατικά όπου οι επιθέσεις με συγκεκριμένους ιούς εξαπλώθηκαν και στα αντίγραφα ασφαλείας,

συνιστώνται τα αντίγραφα ασφαλείας να είναι offline. Η ανάκτηση του OT μπορεί να είναι περισσότερο πολύπλοκη ειδικά εάν δεν υπάρχουν εφεδρικά συστήματα διαθέσιμα και μπορεί να χρειαστεί βοήθεια από την στεριά. Λεπτομέρειες για το πού μπορεί να βρεθεί αυτή η βοήθεια και από ποιόν θα πρέπει να αναγράφεται στο πλάνο ανάκτησης, για παράδειγμα με το να προχωρήσουμε σε ένα λιμάνι για να πάρουμε βοήθεια από έναν τεχνικό. Σε περίπτωση που υπάρχει εξειδικευμένο προσωπικό στο πλοίο, μπορεί να γίνουν εκτεταμένες διαγνώσεις και ενέργειες ανάκτησης, αλλιώς το πλάνο ανάκτησης θα πρέπει να περιορίζεται στο να παρέχει γρήγορη πρόσβαση σε τεχνική υποστήριξη. Είναι σημαντικό οι εταιρίες να τεστάρουν συχνά τις διαδικασίες ανάκτησης και όλη την συνεργασία πλοίου-στεριάς στην ανταπόκριση ενός cyber incident.

2.14 Δυνατότητα ανάκτησης δεδομένων(Data recovery capability)

Η δυνατότητα ανάκτησης δεδομένων αποτελεί την ικανότητα να επαναφέρουμε ένα σύστημα και/ή δεδομένα από ένα ασφαλές αντίγραφο ή εικόνα και κατ' επέκταση την επαναφορά ενός καθαρού συστήματος. Θα πρέπει να είναι διαθέσιμες απαραίτητες πληροφορίες και επαρκή software backup για την διασφάλιση της ανάκτησης έπειτα από ένα cyber incident. Οι περίοδοι διατήρησης και τα σενάρια επαναφοράς πρέπει να είναι καθιερωμένα ώστε να δίνεται προτεραιότητα στα κρίσιμα συστήματα που χρειάζονται γρήγορη επαναφορά δυνατοτήτων για να μειώσουν το αντίκτυπο ενός συμβάντος. Συστήματα που έχουν υψηλές απαιτήσεις διαθεσιμότητας δεδομένων θα πρέπει να φτιάχνονται ελαστικά. Τα συστήματα OT τα οποία είναι ζωτικής σημασίας για την ασφαλή ναυσιπλοΐα και τη λειτουργία του πλοίου, θα πρέπει να έχουν εφεδρικά συστήματα ώστε να επιτρέπουν στο πλοίο να ανακτά γρήγορα και με ασφάλεια τις δυνατότητες λειτουργίας και ναυσιπλοΐας μετά από ένα cyber incident.

2.15 Έρευνα ενός cyber incident

Η έρευνα ενός cyber incident μπορεί να παρέχει πολύτιμες πληροφορίες για τον τρόπο με τον οποίο μία αδυναμία έγινε εκμεταλλεύσιμη. Οι εταιρίες θα πρέπει, όποτε είναι δυνατόν, να ερευνούν ένα cyber incident που επηρέασε τα συστήματα IT και/ή OT στο πλοίο σε συμφωνία με τις διαδικασίες τις εταιρίας. Μια λεπτομερής έρευνα μπορεί να απαιτεί εκτεταμένη υποστήριξη από ειδικούς. Όπου αυτό είναι απαραίτητο η πλήρες εικόνα που πάρθηκε κατά τη φάση περιορισμού (βλ. 2.11 στη σελίδα 18) μπορεί να μοιραστεί με την ομάδα έρευνας. Κάθε στοιχείο που μπορεί να αποκτήθηκε και να διατηρήθηκε, θα είναι επιτρεπτό στο δικαστήριο αφού η διαδικασία δείχνει πως τα στοιχεία δεν έχουν νοθευτεί. Οι πληροφορίες από μια έρευνα μπορεί να χρησιμοποιηθούν ώστε να βελτιώσουν τα τεχνικά και τα διαδικαστικά μέτρα προστασίας στο πλοίο και στη στεριά. Μπορεί ακόμα να βοηθήσει στην ευρύτερη ναυτιλιακή βιομηχανία παρέχοντας καλύτερη κατανόηση στις απειλές στον κυβερνοχώρο. Κάθε έρευνα μπορεί λοιπόν να οδηγήσει σε:

- Καλύτερη κατανόηση των πιθανών κινδύνων που αντιμετωπίζει η ναυτιλιακή βιομηχανία τόσο στο πλοίο όσο και στην στεριά

- Αναγνώριση των διδαγμάτων ενός περιστατικού, ώστε να συμπεριληφθούν βελτιώσεις στην εκπαίδευση με σκοπό να αυξηθεί η επίγνωση του προσωπικού
- Ενημερώσεις σε τεχνικά και διαδικαστικά μέτρα προστασίας προκειμένου να παρεμποδίσουμε παρόμοια συμβάντα στο μέλλον

2.16 Απώλειες που προκύπτουν από ένα cyber incident

Καθώς τα ρίσκα που σχετίζονται με τον κυβερνοχώρο γίνονται κομμάτι του συνολικού ρίσκου που υπάρχει στο τοπίο, οι ναυτικές ασφαλιστικές αντιμετωπίζουν αυξημένες απαιτήσεις για ασφαλιστικά προϊόντα και υπηρεσίες κατά των ρίσκων σχετικά με τον κυβερνοχώρο. Η αξιολόγηση και η μείωση του ρίσκου είναι το πρώτο και κύριο, καθώς και βασική προϋπόθεση για την κάλυψη από την ασφαλιστική εταιρία. Τα cyber incidents μπορεί να προκαλέσουν οικονομικές απώλειες ή κόστη για την επαναδημιουργία χαμένων δεδομένων. Αυτά δεν ασφαλίζονται γενικά, αλλά για το κακόβουλο λογισμικό ransomware συγκεκριμένα υπάρχουν πλέον ασφαλιστικά πακέτα, τόσο στις ναυτιλιακές ασφαλιστικές αγορές όσο και στις υπόλοιπες ασφαλιστικές, προκειμένου να προστατεύσουν από αυτό το ρίσκο. Αυτό που αποτελεί πρόκληση για τους ασφαλιστές είναι η απώλεια δεδομένων ή φυσική ζημιά και πιθανό ρίσκο του συστήματος. Ένα επιτυχημένο cyber incident μπορεί να έχει σοβαρές επιπτώσεις σχετικά με την ασφάλιση:

- Απώλεια ζωής
- Τραυματισμός
- Μόλυνση
- Απώλεια/ζημιά φορτίου, εξοπλισμού διαχείρισης φορτίου
- Διακοπή της επιχείρησης
- Αξιοπιστία της επιχείρησης
- Απώλεια αγαθών
- Απώλεια δεδομένων
- Απώλεια φήμης
- Γενικά κάθε επακόλουθη ζημιά

Μία έρευνα που διεξήχθη από τους Lloyd's of London του 2017 δείχνει πως τα ρίσκα που σχετίζονται με cyber incidents εξελίσσονται ραγδαία και είναι ικανά να αποτελέσουν κίνδυνο του συστήματος, και συνεπώς δεν είναι κατ' ανάγκη ενιαία η προσέγγιση όσον αφορά την παρακολούθηση και την ποσοτικοποίηση του ρίσκου. Η έκθεση σε ένα cyber incident είναι ως εκ τούτου τακτικά ασφαλισμένη με κατάλληλους χειρισμούς και με το σύνολο των εκθέσεων να παρακολουθούνται κατάλληλα. Οι εταιρίες θα πρέπει να είναι σε θέση να επιδεικνύουν ότι δρουν μεριμνώντας σε ότι έχει να κάνει με την διαχείριση του cyber risk και την προστασία του πλοίου από κάθε είδους ζημιά που μπορεί να προκληθεί από τέτοιο περιστατικό.

2.16.1 Ασφάλιση φθοράς ιδιοκτησίας

Οι ασφαλιστικές λύσεις που καλύπτουν ζημιές και φθορές οι οποίες προκύπτουν από cyber risks γενικά και συγκεκριμένα από cyber incidents πρέπει να αναπτύσσονται σε κάθε εταιρία ατομικά. Η τρέχουσα κατάσταση μπορεί να συνοψιστεί ως εξής:

- Μερικές τοπικές ασφαλιστικές αγορές ακόμα εκδίδουν ασύνδετες συστάσεις για συγκεκριμένες γραμμές επιχειρήσεων αποκλείοντας τις ζημιές που σχετίζονται με το cyber risk/incident. Ιστορικά, η πιο διαδεδομένη εξαίρεση ήταν η CL380 για κακόβουλα cyber incidents (Institute Cyber Attack Exclusion Clause). Χρησιμοποιείται σε όλους τους τομείς και σε όλες τις δραστηριότητες της ναυτιλίας (φορτίο, ενέργεια, υπέρβαση απώλειας, hull, αξιοπιστία, ειδικότητα και πόλεμο). Ακόμα μια ευρέως χρησιμοποιούμενη εξαίρεση είναι η American Institute Cyber Exclusion Clause (01/06/2015).
- Άλλες αγορές μπορεί είτε να αναφέρουν ρητά την ασφάλιση του ρίσκου ή –σε όλες τις πολιτικές κινδύνου- να μην το ξεχωρίζει και να χορηγείται «σιωπηρή ασφάλιση» (π.χ. οι κίνδυνοι του κυβερνοχώρου να καλύπτονται στο συμβόλαιο χωρίς να αναφέρονται αποκλειστικά. Παρόλα αυτά θα πρέπει να σημειωθεί πως η προσέγγιση της σιωπηρής ασφάλισης εμπίπτει συχνά σε λεπτομερή έλεγχο.
- Τέλος, αυτό που αποκαλούμε «buy back solutions» μπορεί να εμπεριέχει το ρίσκο κάτω από ορισμένες προϋποθέσεις και έναντι πρόσθετου ασφάλιστρου με διαπραγμάτευση. Το buy back σημαίνει ότι το ρίσκο εξαιρείται στο συμβόλαιο αλλά υπάρχει επιλογή να συμπεριληφθεί επιπλέον κάλυψη για cyber risks/incidents υπό συγκεκριμένους όρους και έναντι πρόσθετου ασφάλιστρου.

Συνίσταται στις εταιρίες να ελέγξουν με τους ασφαλιστές/μεσίτες τους εκ των προτέρων εάν η πολιτική τους καλύπτει claims που προκλήθηκαν από ένα cyber incident. Έχουν δημοσιοποιηθεί κατευθυντήριες γραμμές για τις αγορές, όπου οι ναυτιλιακές ασφαλιστικές συνιστούνται να κάνουν ερωτήσεις στις εταιρίες για διαπιστώσουν τις γνώσεις τους σε ότι αφορά το cyber risk και τις μη-τεχνικές διαδικασίες. Οι εταιρίες θα πρέπει συνεπώς να περιμένουν αιτήματα για μη-τεχνικές πληροφορίες σε ότι αφορά την προσέγγιση τους στη διαχείριση του cyber risk από τους ασφαλιστές

2.16.2 Ασφάλιση της αξιοπιστίας

Συνίσταται η επικοινωνία με το P&I Club για λεπτομερείς πληροφορίες σχετικά με την κάλυψη που παρέχεται στους πλοιοκτήτες και τους ναυλωτές σε σχέση με την αξιοπιστία σε τρίτους (και τα σχετικά κόστη) που προκύπτουν από τις λειτουργίες των πλοίων. Ένα συμβάν, για παράδειγμα δυσλειτουργία των συστημάτων ναυσιπλοΐας ή των μηχανικών συστημάτων εξαιτίας μιας εγκληματικής ενέργειας ή ενός τυχαίου cyber incident, δεν αποτελεί αυτό καθ' αυτό την αφορμή για να προκαλέσει εξαίρεση από τη κανονική P&I ασφάλιση. Στην περίπτωση που ένα claim περιλαμβάνει cyber incident, μπορεί κάλλιστα να υπάρξει διαφωνία και να ισχυριστεί κάποιος ότι ήταν αποτέλεσμα ανεπαρκούς επιπέδου cyber security και προετοιμασίας. Έτσι λοιπόν τονίζεται περαιτέρω η σημασία του να έχει τη δυνατότητα η εταιρία να επιδείξει ότι δρα με σωστές προσεγγίσεις σε ότι αφορά τη διαχείριση του cyber risk και της προστασίας του πλοίου. Θα πρέπει να σημειωθεί πως πολλές απώλειες , οι οποίες μπορεί να προκύψουν από ένα cyber incident, δεν αποτελούν ευθύνες τρίτων που προκύπτουν από τη λειτουργία του πλοίο και έτσι το P&I δεν καλύπτει τέτοια ασφάλιση. Για παράδειγμα, η οικονομική απώλεια η οποία προέκυψε από ransomware ή η ανακατασκευή κατεστραμμένων δεδομένων δεν θα υπάρξει στην κάλυψη. Να σημειωθεί πως κανονικά η κάλυψη του P&I σε σχέση με την αξιοπιστία υπόκειται στην εξαίρεση του ρίσκου πολέμου και πως cyber incidents υπό συνθήκες πολέμου ή τρομοκρατικού είδους ρίσκα δεν καλύπτονται.

ΕΠΙΛΟΓΟΣ

Εν κατακλείδι, λαμβάνοντας υπόψη τα όσα αναφέρθηκαν και αναλύθηκαν στην παρούσα πτυχιακή, γίνεται πλέον φανερή η σημασία των κανονισμών που αφορούν στην πρόληψη και την αντιμετώπιση των cyber incidents. Οι κίνδυνοι και τα ρίσκα που έχουν προκύψει από την χρήση της τεχνολογίας στην ναυτιλία, δεν είναι κάτι το οποίο θα πρέπει να παίρνουμε αψήφιστα καθώς υπάρχουν παντού και μπορεί να έχουν καταστροφικά αποτελέσματα για το φορτίο, το περιβάλλον, την ανθρώπινη ζωή, την επιχείρηση και κατ΄ επέκταση την οικονομία. Οι εταιρίες και ο στόλος τους θα πρέπει να συμμορφώνονται με τους κανονισμούς και να λαμβάνουν όλα τα μέτρα πρόληψης και αντιμετώπισης, να εκπαιδεύουν και να ενημερώνουν το προσωπικό και τα πληρώματα τους. Οι κανονισμοί θα πρέπει πάντα να αναθεωρούνται και να εκσυγχρονίζονται όσο το δυνατόν συμβαδίζοντας με τους ρυθμούς της εξέλιξης της τεχνολογίας προκειμένου να καλύπτονται περισσότερα «ανοιχτά μέτωπα». Βασικότερο όλων είναι η πρόληψη ενός cyber incident και η επαγρύπνηση του προσωπικού ώστε να μην χρειαστεί ,όσο αυτό είναι δυνατόν, να φτάσουμε στο στάδιο της αντιμετώπισης ενός cyber incident καθώς ακόμα και αν αντιμετωπιστεί εν τέλει μπορεί ήδη να έχει προκληθεί κάποια ζημιά. Το cyber risk δεν είναι ένας θεωρητικός όρος. Όσες διευκολύνσεις κι αν έχει προσφέρει η χρήση της τεχνολογίας έχει φέρει μαζί της κινδύνους. Υπερνικούν τα οφέλη της τεχνολογίας τα ρίσκα; Ναι. Θα καταφέρει η ναυτιλιακή κοινότητα, σε συμμόρφωση πάντα με τους κανονισμούς, να ελαχιστοποιήσει και να αποφύγει τους κινδύνους; Αυτό θα το δείξει ο χρόνος.

ΠΗΓΕΣ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- **https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/**

- **http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf**

- **https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf**