ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΒΙΟΜΗΧΑΝΙΑΣ ΚΑΙ ΝΑΥΤΙΛΙΑΣ
ΤΜΗΜΑ ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΧΟΛΗ ΝΑΥΤΙΚΩΝ ΔΟΚΙΜΩΝ
ΤΜΗΜΑ ΝΑΥΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΔΠΜΣ ‘Διοίκηση στη Ναυτική Επιστήμη και Τεχνολογία’

ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΚΑΛΥΠΤΟΜΕΝΩΝ ΚΙΝΔΥΝΩΝ ΣΤΗ ΘΑΛΑΣΣΙΑ ΑΣΦΑΛΙΣΗ

MODERN FORMS OF COVERED RISKS AT SEA INSURANCE

Τουφεξής Αλέξανδρος

Διπλωματική Εργασία

που υποβλήθηκε στο Τμήμα Ναυτιλιακών Σπουδών του Πανεπιστημίου Πειραιώς ως μέρος των απαιτήσεων για την απόκτηση του Μεταπτυχιακού Διπλώματος Ειδίκευσης στην ΄Διοίκηση στη Ναυτική Επιστήμη και Τεχνολογία’

Πειραιάς

Οκτώβριος 2023

ΔΗΛΩΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ / ΖΗΤΗΜΑΤΑ COPYRIGHT

Το άτομο το οποίο εκπονεί την Διπλωματική Εργασία φέρει ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στην βάση των εξής παραγόντων: του σκοπού και χαρακτήρα της χρήσης (εμπορικός, μη κερδοσκοπικός ή εκπαιδευτικός), της φύσης του υλικού που χρησιμοποιεί (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες ή χάρτες), του ποσοστού και της σημαντικότητας των πιθανών συνεπειών αυτής στην αγορά ή στη γενικότερη αξία του υπό copyright κειμένου.

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

ΜΕΛΟΣ Α΄: Επίκουρος καθηγητής Κ. Δανιήλ Γεώργιος (Επιβλέπων)

ΜΕΛΟΣ Β΄: Επίκουρος καθηγητής Κ. Ζάννης Θεόδωρος

ΜΕΛΟΣ Γ΄: Επίκουρος καθηγητής Κ. Βαζούρας Χρήστος

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Δανιήλ Γεώργιο για την πολύτιμη βοήθεια και καθοδήγηση κατά την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας καθώς και να ευχαριστήσω θερμά τους αξιότιμους καθηγητές, μέλη της Τριμελούς Εξεταστικής Επιτροπής Κ. Ζάννη Θεόδωρο και Κ. Βαζούρα Χρήστο που με τίμησαν ως προς την βοήθεια και εξέταση της παρούσας εργασίας μου.

Τέλος, αισθάνομαι την ανάγκη να ευχαριστήσω θερμά τους γονείς μου για όλα όσα μου έχουν προσφέρει στη διάρκεια των φοιτητικών μου χρόνων, καθώς και την αμέριστη υποστήριξή τους σε κάθε μου επιλογή.

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη 6
Abstract 7
Εισαγωγή 8
Κεφ. 1. Θαλάσσια ασφάλιση πλοίου – Οι κλασικές μορφές θαλάσσιου κινδύνου 10
1.1 Η Θαλάσσια ασφάλιση πλοίου 10
1.2 Κλασικές μορφές κινδύνων – Κλασικοί και ανθρωπογενείς 11
1.3 Ρήτρες κάλυψης κλασικών κινδύνων στην θαλάσσια ασφάλιση 15
Κεφ. 2. Οι Κυβερνοεπιθέσεις στην Ναυτιλία 16
2.1 Ορισμοί 16
2.2 Τύποι κυβερνοεπιθέσεων 17
2.3 Στάδια κυβερνοεπίθεσης 27
2.4 Καταγραφή κυβερνοεπιθέσεων 28
Κεφ. 3. Τρωτά σημεία του πλοίου 31
3.1 Συστήματα του πλοίου που είναι ευάλωτα σε κυβερνοεπιθέσεις 31
3.2 Τα τρωτά σημεία του πλοίου 33
Κεφ. 4. Διεθνές νομοθετικό πλαίσιο για την Κυβερνοασφάλεια 34
4.1 Έρευνα 34
4.2 Ισχύουσες ρυθμίσεις 35
Κεφ. 5. Μέτρα αντιμετώπισης κυβερνοεπιθέσεων 43
5.1 Άμυνα σε βάθος 43
5.2 Άμυνα σε πλάτος 45
5.3 Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (CIA) 47
5.4 Αξιολόγηση του κινδύνου 48
5.5 Αξιολόγηση Κινδύνου Από Την Εταιρεία 50
5.6 Αξιολόγηση Κινδύνου από Τρίτους 51
5.7 Διαχείριση Κινδύνου – Μέτρα τεχνικής προστασίας 51
5.8 Διαδικαστικά Μέτρα προστασίας 58
Κεφ. 6. Αντιμετώπιση περιστατικών κυβερνοεπίθεσης 62
6.1 Αξιολόγηση κινδύνων - κατάρτιση Σχεδίου Αποτίμησης Επικινδυνότητας 62
6.2 Λύσεις Έξυπνων Λιμανιών - Κυβερνοασφάλεια των δικτύων 5ης γενιάς 64
6.3 Απώλειες που προκύπτουν από μια κυβερνοεπίθεση 65
6.4 Ερωτήσεις αξιολόγησης 67
Κεφ. 7. Συμπεράσματα 68
Κεφ. 8. Βιβλιογραφία 72

ΠΕΡΙΛΗΨΗ

Στον σημερινό κόσμο, η ναυτιλιακή βιομηχανία αντιμετωπίζει μια πρόκληση από τις κυβερνοεπιθέσεις, οι οποίες αυξάνονται συνεχώς με την πρόοδο της τεχνολογίας. Είναι κρίσιμο για όλους εκείνους που εμπλέκονται στον ναυτιλιακό τομέα να παραμένουν επιφυλακτικοί και να μάθουν πώς να προστατευτούν από αυτές τις απειλές. Γι' αυτό το λόγο, η διπλωματική μου εργασία επικεντρώνεται στο θέμα της ασφάλειας των πλοίων και των ναυτιλιακών επιχειρήσεων και των σύγχρονων κινδύνων που συνδέονται με την τεχνολογία, είτε αυτοί καλύπτονται είτε όχι από τους υφιστάμενους νόμους. Συγκεκριμένα, η εργασία μου έχει στόχο να παράσχει δεδομένα για την ανάλυση των κινδύνων που δημιουργούν οι κυβερνοεπιθέσεις, με ιδιαίτερη έμφαση στα θέματα της κυβερνοασφάλειας στα πλοία. Θα εξεταστούν οι τύποι επιθέσεων, οι ευάλωτοι παράγοντες ή τρωτά σημεία και τα στάδια μιας τέτοιας επίθεσης. Επιπλέον, θα αναφερθούν οι υφιστάμενες ρυθμίσεις που έχουν θεσπιστεί από οργανισμούς και νομοθετικά πλαίσια, καθώς επίσης θα προταθούν μέτρα για την αποτελεσματική αντιμετώπιση των περιστατικών που προκαλούνται από τις κυβερνοεπιθέσεις.
Εν κατακλείδι κάποια δικά μου συμπεράσματα και προτάσεις μου.

Λέξεις – Κλειδιά

<<Κυβερνοεπίθεση>>

<<Κυβερνοασφάλεια>>

<<Τρωτά σημεία>>

<<Ιός>>

<<Phishing>>

Abstract

In today's world the maritime industry faces a real challenge, from cyberattacks, which have become more prevalent with the advancement of technology. It is crucial for all those involved in the marine sector to remain vigilant and learn how to safeguard themselves against these threats. my diploma paper focuses on the subject of ship security and the modern risks associated with technology whether they are covered or not by existing laws. Specifically, my work aims to provide data for analyzing the risks posed by cyberattacks with an examination of cybersecurity issues on ships. It will refer to the types of these Cyberattacks, the vulnerabilities and the stages of such attacks. Additionally, it willdiscuss existing regulations established by organizations and legislative frameworks as well, as propose measures to effectively address incidents caused by cyberattacks.
In conclusion, some of my findings and proposals for their mitigation.

Keywords

<<Cyber attack>>
<<Cyber Security>>
<<Vulnerabilities>>
<<Virus>>
<<Phishing>>

ΕΙΣΑΓΩΓΗ

Στον σύγχρονο ψηφιακό κόσμο που ζούμε, στον οποίο η τεχνολογία λειτουργεί ως σημαντική προωθητική δύναμη σε κάθε πτυχή της ζωής μας, ο ναυτιλιακός κόσμος βρίσκεται στην πρώτη γραμμή της προόδου και της καινοτομίας. Είναι σαφές πως προκειμένου να αυξηθεί η παραγωγικότητα στις μεταφορές τους καθώς και η ασφάλεια όλες οι ναυτιλιακές υποδομές, ναυτιλιακές εταιρείες και τα πλοία υιοθετούν ολοένα και νέες τεχνολογίες για την βελτίωσή τους.
Ωστόσο, αυτή η αυξανόμενη βελτίωση χάρη στην τεχνολογία εκθέτει επίσης τον ναυτιλιακό κόσμο σε μια νέα σειρά απειλών και ευπάθειας.

Οι κυβερνοεπιθέσεις αποτελούν πλέον ένα πολύ σοβαρό πρόβλημα για τον ναυτιλιακό τομέα. Λόγω της ραγδαίας αύξησης της τεχνολογίας, τα πλοία και οι ναυτιλιακές επιχειρήσεις αντιμετωπίζουν πρωτοφανείς προκλήσεις με την εμφάνιση περίπλοκων κυβερνοεπιθέσεων απο κακόβουλους δράστες. Οι επιπτώσεις των κυβερνοεπιθέσεων στα πλοία και στις επιχειρήσεις επιφέρουν τρομερά <<πλήγματα>> καθώς πέραν των οικονομικών απωλειών και των επιχειρηματικών καταστροφών, μπορούν να θέσουν σε κίνδυνο την ασφάλεια του πληρώματος, την περιβαλλοντική ακεραιότητα και ακόμη και την εθνική ασφάλεια!

Ο κύριος στόχος της παρούσας έρευνάς μου είναι το μείζον πρόβλημα της κυβερνοασφάλειας και των κυβερνοεπιθέσεων στα πλοία, το οποίο εξετάζω προσεκτικά από όλες τις οπτικές γωνίες. Αναφέρονται όσα περισσότερα στοιχεία για την κατανόηση των λόγων αυτών των επιθέσεων και τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι καθώς αναφέρομαι και στις διάφορες μορφές κυβερνοαπειλών που στοχεύουν τα ναυτικά συστήματα στα πλοία.

Εξετάζονται τα αδύνατα σημεία ή τα τρωτά σημεία των πλοίων, καθώς και οι πιθανές συνέπειες μιας επιτυχημένης κυβερνοεπίθεσης σε αυτά. Είναι ένα σημαντικό βήμα η κατανόηση αυτών των κυβερνοεπιθέσεων καθώς θα βοηθήσει τους ενδιαφερόμενους

φορείς του ναυτιλιακού κλάδου να βελτιώσουν τις αμυντικές τους ικανότητες και να υιοθετήσουν αποτελεσματικά μέτρα κυβερνοασφάλειας στις επιχειρήσεις τους.

Επιπλέον, αναφέρονται τα νομικά πλαίσια για το δίκαιο και τους κανονισμούς που διέπουν την κυβερνοασφάλεια στο ναυτιλιακό τομέα (Ισχύουσες ρυθμίσεις προστασίας). Αυτοί οι νόμοι, που αναφέρονται από διεθνείς συμφωνίες έως κρατικούς κανονισμούς, παίζουν κρίσιμο ρόλο στη διατήρηση της ακεραιότητας και της ασφάλειας των διεθνών ναυτιλιακών λειτουργιών.

Τέλος, η παρούσα έρευνά μου στοχεύει να <<αφοπλίσει>> τους φορείς του ναυτιλιακού κλάδου με τις απαραίτητες πληροφορίες και τους πόρους που απαιτούνται για να προστατεύσουν αποτελεσματικά τα πλοία και τις επιχειρήσεις από τις πιθανές κυβερνοεπιθέσεις.
Η εργασία αποτελεί μια εξερεύνηση στα μείζον ζητήματα της κυβερνοασφάλειας και των κυβερνοεπιθέσεων στα πλοία και στις ναυτιλιακές επιχειρήσεις, όπου η συνέπεια, η προσαρμοστικότητα και η εγρήγορση αποτελούν τους καθοδηγητικούς φάρους για την εξασφάλιση του μέλλοντος των ναυτιλιακών οργανισμών.

<u>Κεφάλαιο 1.</u> Θαλάσσια ασφάλιση πλοίου – Οι κλασικές μορφές θαλάσσιου κινδύνου

1.1 Η Θαλάσσια ασφάλιση πλοίου

Η θαλάσσια ασφάλιση ενός πλοίου αποτελεί ένα αναπόσπαστο μέρος της ναυτιλιακής βιομηχανίας, προστατεύοντας τα πλοία και το φορτίο τους από τους διάφορους κινδύνους που συναντούν κατά τη διάρκεια των ταξιδιών.

Ο ορισμός που μπορούμε να δώσουμε είναι ότι η θαλάσσια ασφάλιση αποτελεί ένα είδος ασφάλισης που καλύπτει τους κινδύνους που μπορούν να προκύψουν στα πλοία με τη μεταφορά αγαθών και άλλων δραστηριοτήτων που σχετίζονται με τη θαλάσσια ή ότι αναφέρεται στο είδος της ασφάλισης που καλύπτει τα πλοία από διάφορους κινδύνους και απώλειες που μπορούν να προκύψουν κατά την διάρκεια της λειτουργίας τους στην θάλασσα. Σημαντικό κομμάτι της είναι ότι παρέχεται οικονομική προστασία στους ιδιοκτήτες πλοίων, και σε άλλους ενδιαφερόμενους φορείς του ναυτιλιακού τομέα απέναντι σε πιθανές απώλειες ή ζημίες των φορτίων τους ή των πλοίων τους.

Παρακάτω παρουσιάζονται ορισμένοι κοινοί κίνδυνοι που συνήθως καλύπτονται στην ασφάλιση του πλοίου:

<u>Θαλάσσιοι κίνδυνοι</u>: Σε αυτή την κατηγορία περιλαμβάνονται οι κίνδυνοι που σχετίζονται με το θαλάσσιο περιβάλλον, όπως καταιγίδες, τυφώνες, θαλασσοταραχές, αστραπές και άλλες δυσμενείς καιρικές συνθήκες.

<u>Πυρκαγιά και Έκρηξη</u>: Οι ζημιές από πυρκαγιές και εκρήξεις στο εσωτερικό του πλοίου καλύπτονται από τη θαλάσσια ασφάλεια. Μπορούν να αποτελέσουν σοβαρές απειλές για το πλοίο και το φορτίο του.

<u>Σύγκρουση:</u> Αφορά τις ζημιές που προκαλούνται από συγκρούσεις με άλλα πλοία, συγκρούσεις με επικίνδυνα αντικείμενα ή κινδύνους από την θάλασσα όπως βράχους ή ύφαλους.

<u>Ναυάγιο</u>: Όταν ένα πλοίο βυθίζεται ως αποτέλεσμα ατυχήματος ή άλλου απρόβλεπτου γεγονότος, παρέχεται κάλυψη στην περίπτωση που το πλοίο χάνεται εντελώς στη θάλασσα.

Αγκυροβολισμός: Αυτή η κάλυψη ισχύει σε περίπτωση παρατεταμένου αγκυροβολισμού λόγω απόκλισης του πλοίου από την προοριζόμενη διαδρομή, βλάβης εξοπλισμού ή κακών καιρικών συνθηκών.

Ληστεία - Πειρατεία: Περιλαμβάνουν ασφάλεια κάλυψης για απώλειες λόγω πειρατείας ή ληστείας με ένοπλα μέσα στη θάλασσα, κτλ.

1.2 Κλασικές μορφές κινδύνων – Φυσικοί και ανθρωπογενείς

Οι κλασικοί θαλάσσιοι κίνδυνοι οι οποίοι χωρίζονται είτε σε φυσικούς είτε σε ανθρωπογενείς είναι από παλιών χρόνων και είναι οι κίνδυνοι που απορρέουν από τη ναυσιπλοΐα. Ας αναφέρουμε ονομαστικά ορισμένους από αυτούς τους κινδύνους: Η φωτιά στο πλοίο, οι πολεμικοί κίνδυνοι, η πειρατεία, η κλοπή, οι συλλήψεις, οι κατασχέσεις, οι περιορισμοί από αρχές ή από λαούς, οι αβαρίες, οι ναυταπάτες κτλ.

Εν συνέχεια, θα δοθεί λίγη έμφαση σε μερικούς από τους κλασικούς κινδύνους που μπορεί να συμβούν κατά την διάρκεια ενός ταξιδιού στο πλοίο:

1.2.1 Κίνδυνος πυρκαγιάς

Σαν ορισμός, πυρκαγιά είναι η ανεξέλεγκτη φωτιά, η οποία προκαλείται από μη ελεγχόμενη καύση με το οξυγόνο και συνοδεύεται από πρόκληση μεγάλων ποσών θερμότητας και φωτός, γεγονός που έχει ως συνέπεια την καταστροφή του καιγόμενου υλικού. Το τελευταίο γεγονός, συνέβη τον Μάρτιο του 2022, στο οποίο προέκυψε κάτω από αδιευκρίνιστες συνθήκες φωτιά σε φορτηγό πλοίο που μετέφερε αυτοκίνητα του VW Group.
Το Felicity Ace εξέπεμψε σήμα κινδύνου ύστερα από φωτιά που ξέσπασε στο αμπάρι του. Διασώθηκαν και τα 22 μέλη του πληρώματος, όμως μεγάλη ήταν η ζημιά στα αυτοκίνητα που μετέφερε.

(εικ.1 – η φωτιά που προκλήθηκε στο Felicity Ace)

Οι πυρκαγιές στα καράβια χαρακτηρίζονται ως ένας από τους κλασικούς κινδύνους που μπορεί να συμβούν από απροσεξία του πληρώματος πάνω σε θέματα που αφορούν τις τροφοδοτήσεις συστημάτων του πλοίου πχ (λόγω της βλάβης του υδραυλικού συστήματος) κτλ, είτε ενός αδιάφορου αιτίου εξαιτίας του οποίου αυτή προκλήθηκε.

1.2.2 Τρικυμία – Θαλασσοταραχή

Πρόκειται για τις εν γένει δυσμενείς καιρικές συνθήκες στη θάλασσα, συνεπεία των ισχυρών επικρατούντων ανέμων με αποτέλεσμα να προκληθούν ζημιές στα εμπορεύματα που μεταφέρει το πλοίο είτε αυτά να σπάσουν / χαλάσουν είτε αυτά να χαθούν στην θάλασσα. Π.χ, το συγκεκριμένο tanker που απέπλευσε με άνεμο άνω των 11 μποφόρ (τυφώνας – ισχυρή θύελλα), με αποτέλεσμα την πρόκληση ζημιών επί του καραβιού.

(εικ.2 – ισχυροί άνεμοι μποφόρ άνω του 11 της κλίμακας)

1.2.3 Πειρατεία – Κλοπές

Ως πειρατεία ορίζουμε οποιεσδήποτε παράνομες πράξεις βίας ή κράτησης ή πράξεις καταστροφής που διαπράχθηκαν για ιδιωτικούς σκοπούς από το πλήρωμα ή τους επιβάτες ενός ιδιωτικού πλοίου, που συμβαίνει στην θάλασσα, εναντίον άλλου πλοίου ή κατά προσώπων ή περιουσιακών στοιχείων επί του πλοίου.

Οι πειρατές εμποδίζουν τις θαλάσσιες μεταφορές σε διαφορετικές τοποθεσίες σε ολόκληρο τον πλανήτη όπως πχ, (Σομαλία, ο κόλπος τους Νιγηρίας, κτλ), με σκοπό την εκμετάλλευση των αγαθών που μεταφέρει το πλοίο ή και την αιχμαλωσία του πληρώματος, για την είσπραξη λύτρων. Δεδομένου ότιπάνω από το 75% του παγκόσμιου εμπορίου μεταφέρεται δια θαλάσσης, ο εμπορικός αντίκτυπος τους πειρατείας στη ναυτιλιακή βιομηχανία είναι τεράστιος.

Τελευταίο γεγονός πειρατείας, συνέβη σε δεξαμενόπλοιο εγγεγραμμένο στον νηογνώμονα της Σιγκαπούρης, στα ανοικτά της Ακτής Ελεφαντοστού. Στο δεξαμενόπλοιο <<Success 9>> βρίσκονταν 20 μέλη πληρώματος, με ευτυχώς όλο το πλήρωμα, συμπεριλαμβανομένων των μελών των πληρώματος από τη Σιγκαπούρη, να είναι σώο και αβλαβές.

1.2.4 Αβαρίες

Αβαρίες είναι αυτές που απαντώνται κυρίως στις θαλάσσιες μεταφορές, όπου κατά τη διεξαγωγή τους πολλές φορές καθίσταται αναγκαία, λόγω εκτάκτων καταστάσεων, η απόρριψη (εκβολή – θυσία), μέρους του μεταφερόμενου φορτίου στη θάλασσα, προς ανακούφιση και διάσωση του πλοίου και του υπόλοιπου φορτίου.

1.2.5 Κίνδυνος ναυαγίου

Το ναυάγιο αποτελεί έναν από τους σοβαρότερους κινδύνους στη θαλάσσια ασφάλιση. Περιλαμβάνει το ατύχημα και την καταστροφή του πλοίου, με την πιθανή απώλεια ανθρώπινων ζωών και φορτίου.

1.2.6 Κίνδυνος ρύπανσης

Τα ατυχήματα που οδηγούν στη διαρροή ρυπαντικών υλικών από πλοία μπορούν να έχουν σοβαρές επιπτώσεις στο περιβάλλον και την υγεία του ανθρώπου.

1.2.7 Κίνδυνος σύγκρουσης

Οι συγκρούσεις μεταξύ πλοίων, είτε πρόκειται για σύγκρουση με άλλο πλοίο είτε με αντικείμενα όπως βράχους ή ρηχά, μπορούν να προκαλέσουν ζημιές.

1.3 Μερικές από τις ρήτρες κάλυψης κλασικών κινδύνων στην θαλάσσια ασφάλιση

Όπως αναφέραμε, υπάρχουν πολλοί φυσικοί είτε ανθρωπογενείς κλασικοί κίνδυνοι πέραν των ψηφιακών που μπορούν να συμβούν σε ένα πλοίο κατά το ταξίδι του, όπως, η πυρκαγιά, η έκρηξη, η κλοπή, η εκβολή, η πειρατεία, η πρόσκρουση του πλοίου, η σύγκρουση πλοίων, η αμέλεια του πληρώματος, η γενική αβαρία, οι κίνδυνοι πολέμου και τρομοκρατικών ενεργειών, κτλ. Όλοι αυτοί οι κίνδυνοι καλύπτονται από ρήτρες και ασφαλιστικές καλύψεις (H&M, War, IV. LOH, κτλ) αλλά και από τις ρήτρες ασφάλισης των φορτίων αυτών:

Η ρήτρα ασφάλισης C, είναι αυτή η οποία καλύπτει τους βασικούς κινδύνους στις θαλάσσιες μεταφορές όπως, η πυρκαγιά, η προσάραξη, η βύθιση, η σύγκρουση, συμμετοχή σε γενική αβαρία κλπ. ή σε σχετικούς κινδύνους που προέρχονται από ατύχημα (τυχαίο γεγονός, ανεξάρτητο από τη θέληση κάποιου, με άμεση συνέπεια τις υλικές ζημίες των ασφαλισμένων αντικειμένων).

Η ρήτρα ασφάλισης B, είναι αυτή που αφορά κατονομαζόμενους κινδύνους. Καλύπτονται όλοι οι βασικοί κίνδυνοι όμως λιγότεροι της Ρήτρας A, και περιλαμβάνει ότι ακριβώς και η ρήτρα C και επιπλέον και άλλες μορφές κινδύνων, όπως ο σεισμός, η έκρηξη ηφαιστείου, ο κεραυνός, κτλ.

Η ρήτρα ασφάλισης A, (κατά παντός κινδύνου) με την οποία καλύπτονται όλοι οι κίνδυνοι ζημιών κατά τη διάρκεια του ταξιδιού.

Κεφάλαιο 2. Οι Κυβερνοεπιθέσεις στην Ναυτιλία

2.1 Ορισμοί

Κυβερνοεπιθέσεις (Cyber Attacks): Κυβερνοεπιθέσεις ονομάζονται οι επιθέσεις που γίνονται με την χρήση της τεχνολογίας στα υπολογιστικά συστήματα. Όλα τα υπολογιστικά συστήματα (στα πλοία, σε εταιρείες, κτλ), τα δίκτυα, οι συσκευές και τα δεδομένα αποτελούν πιθανούς στόχους επιθέσεων από επιτιθέμενους που αναφέρονται ως κυβερνοεπιθέσεις. Αυτές οι επιθέσεις πραγματοποιούνται από άτομα που είναι γνωστά ως "χάκερ" ή από οργανισμούς με σκοπό να διεισδύσουν στα συστήματα και να τα εκμεταλλευτούν με διάφορους αρνητικούς τρόπους. Οι κυβερνοεπιθέσεις έχουν τη δυνατότητα να προκαλέσουν πολύ σοβαρές ζημιές σε άτομα, επιχειρήσεις, πλοία και ακόμη και ολόκληρες χώρες, οδηγώντας σε οικονομικές απώλειες, παραβίαση δεδομένων, και ακόμη και κινδύνους για την εθνική ασφάλεια.

Κυβερνοασφάλεια (Cyber Security):. Είναι ένα πολύ σημαντικό κομμάτι για όλες τις επιχειρήσεις διάφορων κλάδων καθώς είναι η διαδικασία προστασίας των υπολογιστικών συστημάτων, των δικτύων, των συσκευών και των δεδομένων από διάφορους ψηφιακούς κινδύνους όπως οι κυβερνοεπιθέσεις. Ο κύριος στόχος της κυβερνοασφάλειας είναι η διατήρηση της προστασίας και της ασφάλειας των υποδομών της πληροφορικής και των περουσιακών στοιχείων των επιχειρήσεων από πιθανές επιθέσεις στο διαδίκτυο, διατηρώντας την ακεραιότητα και την προσβασιμότητα των δεδομένων.

Hacker: Είναι ένα άτομο που κατέχει τεχνικές δεξιότητες και γνώσεις στον υπολογιστικό χώρο και χρησιμοποιεί αυτές τις γνώσεις προς όφελός του ή προς κοινό σκοπό για να αναζητήσει, να εισχωρήσει (ή παραβιάσει) και να επωφεληθεί από αυτές μέσω των ευπαθειών ή κάποιων τρωτών σημείων στα υπολογιστικά συστήματα και στα δίκτυα. Οι χάκερς μπορούν να χρησιμοποιήσουν τις δεξιότητές τους για διάφορους σκοπούς, συμπεριλαμβανομένων των διαρρήξεων ασφάλειας επιχειρήσεων, της προσπάθειας παραβίασης δικτύων, των κλοπών δεδομένων ή της καταστροφής των δεδομένων.

Κυβερνοαπειλές (Cyber Threats): Αυτές αναφέρονται σε ενδεχόμενες ή πιθανές επιθέσεις που μπορούν να απειλήσουν την Κυβερνοασφάλεια.

Cracker: Είναι αυτός που με σκοπό να αποκτήσει πρόσβαση σε διάφορες πληροφορίες ή να προκαλέσει ζημιά, παραβιάζει την ασφάλεια δικτύων και υπολογιστικών συστημάτων. Οι crackers χρησιμοποιούν όλη αυτή την γνώση για να "σπάσουν" προγράμματα, να δημιουργήσουν ζημιά ιστοσελίδες, να κλέψουν δεδομένα, να φτιάξουν ιούς με κακόβουλο σκοπό, κλπ.

2.2 Τύποι κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις που πραγματοποιούνται σε ναυτιλιακές εταιρίες αλλά και στα πλοία μπορούν να πάρουν διάφορες μορφές ανάλογα με το εύρος της ζημιάς που προκαλούν, διακρίνοντάς τες σε δύο κατηγορίες: **α) στοχευμένες επιθέσεις** και **β) μη στοχευμένες επιθέσεις**.

<u>Στοχευμένες επιθέσεις:</u> Ορίζονται οι επιθέσεις στην οποία μια εταιρία ή τα συστήματα ενός πλοίου είναι ο στόχος από τους επιτιθέμενους Hackers. Συνήθως είναι πιο περίπλοκες και οι συγκεκριμένες επιθέσεις χρησιμοποιούν τα ακόλουθα μέσα/ εργαλεία για να επιτύχουν τον στόχο τους:

Phishing

Το Phishing είναι μια μορφή κυβερνοεπίθεσης όπου οι επιτιθέμενοι προσποιούνται και φέρονται ως έμπιστοι άνθρωποι ή έμπιστες ιστοσελίδες με σκοπό να απατήσουν τα θύματά τους και να τους κάνουν να δώσουν ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών. Αυτό συνήθως γίνεται μέσω ψεύτικων ηλεκτρονικών μηνυμάτων, emails, spams και ιστοσελίδων ή λογαριασμών κοινωνικών μέσων που

μοιάζουν πολύ με τις πραγματικές. Είναι η πιο διαδεδομένη μέθοδος κυβερνοεπίθεσης στον ψηφιακό κόσμο. Συνήθως όλοι μας έχουμε στα ανεπιθύμητα μηνύματα στο email μας κάποιου μορφή αυτής της επίθεσης (spam folders, τράπεζες, κτλ).

Γενικώς μέσω του Phishing προσπαθούν να απατήσουν τους χρήστες και να τους πείσουν να αποκαλύψουν τις προσωπικές τους πληροφορίες. Οι κακόβουλοι δράστες μπορούν στη συνέχεια να χρησιμοποιήσουν αυτές τις πληροφορίες για να κλέψουν χρήματα ή να πραγματοποιήσουν άλλες παράνομες ενέργειες. Όλες οι ναυτιλιακές επιχειρήσεις και οι στόλοι τους πρέπει να επιδεικνύουν ιδιαίτερη προσοχή κατά τη χρήση των διαδικτυακών επικοινωνιών, αποφεύγοντας να παρέχουν σημαντικές πληροφορίες σε αναξιόπιστες πηγές.

Spear-phishing

Η αλλιώς το στοχευμένο ηλεκτρονικό ψάρεμα. Είναι πιο εξελιγμένη και αρκετά πιο επικίνδυνη μέθοδος επίθεσης του 'ηλεκτρονικού ψαρέματος'. Ο επιτιθέμενος (Hacker) συλλέγει τις πληροφορίες που θέλει σχετικά με το θύμα ή κάποια εταιρεία χρησιμοποιώντας μεθόδους κοινωνικής αναζήτησης όπως forums, ανοικτά κοινωνικά δίκτυα, κ.τ.λ. Πρόκειται για μια μορφή απάτης στο διαδίκτυο, όπου ο επιτιθέμενος στοχεύει ειδικά μια συγκεκριμένη ομάδα ατόμων με προσαρμοσμένα μηνύματα email ή άλλες μεθόδους, προκειμένου να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες.

PARAMETER	PHISHING	SPEAR PHISHING
TARGET	Hackers go after a large number of targets	The target is usually one organization. Fraudulent emails are sent to a handful of well-researched employees.
VALUE	Phishing targets are low-yield, with not many organizational assets at stake	Phishing targets are high-yield. In personalized attacks, victims willingly compromise extra-sensitive data.

(εικ.3 – Διαφορές Phishing με Spear – Phishing)

Όπως βλέπουμε και στην παραπάνω εικόνα οι διαφορές του Phishing με το Spear Phishing, είναι η στοχευμένη επίθεση – σε ένα κοινό/ εταιρεία/οργανισμό κτλ, με τους Hackers, να συμβάλλουν στην βέλτιστη δημιουργία μιας μη αξιόπιστης ιστοσελίδας που φαίνεται σχεδόν 100% αληθινή σε αντίθεση με το απλό ηλεκτρονικό ψάρεμα, με σκοπό την υποκλοπή των στοιχείων του θύματος.

Denial of Services (DDoS Attack) - Επιθέσεις άρνησης υπηρεσιών

Οι επιθέσεις που στοχεύουν στην υπερφόρτωση ενός δικτύου ή μιας ιστοσελίδας με υπερβολικά μη χρήσιμα αρχεία με σκοπό να την καταρρίψουν αποκαλούνται "Διανεμημένες επιθέσεις Άρνησης Υπηρεσίας" (DDoS). Είναι η πιο κοινή μέθοδος που χρησιμοποιούν οι επιτιθέμενοι, μαζί με το phishing, για να στοχεύσουν τα πλοία και να υπερφορτώσουν τα συστήματά τους, καθιστώντας τα ανίκανα να ανταποκριθούν στις εντολές του πληρώματος και οδηγώντας στην αναποτελεσματικότητα ή τον έλεγχο του πλοίου από τον επιτιθέμενο. Παρακάτω παρουσιάζεται σε βήματα μια λεπτομερής περιγραφή του μοτίβου της DDoS:

Επίθεση DDoS (Διανεμημένη Άρνηση Υπηρεσίας):

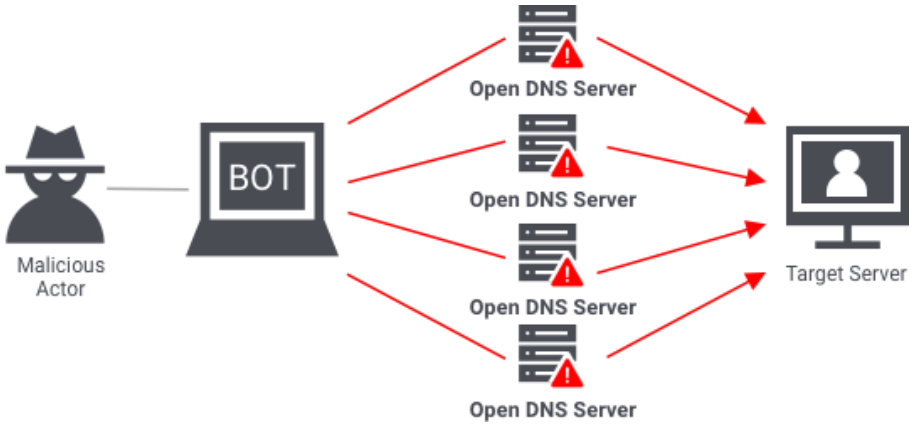
Α) Ο χάκερ χρησιμοποιεί ένα botnet που είναι μια συλλογή από μολυσμένους μη συνδεδεμένους υπολογιστές υπό τον έλεγχό του για να προκαλέσει μια επίθεση.
Β) Το κύκλωμα αυτό, το οποίο αποτελείται από πολλούς υπολογιστές έχει μολυνθεί από κακόβουλο λογισμικό malware.

Γ) Η επίθεση DDoS ξεκινά από τον χάκερ με την ταυτόχρονη παράδοση ενός τεράστιου όγκου κίνησης ή αιτημάτων στον στόχο, το δίκτυο ή τον ιστότοπο του πλοίου.

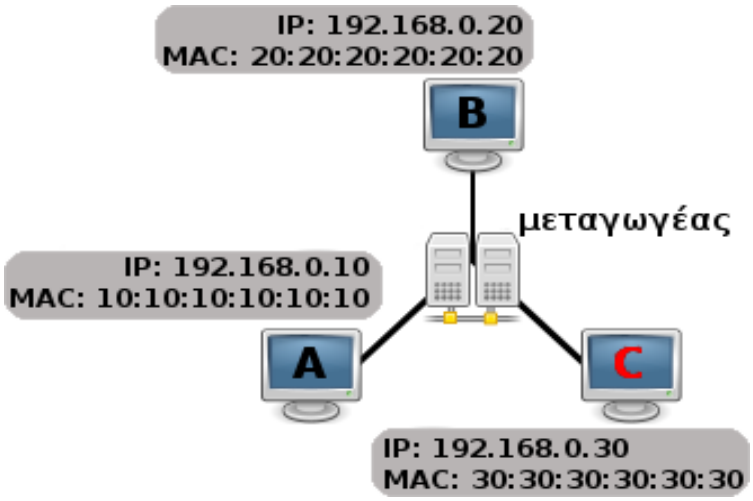
Δ) Ο τεράστιος όγκος αυτός της εισερχόμενης κίνησης επιβαρύνει το δίκτυο του στόχου, μειώνοντας την ανταπόκριση και τη διαθεσιμότητα.

Ε) Τα συστήματα του πλοίου μπορούν να σταματήσουν να λειτουργούν σωστά, καθιστώντας δυσκολότερο για το πλήρωμα τον έλεγχο του σκάφους.

Ζ) Αυτό έχει σαν αποτέλεσμα κατάρριψη όλων των υπολογιστικών συστημάτων του πλοίου και τον έλεγχο του χάκερ.



(εικ. 4 – πρότυπο επίθεσης DDoS)



(Είκ.5 - παράδειγμα DDoS Attack με χρήση IP)

Social engineering

Απάτες που χρησιμοποιούν την ψυχολογία και την καλή πίστη ατόμων που ανήκουν στο ανθρώπινο δυναμικό της εταιρίας ή είναι μέλη του πληρώματος του πλοίου, ώστε να σπάσουν τις διαδικασίες ασφαλείας που ακολουθεί η εταιρία για να τους παρασύρουν σε αποκάλυψη ευαίσθητων πληροφοριών.

Credential stuffing

Πρόκειται για την επίθεση στην οποία ο Hacker χρησιμοποιεί μεθόδους / πιστοποιητικά που έχει παραβιάσει στο παρελθόν ή συγκεκριμένους κοινούς κωδικούς πρόσβασης με σκοπό την απόπειρα μη εξουσιοδοτημένης πρόσβασης σε συστήματα του πλοίου. Η επίθεση χρησιμοποιεί bots για αυτοματοποίηση και κλίμακα και βασίζεται στην υπόθεση ότι πολλοί χρήστες επαναχρησιμοποιούν ονόματα χρήστη και κωδικούς πρόσβασης σε πολλές υπηρεσίες του πλοίου.

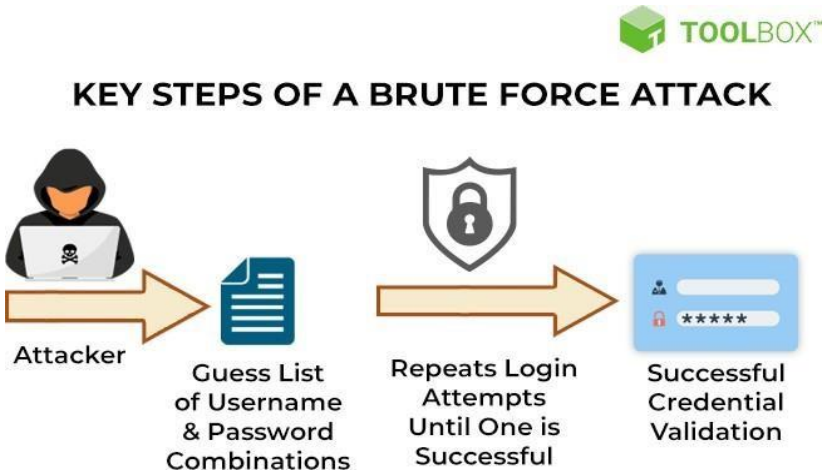
Brute force Attacks

Μπορούμε να αναφέρουμε 2 ορισμούς για αυτή την μέθοδο κυβερνοεπίθεσης.

Πρώτον, πρόκειται για επιθέσεις που προσπαθούν να βρουν κωδικούς πρόσβασης ή πιστοποιητικά με δοκιμαστικές μεθόδους. (Μέσα κοινωνικής δικτύωσης, κτλ).

Δεύτερον, η brute-force attack αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Δηλαδή αναφέρεται στην εξαντλητική δοκιμή απεριόριστων κλειδιών και κωδικών στα συστήματα επί του πλοίου με στόχο την διάρρηξη και την είσοδο των επιτιθέμενων σε αυτά. (Breach).

Είναι πολύ κοινή και επικίνδυνη μέθοδος καθώς δεν σταματάει μέχρι να βρεθεί το κλειδί ή ο κωδικός για την απόκτηση εισόδου. Παρακάτω, σχεδιαγραμματικά η επίθεση:



(Είκ.6 - ,παράδειγμα Brute Force Attack)

Μη Στοχευμένες επιθέσεις: Είναι οι επιθέσεις όπου τα συστήματα ενός πλοίου τυχαία γίνονται ο στόχος από τους hackers. Ο επιτιθέμενος συνήθως χρησιμοποιεί εργαλεία και τεχνικές που παρέχουν πληροφορίες για τους πιθανούς στόχους ανακαλύπτοντας τα ευάλωτα σημεία του πλοίου. Οι μέθοδοι επιθέσεων που χρησιμοποιούνται είναι:

Χρήση κακόβουλου λογισμικού *(malware)*

Το malware είναι κακόβουλο λογισμικό (malicious software) το οποίο έχει σχεδιαστεί με σκοπό την πρόσβαση αλλά και την πρόκληση βλάβης σε ένα ή περισσότερα υπολογιστικά συστήματα ενός πλοίου χωρίς την γνώση και άδεια του χρήστη. Υπάρχουν διάφοροι τύποι κακόβουλου λογισμικού όπως:

Α) Δούρειοι ίπποι *(Trojans)*: Είναι μια μορφή κακόβουλου λογισμικού που προσποιείται ότι είναι χρήσιμο ή αξιόπιστο πρόγραμμα, αλλά στην πραγματικότητα, κρύβει κάποιο κακόβουλο κώδικα. Μπορούν να εισέλθουν στα υπολογιστικά συστήματα πολύ εύκολα καθώς μοιάζουν σαν αληθινά αξιόπιστα προγράμματα.

Όταν ένας δούρειος ίππος εκτελείται σε έναν υπολογιστή, μπορεί να κάνει διάφορα κακόβουλα πράγματα, όπως την κλοπή προσωπικών πληροφοριών, την κατασκοπεία, την καταστροφή αρχείων, ή ακόμη και να παρακολουθεί τις δραστηριότητες του χρήστη ή του πλοίου χωρίς την γνώση του. Οι Δούρειοι ίπποι συχνά διακινούνται μέσω ψεύτικων email, μολυσμένων ιστοσελίδων, ή μέσω κοινωνικής μηχανικής για να πείσουν το χρήστη να τους εκτελέσει.

Β) Ιοί (viruses): Οι ιοί στον υπολογιστή είναι ένα κακόβουλο λογισμικό που μολύνουν τον υπολογιστή και του προκαλούν μεγάλη ζημιά. Αυτά τα κακόβουλα προγράμματα αναπαράγονται και εξαπλώνονται, εισβάλλοντας σε άλλα αρχεία ή προγράμματα και μπορούν να προξενήσουν πολλαπλά προβλήματα στον υπολογιστή.

Οι ιοί μπορούν να διαγράψουν οριστικά χρήσιμα αρχεία ή να καταστρέψουν δεδομένα, να κλέψουν προσωπικές πληροφορίες των εταιρειών, να καταστήσουν αδύνατη την λειτουργία

του υπολογιστή ή να προκαλέσουν προβλήματα στην λειτουργία του λογισμικού στο πλοίο. Συνήθως, οι ιοί μολύνουν τον υπολογιστή μέσω υποκρυπτικών τρόπων, όπως κακόβουλα email, ιστοσελίδες, ή φορητές συσκευές.

Γ) (ransomware): Το ransomware είναι ένας τύπος κακόβουλου λογισμικού στον κυβερνοχώρο, γνωστός και ως "λογισμικό λύτρων". Αυτό το κακόβουλο πρόγραμμα κρυπτογραφεί τα αρχεία του χρήστη και τα κλειδώνει, εμποδίζοντας τον πρόσβαση σε αυτά. Στη συνέχεια, οι δράστες του ransomware απαιτούν καταβολή λύτρων από το θύμα προκειμένου να παράσχουν το κλειδί ή την αποκρυπτογράφηση των αρχείων.

Τα υπολογιστικά συστήματα του πλοίου μπορεί να μολυνθούν από ransomware μέσω κακόβουλων email, μολυσμένων συνδέσμων, ή μέσω τρωτών σημείων στο λογισμικό τους. Όταν ένας υπολογιστής μολύνεται από ransomware, οι επιτιθέμενοι ζητούν τον πληρωμή ενός ποσού λυτρών για να αποκρυπτογραφήσουν τα αρχεία και να επαναφέρουν την πρόσβαση του χρήστη σε αυτά.

Το ransomware αποτελεί σοβαρή απειλή για τους χρήστες και τις ναυτιλιακές επιχειρήσεις, καθώς μπορεί να προκαλέσει σημαντική απώλεια δεδομένων και οικονομική ζημιά.

Δ) (spyware): Το spyware είναι ένα είδος κακόβουλου λογισμικού στον κυβερνοχώρο, το οποίο εγκαθίσταται στον υπολογιστή χωρίς την άδεια του χρήστη και συλλέγει πληροφορίες για αυτόν, χωρίς να το γνωρίζει. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν τα προγράμματα που χρησιμοποιεί, το ιστορικό περιήγησης στο διαδίκτυο, τα προσωπικά του στοιχεία και άλλες ευαίσθητες πληροφορίες.

Το spyware μπορεί να εγκατασταθεί στον υπολογιστή μέσω υποκρυπτικών τρόπων, όπως κακόβουλα email, μολυσμένων ιστοσελίδων, ή μέσω κοινωνικής μηχανικής. Οι δράστες του spyware χρησιμοποιούν αυτές τις πληροφορίες για να παρακολουθούν τις δραστηριότητες του χρήστη, να προβούν σε κλοπή ταυτότητας, να προσαρμόσουν τη διαφήμιση ή να προβούν σε άλλες παράνομες δραστηριότητες.

Ε) Botnet: Ένα botnet είναι μια συλλογή υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό και διαχειρίζονται από εγκληματίες, οι οποίοι ονομάζονται μερικές φορές "botmasters" ή "bot herders", για να πραγματοποιούν επιθέσεις ή να προκαλούν ζημιά. Ο όρος "botnet" (ρομποτικό δίκτυο) χρησιμοποιείται για να περιγράψει μια ομάδα μολυσμένων υπολογιστών που συχνά δημιουργούνται χωρίς τη συνείδηση των χρηστών.

Οι επιτιθέμενοι χρησιμοποιούν αυτούς τους υπολογιστές, που καλούνται περιστασιακά "bots" ή "zombies", για να πραγματοποιήσουν μαζικές επιθέσεις, όπως επιθέσεις Διανομής Αρνητικής Υπηρεσίας (DDoS), διανομή ανεπιθύμητων email (spam) και κλοπή ταυτότητας. Για να σχεδιάσουν τις επιθέσεις τους και να αποφύγουν την ανίχνευση, οι επιτιθέμενοι συνήθως διατάσσουν τα μέλη του botnet από απομακρυσμένους υπολογιστές.

Τα botnet αποτελούν σοβαρό κίνδυνο για την κυβερνοασφάλεια, καθώς μπορούν να πραγματοποιήσουν ευρείες επιθέσεις και να προκαλέσουν σοβαρές ζημιές σε συστήματα και δίκτυα.

Ζ) Worms (σκουλήκια): Συνήθως αυτοαντιγράφονται και εξαπλώνονται ανεξάρτητα από τον χρήστη. Τα worms μπορούν να δημιουργήσουν πολλά προβλήματα στα συστήματά του υπολογιστή.

Watering hole

Με βάση αυτές τις μορφές των επιθέσεων, ο Hacker γνωρίζει ή ανακαλύπτει ιστοσελίδες τις οποίες επισκέπτεται ο χρήστης και στη συνέχεια εγκαθιστά κακόβουλο λογισμικό σε αυτές. Δεν είναι συχνές επιθέσεις, ειδικά στον τομέα της ναυτιλίας γι’ αυτόν το λόγο δεν ανιχνεύονται εύκολα.

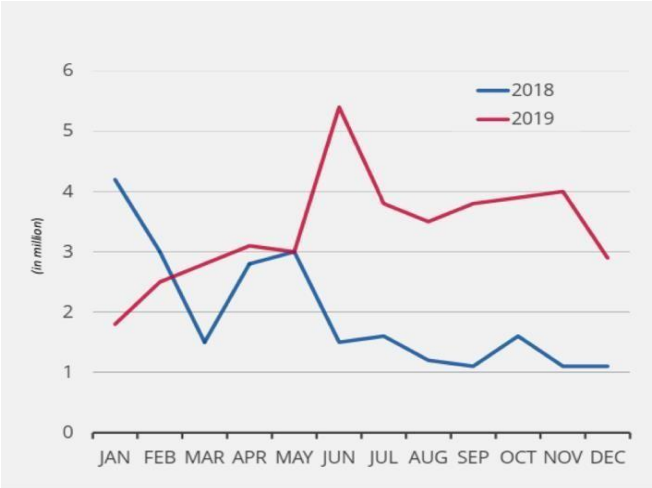
Διαρροή Πληροφοριών (Information Leakage)

Η διαρροή πληροφοριών (information leakage) είναι η φανέρωση, απόκτηση ή διαρροή ευαίσθητων ή προσωπικών πληροφοριών μιας ναυτιλιακής εταιρείας που θα έπρεπε να παραμείνουν απόρρητες ή εμπιστευτικές. Αυτή η διαρροή μπορεί να συμβεί κατά λάθος ή με σκόπιμη πρόθεση και μπορεί να αποτελέσει σοβαρό πρόβλημα για την ασφάλεια και την ιδιωτικότητα των ατόμων ή των οργανισμών που εμπλέκονται.

Οι πληροφορίες που διαρρέουν μπορεί να περιλαμβάνουν προσωπικά δεδομένα, όπως ονόματα, διευθύνσεις, αριθμούς κοινωνικής ασφάλισης, τραπεζικά στοιχεία, κωδικούς πρόσβασης, ιατρικά αρχεία, επιχειρηματικά μυστικά κ.λπ. Οι διαρροές πληροφοριών μπορεί να προκαλέσουν ανεπιθύμητες συνέπειες, όπως κλοπή ταυτότητας, απάτες, επιθέσεις κυβερνοασφάλειας ή κατάχρηση ευαίσθητων πληροφοριών για εμπορικούς σκοπούς.

Crypto Jacking

Είναι η μη εξουσιοδοτημένη χρήση κάποιων πόρων μιας συσκευής για την εξόρυξη κρυπτονομισμάτων. Περιλαμβάνουν οποιαδήποτε συνδεδεμένη συσκευή, όπως υπολογιστές και κινητά τηλέφωνα.



(Είκ.7 - Γράφημα κυβερνοεπιθέσεων ανα μήνα τα έτη 2018,2019)

2.3 Στάδια Κυβερνοεπίθεσης

Η προετοιμασία μιας επίθεσης στον κυβερνοχώρο από έναν επιτιθέμενο Hacker, απαιτεί χρόνο και προετοιμασία λόγω της ασφάλειας και ανθεκτικότητας των τεχνικών ελέγχων κινδύνου στον κυβερνοχώρο που υλοποιούνται από την εταιρεία στην στεριά, αλλά και εκείνων που γίνονται και υλοποιούνται στα πλοία της. Ως στάδια μιας Κυβερνοεπίθεσης μπορούν να αναφερθούν τα ακόλουθα:

Α) Προετοιμασία - Παρακολούθηση: Ο Hacker για αρκετό καιρό συλλέγει πληροφορίες και δεδομένα χρησιμοποιώντας τα ελεύθερα κοινωνικά δίκτυα των μελών του πληρώματος επί του πλοίου αλλά και των υπαλλήλων της εταιρείας. Στο πλαίσιο της προετοιμασίας για την υποψήφια κυβερνοεπίθεση ο Hacker παρακολουθεί κρυφά συζητήσεις στο διαδίκτυο, όπως σε forums και καταγράφει πληροφορίες για τεχνικά ζητήματα και για διαδικασίες ρουτίνας του πλοίου. Επίσης αναζητά έγγραφα και δεδομένα του πλοίου που περιγράφουν είτε σχέδιατου πλοίου είτε πληροφορίες για το φορτίο που μεταφέρει και στη συνέχεια τα μελετεί με σκοπό να ανακαλύψει τα ευάλωτα σημεία του πλοίου ή της εταιρείας.

Β) Παραβίαση: Ο Hacker αφού έχει εντοπίσει τα τρωτά σημεία στο δίκτυο είτε του πλοίου είτε της εταιρείας, επιτίθεται μέσω των τύπων/μορφών επιθέσεων που αναφέραμε προηγουμένως, *Phishing, Brute Force, Spear Phising,* είτε *Spyware,* με στόχο την υποκλοπή δεδομένων ή κωδικών κατά τη διαδικασία αναβάθμισης συστημάτων του πλοίου.

Γ) Έλεγχος: Είναι η κατάσταση όπου ο Hacker αφού έχει αποκτήσει πρόσβαση σε κάποιο από τα συστήματα του πλοίου, χρησιμοποιεί το παραβιασμένο σύστημα ή μέρος αυτού, με σκοπό την παραβίαση και άλλων συστημάτων του πλοίου ή αλλαγές που επηρεάζουν την ομαλή λειτουργία συστημάτων του, για να διακόψει ή να αλλάξει πληροφορίες σχετικά με την πλοήγησή του, να αποκτήσει πρόσβαση σε δεδομένα της εταιρείας καθώς και σε πληροφορίες για το φορτίο του πλοίου και το πλήρωμα.

2.4 Καταγραφή Κυβερνοεπιθέσεων

Οι τεχνολογίες OT (ναυτιλιακές), περιλαμβάνουν διάφορα συστήματα όπως:

- Ολοκληρωμένο σύστημα πλοήγησης πλοίων (ολοκληρωμένα συστήματα γέφυρας)
- Παγκόσμιο σύστημα εντοπισμού θέσεως
- Επικοινωνίες μέσω δορυφόρου. Είναι πολύ σημαντικές για τις επικοινωνίες μεγάλων αποστάσεων. Συγκριτικά είναι πολύ καλύτερες από τις κανονικές παλιές σταθερές ραδιοεπικοινωνίες επειδή έχουν την δυνατότητα να στέλνουν και να λαμβάνουν πληροφορίες μέσω του διαστήματος, χρησιμοποιώντας δορυφόρους που βρίσκονται σε τροχιά γύρω από τη Γη. Μεταφέρουν μεγάλο όγκο δεδομένων σταθερά και αναλλοίωτα. Τέλος, χρησιμοποιούνται σε παγκόσμια συστήματα εντοπισμού θέσης, πρόσβαση στο Διαδίκτυο, κτλ.
- AIS: Οι πληροφορίες του AIS μπορούν να εμφανίζονται σε ηλεκτρονικούς χάρτες πλοήγησης, διευκολύνοντας την αναγνώριση και παρακολούθηση των πλοίων. Το Automatic Identification System (AIS), γνωστό και ως σύστημα αναγνώρισης και

παρακολούθησης πλοίου, χρησιμοποιεί δορυφόρους για την επικοινωνία και μεταφορά δεδομένων σχετικά με την ταχύτητα, τη θέση και την πορεία του πλοίου. Το AIS είναι απαραίτητο σε κάθε πλοίο για πλοήγηση, αποφυγή σύγκρουσης, και γενικά για την θαλάσσια ασφάλεια. Όποιο πλοίο έχει τοποθετημένο το σύστημα AIS, χρησιμοποιεί τη συχνότητα VHF. Αυτή η συχνότητα χρησιμοποιείται για την αποστολή πληροφοριών σε άλλα πλοία, στις αρχές και στα συστήματα ξηράς. Τέλος, χρησιμεύει στους ηλεκτρονικούς χάρτες πλοήγησης, γεγονός που βελτιώνει την κατάσταση και την παρακολούθηση του πλοίου.

- Τα συστήματα ραντάρ και οι ηλεκτρονικοί χάρτες. Το ARPA και το ECDIS είναι προηγμένες τεχνολογίες που χρησιμοποιούνται σε αυτά.

Ας δούμε τώρα μερικές από τις καταγραφές κυβερνοεπιθέσεων που έκδηλωθεί:

- *MAERSK, 2017*

Ένας ιός με όνομα NotPetya, εισχώρησε στα συστήματά της, στην Ουκρανία, στις 27 Ιουνίου 2017, μολύνοντας κάθε σύστημα υπολογιστών της εταιρείας παγκοσμίως. Αργότερα αποκαλύφθηκε ότι μέλη του προσωπικού είχαν ανοίξει έναν σύνδεσμο απο μια μη εξουσιοδοτημένη ηλεκτρονική αλληλογραφία (spam folders), που ήταν μια επίθεση Spear Phishing, χωρίς να το καταλάβουν και έτσι ο ιός εισέβαλε στο δίκτυο της εταιρείας. Η μόλυνση στη συνέχεια εξαπλώθηκε, επηρεάζοντας πάνω από 200.000 συστήματα σε 150 χώρες, προκαλώντας ζημιές ύψους δισεκατομμυρίων δολαρίων!

Επιπλέον, επηρεάστηκε το σύστημα παρακολούθησης ακτινοβολίας του πυρηνικού σταθμού του Τσερνομπίλ στην Ουκρανία και απενεργοποιήθηκε κατά τη διάρκεια της επίθεσης. Πολλά υπουργεία, οι τράπεζες και όλα τα συστήματα μετρό της Ουκρανίας επηρεάστηκαν επίσης. Λέγεται ότι ήταν η πιο καταστροφική κυβερνοεπίθεση που έγινε ποτέ. Η επίθεση σταμάτησε αμέσως μετά την πραγματοποίησή της, αλλά επέφερε τρομακτικές ζημιές ύψους δισεκατομμυρίων δολαρίων.

- *Κυβερνοεπίθεση σε πλατφόρμα εξόρυξης πετρελαίου- Μεξικό*

Το γεγονός συνέβη όταν άθελά του προσωπικό της πλατφόρμας κατέβασε περιεχόμενο από μια μη ασφαλή ιστοσελίδα (μέθοδος Phishing) και εγκατέστησε επικίνδυνο ιό (malware). Η μόλυνση αμέσως απενεργοποίησε τους δυναμικούς θραύστες της πλατφόρμας (dynamic positioning thrusters), με αποτέλεσμα να επέλθουν σοβαρές συνέπειες που επηρέασαν την κλίση και λειτουργία της πλατφόρμας και να οδηγήσουν, για λόγους ασφαλείας, στην διακοπή της λειτουργίας της.

- *Κυβερνοεπίθεση σε Λιμάνι- Αμβέρσα, 2013*

Στο χρονικό διάστημα 2011 – 2013, πραγματοποιήθηκε Κυβερνοεπίθεση στο λιμάνι της Αμβέρσας. Στόχος των επιτιθέμενων ήταν η απόκτηση πρόσβασης σε απομακρυσμένα δεδομένα των συστημάτων του λιμένα. Σκοπός τους ήταν να χρησιμοποιήσουν τα δεδομένα αυτά προκειμένου να εντοπίσουν και να ιδιωποιηθούν παρανόμως κρυμμένα ναρκωτικά σε containers που ήταν αποθηκευμένα στο λιμάνι. Η Κυβερνοεπίθεση έγινε αντιληπτή αμέσως μετά την εξαφάνιση των containers.

Κεφάλαιο 3. Τρωτά σημεία του πλοίου

Οι εταιρίες και τα πλοία έχουν συστήματα, τα περισσότερα των οποίων σε μία ενδεχόμενη Κυβερνοεπίθεση αν δεν έχουν ενημερωθεί και αξιολογηθεί και με ακρίβεια καθίστανται ευάλωτα για τον υποψήφιο επίδοξο Hacker, κάνοντας πιο εύκολο το έργο του. Το εκάστοτε τμήμα ασφαλείας κάθε εταιρείας πρέπει να είναι καλά προετοιμασμένο, ενημερωμένο και εξοπλισμένο για να διαχειρίζεται αποτελεσματικά πιθανές επιθέσεις από τους Hackers. Χρειάζεται να γίνει ποσοτικός προσδιορισμός καθώς και διαχείριση των κινδύνων τα οποία αποτελούν και είναι ουσιαστικής σημασίας για την αξιολόγηση της πιθανής ζημίας που μπορεί να προκαλέσει κάθε επίθεση. Αυτή η αξιολόγηση επιτρέπει την εφαρμογή αποτελεσματικών πρακτικών ασφαλείας για τον μετριασμό της εκάστοτε υποψήφιας απειλής.

Όπως αναφέραμε, με την αύξηση της τεχνολογίας οι συνεχείς απειλές στον κυβερνοχώρο για τη ναυτιλιακή βιομηχανία επισημαίνουν τη σημασία της προστασίας τόσο των συστημάτων πληροφορικής όσο και της επιχειρησιακής τεχνολογίας (OT) από τις πιθανές κυβερνοεπιθέσεις. Οι συνέπειες αυτών σε ένα λειτουργικό περιβάλλον μπορεί να είναι από μικρής εντάσεως έως και καταστροφικές, όπως κατάρρευση υποδομών, κίνδυνοι για τη δημόσια ασφάλεια, κίνδυνοι για το περιβάλλον, κτλ. Η συνεχής τάση για αύξηση της ψηφιακής συνδεσιμότητας των βιομηχανικών δικτύων τα καθιστά ευάλωτα σε απειλές στον κυβερνοχώρο, καθιστώντας απαραίτητη την προστασία τους.

3.1 Συστήματα του πλοίου που είναι ευάλωτα σε κυβερνοεπιθέσεις

Τα ακόλουθα συστήματα, που υπάρχουν στα πλοία, μπορεί να είναι ευάλωτα σε κυβερνοαπειλές. Αναλυτικότερα:

- Τα συστήματα της γέφυρας.
- Τα συστήματα διαχείρισης φορτίου.

- Τα συστήματα διαχείρισης μηχανημάτων
- Τα συστήματα ελέγχου προσβασιμότητας.
- Τα συστήματα για τη διαχείριση των επιβατών.
- Τα δημόσια ανοικτά κοινωνικά συστήματα για το όφελος των ταξιδιωτών.
- Τα συστήματα ασφαλείας και υγείας του πληρώματος.
- Τα συστήματα επικοινωνίας.

Τα Συστήματα των γεφυρών: Τα συστήματα γεφυρών καθίστανται ευάλωτα σε επιθέσεις από χάκερς, επειδή χρησιμοποιούν ψηφιακά συστήματα πλοήγησης που συνδέονται με τα συστήματα στεριάς.

Συστήματα διαχείρισης φορτίου: Τα συστήματα διαχείρισης φορτίου είναι εξίσου ευάλωτα επειδή αλληλεπιδρούν με ψηφιακά συστήματα εκτός του πλοίου και με συστήματα που βασίζονται στην ξηρά τα οποία παρακολουθούν πού βρίσκεται το πλοίο και τι φορτίο μεταφέρει.

Συστήματα ελέγχου προσβασιμότητας: Αυτά τα ηλεκτρονικά συστήματα έχουν σχεδιαστεί για να διασφαλίζουν την ασφάλεια και την προστασία των επιβατών περιορίζοντας την πρόσβαση σε οποιοδήποτε μέρος του πλοίου. Έχουν επίσης τη δυνατότητα να παρακολουθούν το πλοίο και να ενεργοποιούν τον συναγερμό ασφαλείας του οποιαδήποτε στιγμή.

Συστήματα διαχείρισης επιβατών και εξυπηρέτησης αυτών: Αυτά είναι ψηφιακά συστήματα που έχουν ως στόχο να διαχειρίζονται την επιβίβαση των επιβατών και τον έλεγχο πρόσβασης. Ψηφιακά συστήματα εξυπηρέτησης επιβατών, όπως WiFi, κινητά τηλέφωνα, κλπ., μπορεί να θέσουν σε κίνδυνο την κυβερνοασφάλεια του πλοίου.

Συστήματα για την ασφάλεια και υγεία του πληρώματος: Αυτά εξασφαλίζουν την ασφάλεια και την καλύτερη δυνατή διαβίωση του πληρώματος κατά τη διάρκεια του ταξιδιού στη θάλασσα.

Συστήματα επικοινωνίας: Περιλαμβάνουν τη χρήση VHF με την βοήθεια της ψηφιακής επιλεκτικής κλήσης (DSC), η οποία μεταδίδει ή λαμβάνει σήματα κινδύνου, επείγοντα μηνύματα, σήματα ασφαλείας, καθώς και μηνύματα προτεραιότητας.

3.2 Τα τρωτά σημεία του πλοίου

Τα συνηθέστερα τρωτά σημεία του πλοίου είναι:

- Μη αναβαθμισμένα ή παλαιότερης τεχνολογίας λειτουργικά συστήματα.
- Μη ενημερωμένο λογισμικό ή έλλειψη συστήματος προστασίας από ιούς ή κακόβουλο λογισμικό. (AntiVirus + Security).
- Η ανεπαρκής εκπαίδευση του προσωπικού ασφαλείας στην αντιμετώπιση των κυβερνοεπιθέσεων.
- Η μη επικαιροποιημένη και ελλιπής εκπαίδευση αντιμετώπισης περιστατικών κυβερνοασφάλειας
- Τα συστήματα του πλοίου που συνδέονται με τα συστήματα στην ακτή.
- Οι προεπιλεγμένοι λογαριασμοί διαχειριστή και οι κωδικοί πρόσβασης.

Μη αναβαθμισμένα ή παλαιότερης τεχνολογίας λειτουργικά συστήματα: Πρόκειται για παλαιότερης τεχνολογίας συστήματα του πλοίου μη αναβαθμισμένα ή ενημερωμένα έναντι ιών κτλ, με αποτέλεσμα να καθίστανται εύαλωτα σε πιθανές επιθέσεις hackers.

Μη ενημερωμένο λογισμικό ή έλλειψη συστήματος προστασίας από ιούς ή κακόβουλο λογισμικό. (AntiVirus + Security): Αφορά την προστασία του δικτύου και το τείχος προστασίας. Το πλήρωμα συνδέεται με ασφάλεια και σιγουριά και απαγορεύει την πρόσβαση των Hackers σε ευαίσθητα προσωπικά αρχεία. Το έξυπνο τείχος προστασίας παρακολουθεί όλη την κυκλοφορία δικτύου μεταξύ των συστημάτων του πλοίου και αναχαιτίζει τις κακόβουλες εισβολές.

<u>Κεφάλαιο 4</u>: Διεθνές νομοθετικό πλαίσιο για την Κυβερνοασφάλεια

4.1 Έρευνα

Η κατανόηση της ναυτιλιακής βιομηχανίας σχετικά με τις κυβερνοεπιθέσεις και τις πηγές τους είναι ακόμα σχετικά ανεπαρκής λόγω της συνεχούς αύξησης της τεχνολογίας, με αποτέλεσμα ολοένα και να αυξάνεται η πιθανότητα απειλής για την κυβερνοασφάλεια. Το ίδιο ισχύει και για την κατανόηση των κινδύνων αυτών. Ειδικότερα, επτά από τις δέκα κορυφαίες ναυτιλιακές εταιρείες μεταφοράς εμπορευματοκιβωτίων (Containers) στον κόσμο έχουν παραδεχτεί δημοσίως ότι είχαν υποστεί κάποιου είδους κυβερνοεπίθεσης.

Ο ναυτιλιακός κλάδος παραμένει ακόμα ευάλωτος σε υποψήφιες κυβερνοεπιθέσεις, παρά τις προόδους που έχουν σημειωθεί με τις κατευθυντήριες οδηγίες του Διεθνούς Ναυτιλιακού Οργανισμού (IMO). Η CyberOwl, που εξειδικεύεται στην κυβερνοασφάλεια στον ναυτιλιακό κλάδο, εξέδωσε μια έρευνα που έκανε μαζί με την Holman Fenwick Willan (HFW), μια ναυτιλιακή νομική εταιρεία, σχετικά με τα μέτρα προστασίας αλλά και τους συνεχείς αυξανόμενους κινδύνους που υπάρχουν.

Τα αποτελέσματα της έρευνας δείχνουν ότι το **3%** των κυβερνοεπιθέσεων στον ναυτιλιακό τομέα κατά τα προηγούμενα τρία χρόνια είχε ως αποτέλεσμα την καταβολή λύτρων. Τα λύτρα που καταβλήθηκαν κατά μέσο όρο ήταν περίπου 3,1 εκατομμύρια δολάρια. Συγκριτικά, η μέση ετήσια δαπάνη για την κυβερνοασφάλεια μιας μεσαίας ναυτιλιακής εταιρείας για το σύνολο του στόλου της το έτος 2021 δεν ξεπέρασε τις 100.000 δολάρια. Επιπλέον, το μέσο κόστος καταβολής λύτρων για τον έλεγχο του κυβερνοκινδύνου για την επηρεαζόμενη ναυτιλιακή εταιρεία ήταν μόλις 3 λεπτά για κάθε 1 δολάριο, ενώ για την προστασία κατά της φυσικής πειρατείας ήταν 524 δολάρια.

Η προσέγγιση του ναυτιλιακού κλάδου σε αυτούς τους κινδύνους, καθώς και η διαχείριση θεμάτων κυβερνοασφάλειας σε ναυτιλιακούς οργανισμούς και στην ευρύτερη αλυσίδα εφοδιασμού, αποδείχθηκε ότι είχε σημαντικά κενά από την ερευνητική ομάδα.

Συνεχώς, η διεθνής ναυτιλιακή κοινότητα αναζητά κατευθυντήριες γραμμές και οδηγίες για τη ρύθμιση της ασφάλειας στον κυβερνοχώρο. Αυτά θα αποτελέσουν τη βάση των μελλοντικών συνθηκών για κάθε ναυτιλιακή. Ας δούμε παρακάτω μερικές από τις ισχύουσες ρυθμίσεις.

4.2 Ισχύουσες ρυθμίσεις

4.2.1 Εγκύκλιος I.M.O

Το 2017, η Επιτροπή Ασφαλείας του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) πραγματοποίησε αποφάσεις που περιελάμβαναν διαδικασίες διαχείρισης κινδύνων κυβερνοασφάλειας και ενέκρινε συστάσεις για τον έλεγχο των κινδύνων κυβερνοασφάλειας λαμβάνοντας υπόψη τις ευάλωτες πτυχές των πλοίων. Οι κανόνες της επιτροπής περιλαμβάνουν οδηγίες για την ασφάλεια του προσωπικού καθώς και διαδικασίες ασφαλείας υψηλού επιπέδου για την αντιμετώπιση των ενδεχόμενων κυβερνοεπιθέσεων. Η IMO δημιούργησε επίσης υψηλού επιπέδου κανόνες για να προστατεύσει το ναυτιλιακό κλάδο από υφιστάμενους και μελλοντικούς κινδύνους κυβερνοασφάλειας. Όπως υπογραμμίζεται στις συστάσεις της IMO, η αποτελεσματική διαχείριση κινδύνων κυβερνοασφάλειας πρέπει να ξεκινά από το ανώτατο επίπεδο διευθυντικών στελεχών των ναυτιλιακών επιχειρήσεων. Οι ανώτεροι ηγέτες πρέπει να προωθήσουν την ευαισθητοποίηση σχετικά με τα θέματα κυβερνοασφάλειας σε όλη την ναυτιλιακή εταιρεία καθώς και στα πλοία, και μετέπειτα προς τα κατώτερα επίπεδα-στελέχη. Έτσι όλοι θα γνωρίζουν για πως πρέπει να πράξουν σε περίπτωση μιας κυβερνοεπίθεσης.

4.2.2 Ο κώδικας I.S.M (International Safety Management Code)

Κατά την σύνοδο της Επιτροπής Ναυτιλιακής Ασφάλειας (Maritime Safety Committee - MSC) τον Ιούνιο του 2017, συμφωνήθηκαν και δημοσιεύτηκαν συγκεκριμένοι κανόνες για τη διαχείριση κινδύνων στον ναυτιλιακό κυβερνοχώρο υπό τον τίτλο MSC(98), στο Σύστημα Διαχείρισης Ασφαλείας (Safety Management System - SMS) του πλοίου. Ο Κώδικας Διεθνούς Διαχείρισης Ασφαλείας (International Safety Management - ISM) πρέπει να λαμβάνεται υπόψη στο εξουσιοδοτημένο SMS, το οποίο πρέπει επίσης να περιλαμβάει μια λίστα προληπτικών μέτρων.

Προκειμένου να μειωθεί η πιθανότητα κυβερνοεπιθέσεων, δόθηκαν επίσης οδηγίες σε όλους τους ναυτιλιακούς οργανισμούς κατά τη διάρκεια της συνεδρίασης σχετικά με την θέσπιση κανονισμών, πρωτοκόλλων και την κατάρτιση του προσωπικού τους. Ο ISM καθορίζει ότι κάθε ναυτιλιακή επιχείρηση πρέπει να αναπτύξει και να εφαρμόσει ένα SMS που περιλαμβάνει τις παρακάτω πληροφορίες:

1. Καθορισμός επιπέδων αρμοδιοτήτων, ρόλων και ευθυνών μεταξύ πλοίου και ξηράς.
2. Διαδικασίες αναφορών επιθέσεων και μη συμμόρφωση με τις διατάξεις του κώδικα.
3. Διαδικασίες αντιμετώπισης καταστάσεων έκτακτης ανάγκης.
4. Προσδιορισμός ευαίσθητων συστημάτων του πλοίου.
5. Την πολιτική προστασίας του περιβάλλοντος.

4.2.3 Ο κώδικας I.S.P.S (International Ship and Port Facility Security Code)

Ύστερα απο τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) εισήγαγε έναν παγκόσμιο κώδικα ασφαλείας που αφορά όλα τα πλοία και τα λιμάνια. Αυτός ο κώδικας ο οποίος αποτελεί μέρος της Διεθνούς Σύμβασης για την Ασφάλεια της Ζωής στη Θάλασσα (SOLAS), αποτελείται από δύο κατευθυντήριες παραγράφους, μία που είναι υποχρεωτική και μια προαιρετική. Ο συγκεκριμένος παγκόσμιος κώδικας τέθηκε σε ισχύ την1η Ιουλίου 2004.

Ο κώδικας είχε ως πρωταρχικό στόχο την διασφάλιση ακεραιότητας και της ασφάλειας των πλοίων και των λιμενικών εγκαταστάσεων, η οποία είναι εφικτό να επιτευχθεί μέσω μιας ολοκληρωμένης προσέγγισης διαχείρισης κινδύνου καθορίζοντας τα αναγκαία μέτρα ασφαλείας αλλά και ταυτόχρονη διεξοδική αξιολόγηση των κινδύνων.

Ο στόχος του Κώδικα είναι να παρέχει στην αξιολόγηση κινδύνου ένα ομοιόμορφο, συνεκτικό πλαίσιο που θα επιτρέψει στις κυβερνήσεις να αντισταθμίσουν τις αλλαγές στον κίνδυνο με τροποποιήσεις στην ευπάθεια των πλοίων και των λιμενικών εγκαταστάσεων. Προκειμένου να επιτευχθούν στόχοι όπως η δημιουργία ενός διεθνούς πλαισίου συνεργασίας ανάμεσα στις τοπικές αρχές, τις κυβερνήσεις και τις κυβερνητικές υπηρεσίες με τις εταιρείες ναυτιλίας και λιμένων, πρέπει να προσδιοριστούν κατάλληλα επίπεδα ασφάλειας και να ληφθούν αντίστοιχα μέτρα ασφαλείας. Ο στόχος είναι να αντιμετωπιστούν κίνδυνοι που μπορεί να απειλήσουν την ασφάλεια των πλοίων και των λιμενικών υποδομών και να διευκολυνθεί η ασφαλής ανταλλαγή πληροφοριών σχετικά με αυτήν την ασφάλεια.

Τα επίπεδα ασφαλείας που θέσπισε ο κώδικας αφορούν τα πλοία και είναι 3:

- Επίπεδο ασφαλείας 1: Εφαρμογή ελάχιστων κατάλληλων μέτρων προστασίας
- Επίπεδο ασφαλείας 2: Εφαρμογή πρόσθετων κατάλληλων μέτρων προστασίας για ορισμένο χρονικό διάστημα λόγω ενός περιστατικού ασφαλείας
- Επίπεδο ασφαλείας 3: Εφαρμογή ειδικών μέτρων προστασίας όταν ένα πιθανό περιστατικό αναμένεται να διαρκέσει μόνο για λίγο χρονικό διάστημα.

1ο επίπεδο ασφάλειας

Οι διαδικασίες συχνά αφορούν στην επικύρωση της ταυτότητας όλων όσων εισέρχονται στο πλοίο και τον λόγο εισόδου τους, καθώς και τον καθορισμό των σημείων πρόσβασης που πρέπει να κλειδωθούν για να μην επιτρέπεται η είσοδος.

2ο επιπεδο ασφάλειας

Για να αποτραπεί η παράνομη είσοδος, ακολουθούνται όλα τα προαναφερθέντα πρωτόκολλα (επίπεδο ασφάλειας 1) και λαμβάνονται πρόσθετες προφυλάξεις, όπως ορισμός επιπλέον μελών πληρώματος για την παρακολούθηση του καταστρώματος και των απαγορευμένων ζωνών. Σε όλο το πλήρωμα δίνονται επίσης πρόσθετες οδηγίες ασφαλείας και είναι υπεύθυνο για τη συνοδεία των καλεσμένων καθώς και την ασφάλειά τους.

3ο επίπεδο ασφάλειας

Σε αυτό το επίπεδο, αυστηρά μόνο άτομα που εμπλέκονται στη διαχείριση περιστατικών θα έχουν πρόσβαση στο πλοίο. Η επιβίβαση και η αποβίβαση θα σταματήσει για ορισμένο χρονικό διάστημα και το πλοίο μπορεί να χρειαστεί να εκκενωθεί ή να μετακινηθεί.

Αξιολόγηση ασφαλείας και σχέδιο ασφάλειας λιμενικής εγκατάστασης

Σε κάθε λιμενική εγκατάσταση, θα αξιολογούνται οι πιθανοί κίνδυνοι και οι απειλές για τα περιουσιακά στοιχεία και τις υποδομές και θα λαμβάνονται τα κατάλληλα μέτρα ασφαλείας. Το σχέδιο ασφαλείας των λιμενικών εγκαταστάσεων θα καθορίζει προφυλάξεις και θα περιλαμβάνει μέτρα πρόληψης πρόσβασης στις λιμενικές εγκαταστάσεις ή στα πλοία, επικίνδυνα υλικά, όπως πυροβόλα όπλα, τοξικές χημικές ουσίες, ραδιενεργά απόβλητα, κτλ. Τέλος, περιλαμβάνει μέτρα για περιορισμό της πρόσβασης σε ορισμένες περιοχές των λιμενικών εγκαταστάσεων για τα μη εξουσιοδοτημένα άτομα.

SSP

Σύμφωνα με τον κώδικα *I.S.P.S* πρέπει να δημιουργηθεί ένα σχέδιο ασφαλείας πλοίου *(SSP)* που αφορά την ασφάλειά του. Το σχέδιο ασφάλειας του πλοίου (SSP) περιέχει πληροφορίες σχετικά με:

1) Λεπτομέρειες σχετικά με το πλοίο και τον διαχειριστή του

2) την Πολιτική ασφαλείας

Στην πολιτική ασφαλείας περιγράφονται τα πρωτόκολλα και οι διαδικασίες που πρέπει να ακολουθούνται για την προστασία ευαίσθητων πληροφοριών για να μην υπάρξει διαρροή και την αποτροπή μη εξουσιοδοτημένης πρόσβασης από τρίτους. Περιλαμβάνεται επίσης ένα σχέδιο αντιμετώπισης συμβάντων, το οποίο περιγράφει λεπτομερώς τα βήματα που πρέπει να ληφθούν σε περίπτωση παραβίασης ασφάλειας ή παραβίασης δεδομένων. Όλο το πλήρωμα του πλοίου υποχρεούνται να υποβληθεί σε εκπαίδευση σχετικά με την πολιτική ασφαλείας και να υπογράψει συμφωνία εμπιστευτικότητας. Η πολιτική επανεξετάζεται και ενημερώνεται τακτικά για την αντιμετώπιση νέων απειλών. Η συμμόρφωση με την πολιτική ασφαλείας είναι υποχρεωτική και η μη τήρησή της μπορεί να οδηγήσει σε πειθαρχικά μέτρα.

3) Σημεία πρόσβασης στο πλοίο

4) Έλεγχος πρόσληψης πληρωμάτων και ταυτοποίηση προσώπων/επισκεπτών.

5) Ο εξοπλισμός ασφαλείας

Είναι σημαντικό να δίνεται πάντα προτεραιότητα στην ασφάλεια του πληρώματος φορώντας τον κατάλληλο εξοπλισμό για οποιαδήποτε εργασία, όπως κράνη, γάντια και προστατευτικά γυαλιά. Ο εξοπλισμός ασφαλείας είναι ζωτικής σημασίας για την προστασία από πιθανά ατυχήματα και τραυματισμούς.

6) Επικοινωνίες

7) Οι περιοχές περιορισμένης πρόσβασης

Αφορά τα τμήματα του πλοίου που έχουν περιορισμούς σχετικά με το ποιος έχει εξουσιοδότηση να εισέλθει και ποιες εργασίες μπορούν να γίνουν. Ο σκοπός του περιορισμού της πρόσβασης είναι η προστασία ευαίσθητων πληροφοριών, πολύτιμων περιουσιακών στοιχείων και η επίτευξη της ασφάλειας των ατόμων.

8) Οι διαδικασίες έκτακτης ανάγκης

Αφορά διαδικασίες και μέτρα έκτακτης ανάγκης, που αφορούν φυσική καταστροφή (Πυρκαγιά, τρικυμία, κτλ) είτε επείγουσα ιατρική ανάγκη, καθώς και κάθε ανθρωπογενή καταστροφή. Όταν εμφανίζεται μια έκτακτη ανάγκη, το πρώτο πράγμα που πρέπει να κάνει το πλήρωμα είναι η αξιολόγηση της κατάστασης και ο προσδιορισμός της σοβαρότητας της απειλής και τέλος η αντιμετώπισή της.

Αξιολόγησης της ασφάλειας του πλοίου (Ship Security Assessment –SSA)

Κατά την αξιολόγηση ασφάλειας του πλοίου προσδιορίζονται τα υπάρχοντα συστήματα ασφάλειας και επικοινωνίας του σκάφους, καθώς και τα κρίσιμα σημεία εισόδου και εξόδου για το πλήρωμα, τους επιβάτες, το φορτίο, καθώς και τις οδούς διαφυγής έκτακτης ανάγκης. Στη συνέχεια εξηγούνται τα χαρακτηριστικά οποιουδήποτε πρόσθετου εξοπλισμού ασφαλείας που θα μπορούσε να χρειαστεί επί του σκάφους και περιγράφεται ο σχεδιασμός του σχεδίου έκτακτης ανάγκης.

Επιθεώρηση

Παρουσιάζονται οι διαδικασίες επιθεώρησης πλοίου από την διαχειρίστρια εταιρία στα θέματα ασφάλειας και περιγράφονται οι τρόποι σχετικής εκπαίδευσης του πληρώματος.

4.2.4 The General Data Protection Regulation (GDPR)

Τον Μάιο του 2016, εγκρίθηκε από την ΕΕ το πακέτο προστασίας προσωπικών δεδομένων GDPR το οποίο έχει σαν στόχο το <<πέρασμα>> της Ευρώπης στην ψηφιακή εποχή ενισχύοντας ταυτόχρονα τα θεμελιώδη δικαιώματα των ατόμων.

Ο κανονισμός αυτός αναφέρεται στην πλήρη προστασία των προσωπικών δεδομένων όλων των πολιτών της ΕΕ διευκολύνοντας παράλληλα την επιχειρηματική δραστηριότητα για την ναυτιλία και για άλλους φορείς.

Ο κανονισμός αυτός ίσχυε από 24 Μαΐου του 2016 αλλά τελικώς εφαρμόστηκε στις 25 Μαΐου του 2018, και αφορά όλους τους φορείς που εμπλέκονται στη διαχείριση, επεξεργασία, αποθήκευση και διακίνηση δεδομένων προσωπικού χαρακτήρα, είτε πρόκειται για ιδιωτικές είτε δημόσιες επιχειρήσεις, είτε για κρατικές αρχές, κτλ. Η μη συμμόρφωση με τον παραπάνω κανονισμό έχει ως αποτέλεσμα την επιβολή κυρώσεων και προστίμων στις επιχειρήσεις. Δηλαδή αν προκύψει μια διαρροή προσωπικού χαρακτήρα πληροφοριών των πολιτών τα πρόστιμα που μπορούν να δεχτούν αυτές οι επιχειρήσεις φτάνουν έως και τα 1.000.000 ευρώ.

4.2.5 Ο ρόλος της Ε.Ε για την ασφάλεια στη θάλασσα

Ένα ποσοστό 40% του εσωτερικού εμπορίου της ΕΕ και ένα 90% του εξερχόμενου εμπορίου της ΕΕ διεξάγονται δια θαλάσσης. Αυτό σημαίνει ότι είναι απαραίτητη η προστασία και η ασφάλεια των θαλασσών και των ωκεανών κατά τις θαλάσσιες μεταφορές. Έτσι η ΕΕ θέσπισε το λεγόμενο σχέδιο δράσης για τη στρατηγική της που αφορά τη θαλάσσια ασφάλεια η αλλιώς EUMSS.

Βασιζόμενη σε μια σειρά υφιστάμενων εργαλείων και πολιτικών, όπως η Κοινή Πολιτική Ασφάλειας και Άμυνας και το Μέσο Συμβολής στη Σταθερότητα και την Ειρήνη, η ΕΕ αναλαμβάνει δράση μέσω του EUMSS για την προώθηση της διεθνούς συνεργασίας και του κράτους δικαίου στον θαλάσσιο τομέα. Αυτό περιλαμβάνει την ενεργή υποστήριξη της ασφάλειας και της διατήρησης ασφαλών των θαλασσών και των ωκεανών σε όλο τον κόσμο.

Ο EUMSS, υιοθετήθηκε από τα κράτη – μέλη της Ε.Ε τον Ιούνιο του 2014, με σκοπό να προωθήσει την προάσπιση των συμφερόντων της και την προστασία των κατοίκων και των κρατών μελών της.

Αυτό το σχέδιο αφορά στην αντιμετώπιση κινδύνων κατά των πλοίων στη θάλασσα, απειλών κατά της βιοποικιλότητας, παράνομης αλιείας, καθώς και περιβαλλοντικής ρύπανσης. Τελικά, η ΕΕ επιδιώκει:

1.) την επίτευξη άμυνας ενάντια σε υποψήφιες κυβερνοαπειλές στον κυβερνοχώρο.

2.)την μείωση του κυβερνοεγκλήματος.

3.)την ανάπτυξη μιας πολιτικής άμυνας στον κυβερνοχώρο.

4.)την ανάπτυξη βιομηχανικών και τεχνολογικών μέτρων για την Κυβερνοασφάλεια.

Κεφάλαιο 5: Μέτρα αντιμετώπισης κυβερνοεπιθέσεων

Οι δυνητικά καταστροφικές συνέπειες των κυβερνοεπιθέσεων στα πλοία και στις ναυτιλιακές εταιρείες μεταφορών είναι αναρίθμητες και σαφώς πρέπει να αντιμετωπιστούν αμέσως. Η ασφάλεια είναι πολύ σημαντική και καθίστανται ζωτικής σημασίας για κάθε ναυτιλιακό οργανισμό.

Πολλές φορές τα ατυχήματα λόγω των κυβερνοεπιθέσεων θέτουν τα πλοία σε κίνδυνο ή το περιβάλλον, όπως:

- Απειλή κατά της ζωής του πληρώματος.
- απώλεια φορτίου.
- ρύπανση της θάλασσας και του περιβάλλοντος γενικότερα.
- απώλεια επικοινωνίας με το γραφείο και τους ναυλωτές, με αποτέλεσμα τη διακοπή της λειτουργίας του πλοίου, ειδικά στη μεταφορά εμπορευματοκιβωτίων.

Έχουν αναπτυχθεί δύο βασικά μοντέλα για την αποτελεσματική αντιμετώπιση και την οριοθέτηση του κινδύνου. Αναλυτικότερα:

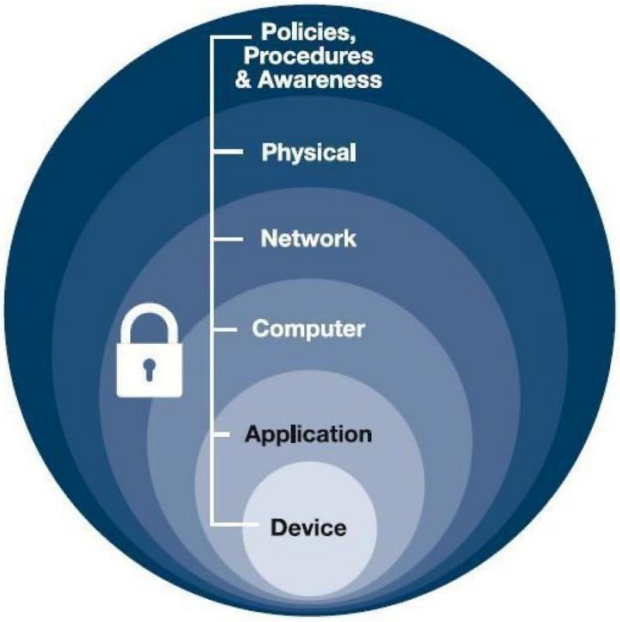
5.1 Άμυνα σε βάθος

Δεδομένης της ύπαρξης διάφορων απειλών στον κυβερνοχώρο, θα πρέπει να ληφθεί υπόψη μια στρατηγική «άμυνας σε βάθος». Κατά την στρατηγική αυτή εφαρμόζονται πολλαπλά επίπεδα ελέγχων ασφαλείας σε ένα σύστημα τεχνολογίας πληροφοριών ως μέρος της αρχής της ασφάλειας των πληροφοριών που είναι γνωστή ως

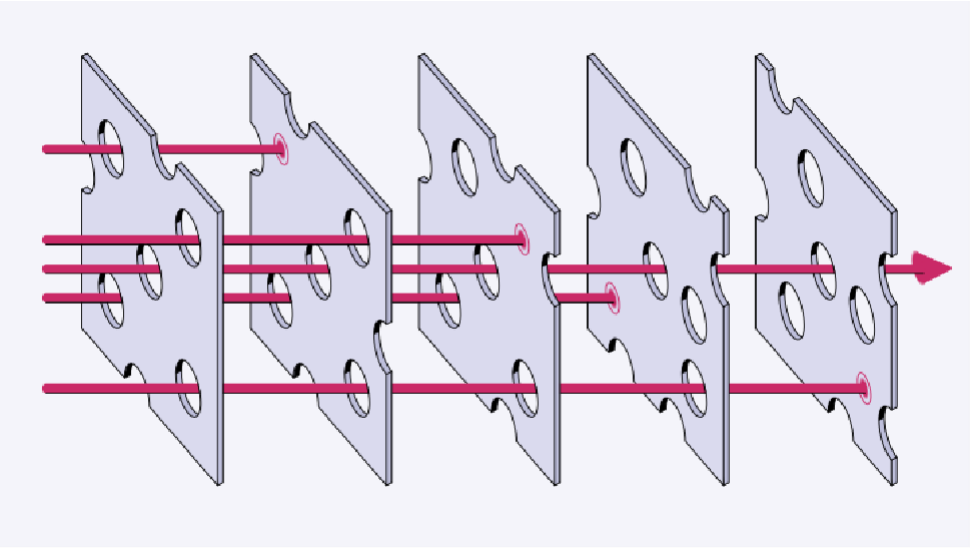
«άμυνα σε βάθος». Αυτή χρησιμοποιείται ως εφεδρικό σχέδιο σε περίπτωση που ένα μέτρο ασφαλείας αποτύχει ή βρεθεί μια ευπάθεια σε ένα από τα συστήματα (Τρωτά σημεία).

Το συγκεκριμένο σύστημα προστασίας περιλαμβάνει έναν συνδυασμό από πολλαπλά επίπεδα ελέγχων ασφαλείας τα οποία αναφέρονται παρακάτω:

- Η ύπαρξη του Συστήματος Ασφαλείας του Πλοίου *(SSP)*
- Αποτελεσματική προστασία των δικτύων
- Ανίχνευση πιθανής εισβολής
- Χρήση τείχους προστασίας (firewall)
- Περιοδικός έλεγχος των τρωτών σημείων του πλοίου
- Προστασία των συσκευών με την χρήση antivirus
- Έλεγχος πρόσβασης χρήστη
- Προστασία εφαρμογών με Data Backup
- Ενημέρωση και εκπαίδευση προσωπικού για τους κινδύνους από μια ενδεχόμενη κυβερνοεπίθεση



(Εικ.8 - Σχηματικά το μοντέλο <<άμυνα σε βάθος>>)



(Είκ.9 - Σχηματικά το πρότυπο <<άμυνα σε βάθος>>)

5.2 Άμυνα σε πλάτος

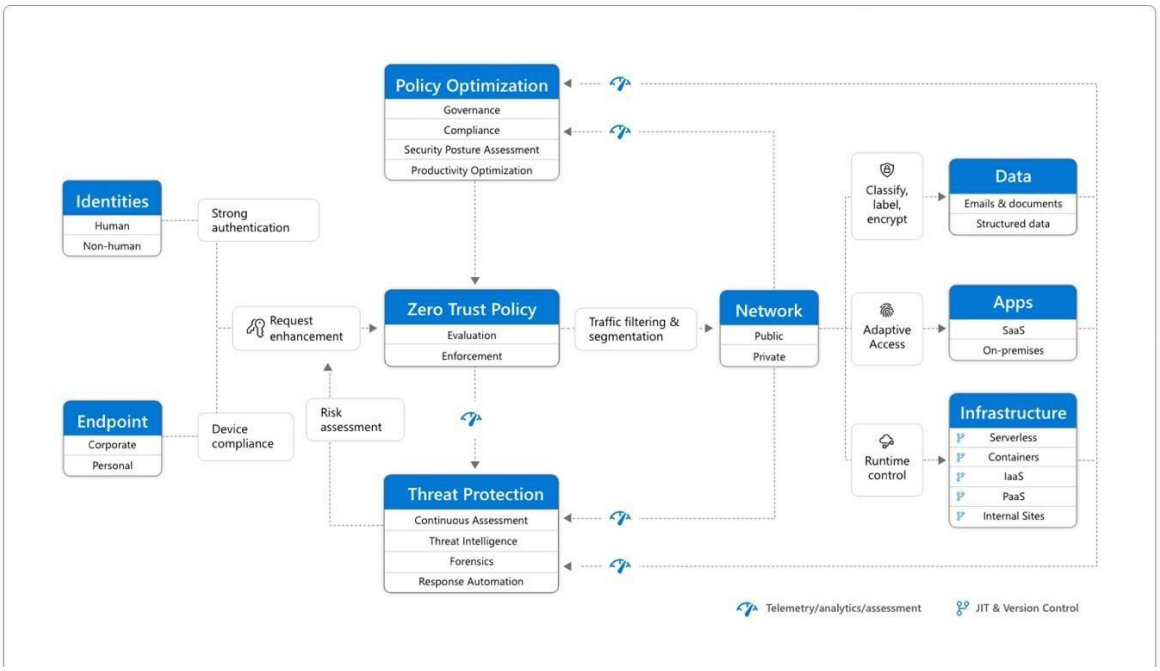
Η άμυνα σε πλάτος είναι μια στρατηγική κατά την οποία προκειμένου να αποφευχθεί η είσοδος κακόβουλων χρηστών, μέσω οποιασδήποτε ευπάθειας σε ένα σύστημα, εφαρμόζει διαδικαστικά και τεχνολογικά/τεχνικά μέτρα προστασίας σε διαφορετικά επίπεδα σε όλα τα τρωτά σημεία του πλοίου.

Μοντέλο μηδενικής εμπιστοσύνης άμυνας σε πλάτος

Οι οργανισμοί χρειάζονται μια νέα στρατηγική ασφάλειας σε αυτόν τον περίπλοκο σύγχρονο ψηφιακό κόσμο. Γενικότερα, στον ψηφιακό χώρο εργασίας θα πρέπει να είναι σε θέση να προσαρμόζονται αποτελεσματικά και να προστατεύουν τα άτομα, τις συσκευές, τις εφαρμογές και τα δεδομένα των ναυτιλιακών επιχειρήσεων. Η καλύτερη στρατηγική λοιπόν είναι η εφαρμογή της έννοιας της μηδενικής εμπιστοσύνης. Κατά αυτή, κάθε αίτημα αντιμετωπίζεται με την ίδια προσοχή σαν να προέρχεται από εξωτερικό δίκτυο, καθώς λειτουργεί υπό την προϋπόθεση ότι πρόκειται να συμβούν παραβιάσεις. Η μηδενική

εμπιστοσύνη βασίζεται στο αξίωμα «ποτέ μην εμπιστεύεσαι κανέναν και πάντα να επαληθεύεις».

Συνεπώς, πριν εκχωρηθεί πρόσβαση σε οποιαδήποτε αίτημα πρέπει να περάσει επιτυχώς αυστηρές διαδικασίες ελέγχου ταυτότητας, εξουσιοδότησης και κρυπτογράφησης, ανεξάρτητα από τον πόρο προέλευσης ή στόχου του. Τα δεδομένα και τα αναλυτικά στοιχεία που χρησιμοποιούνται για τον εντοπισμό και την αντιμετώπιση παρατυπιών σε πραγματικό χρόνο γίνεται με χρήση των αρχών μικροτμηματοποίησης. Παρακάτω σχεδιογραμματικά το μοντέλο:



(Εικ.10 – Το Μοντέλο μηδενικής εμπιστοσύνης)

5.3Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (CIA)

Η τριάδα ασφάλειας λογισμικού ή αλλιώς CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) είναι μια ταξινόμηση μορφής ασφάλειας που χρησιμοποιείται συχνά από τους οργανισμούς για να κατηγοριοποιήσει την ιδέα της κυβερνοασφάλειας. Παρόλα αυτά όμως, πιστεύεται ότι το τρίπτυχο της CIA στερείται ορισμένων πτυχών ασφάλειας λογισμικού. Παρά τα ελαττώματα της, η τριμερής ανάλυση της CIA είναι μια εξαιρετικά πολύτιμη τεχνική για την εξέταση πολλών θεμάτων που σχετίζονται με την ασφάλεια.

Οι όροι περιγράφονται γενικά ως εξής:

- *Εμπιστοσύνη* – Η προστασία των δεδομένων και τον πόρων από μη εξουσιοδοτημένη πρόσβαση.
- *Ακεραιότητα* – Αναφέρεται στην διασφάλιση της πληρότητας και της ακρίβειας των δεδομένων (Προστασία), από μη εξουσιοδοτημένες αλλαγές.
- *Διαθεσιμότητα* – Μόνο οι εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στα δεδομένα ή στους πόρους.

- Η **εμπιστευτικότητα**. Η κρυπτογράφηση ή ο περιορισμός της πρόσβασης σε μη κρυπτογραφημένη αποθήκευση δεδομένων αποτελούν το στάδιο της εμπιστευτικότητας. Με την κρυπτογράφηση διασφαλίζεται το απόρρητο.

- Η **ακεραιότητα** απαιτεί οι εξουσιοδοτημένοι χρήστες να έχουν εμπιστοσύνη στην ακρίβεια των δεδομένων. Τόσο οι μη εξουσιοδοτημένοι χρήστες όσο και οι εξουσιοδοτημένοι χρήστες δεν μπορούν να αλλάξουν κατά λάθος τα δεδομένα (για παράδειγμα, η προστασία κατά της τραπεζικής απάτης εμποδίζει την ανάληψη χρημάτων από έναν λογαριασμό και αφαιρεί τυχόν αποδεικτικά στοιχεία της ανάληψης).

- Η **διαθεσιμότητα**. Η διαθεσιμότητα των δεδομένων είναι ένας πολύ σημαντικός παράγοντας που συχνά παραβλέπεται σε πολλές περιπτώσεις. Τα δεδομένα δεν θα είναι πρακτικά χρήσιμα εάν οι εξουσιοδοτημένοι χρήστες δεν έχουν πρόσβαση σε αυτά. Πρόβλημα μη διάθεσης των δεδομένων προκύπτει εάν ένα κακόβουλο λογισμικό (malware) εισέλθει και διαγράψει ή κρυπτογραφήσει τα δεδομένα σε μια βάση, όπου διατηρείται το μόνο αντίγραφο των δεδομένων. Ένα άλλο χαρακτηριστικό της μη διάθεσης είναι η επίθεση κατανεμημένης άρνησης υπηρεσίας από χάκερ (DDoS Attacks) σε μια υπηρεσία που απαγορεύει στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε δεδομένα. Έτσι λοιπόν είναι εξίσου σημαντικό η διαθεσιμότητα των δεδομένων.

5.4 Αξιολόγηση του κινδύνου

Στον μεγάλο τομέα της κυβερνοασφάλειας, η κύρια εστίαση είναι στην αξιολόγηση και στον μετριασμό του «κινδύνου». Η αξιολόγηση του κινδύνου λοιπόν ποσοτικοποιείται από την εξίσωση A + T + V. Αναλυτικά τι σημαίνουν τα A, T και V:

Το A αντιπροσωπεύει κάτι που έχει αξία – συνήθως ένα περιουσιακό στοιχείο. Το T περιλαμβάνει όλους τους κινδύνους και τις απειλές και το V συμβολίζει ευπάθεια ή τα τρωτά σημεία του συστήματος. Αναλυτικότερα,

- **Στοιχείο:** Ένα στοιχείο μπορεί να είναι τα προσωπικά στοιχεία των χρηστών, κάποια δεδομένα, μια συσκευή ή ένα πολύτιμο μέρος ενός συστήματος, το οποίο παρέχει πρόσβαση σε ευαίσθητα δεδομένα.
- **Απειλή:** Οι κίνδυνοι και οι απειλές αναφέρονται στους κακόβουλους hacker, που προσπαθούν να παραβιάσουν τα συστήματα και έτσι τίθενται τα στοιχεία σε κίνδυνο.
- **Ευπάθεια:** Αναφέρεται σε ένα σφάλμα που έχει τη δυνατότητα να βλάψει, να καταστρέψει ή να υπονομεύσει ένα στοιχείο γνωστό ως ευπάθεια του συστήματος.

Μια ευπάθεια στα υπολογιστικά συστήματα είναι συνήθως ένα ελάττωμα ή ένα σφάλμα στον τρόπο με τον οποίο το πρόγραμμα εκθέτει ή επιτρέπει την πρόσβαση σε δεδομένα.

Σημειωτέων ότι η ευπάθεια δεν είναι απαραίτητα ένα ακούσιο ελάττωμα, αλλά μπορεί να είναι μια αδυναμία που δημιουργήθηκε εσκεμμένα, η οποία στους υπολογιστές ονομάζεται backdoor.

Τύποι ευπαθειών

Οι τύποι ευπαθειών ή αλλιώς τα τρωτά σημεία παρουσιάζονται σε μια ευρεία ποικιλία μορφών και καλύπτουν ένα ευρύ φάσμα στόχων και στρατηγικών καταπολέμησης. Μερικά παραδείγματα τρωτών σημείων είναι ο ατελής έλεγχος πρόσβασης, η κακή επεξεργασία δεδομένων εισόδου, η χρήση δεδομένων από μη εξουσιοδοτημένα άτομα, κτλ. Σύμφωνα με το πρότυπο ISO 27005, υπάρχει μια κατηγοριοποίηση των τρωτών σημείων ανά στοιχείο. Αναλυτικότερα:

- Υλικό

- Ευαισθησία στη σκόνη ή την υγρασία
- Έκθεση σε απροστάτευτη αποθήκευση
- Φθορά που σχετίζεται με τη γήρανση που προκαλεί υπερθέρμανση

- Λογισμικό

- Ανεπαρκής δοκιμή λογισμικού
- Αναξιόπιστη κωδικοποίηση
- Σφάλμα σχεδίασης Δικτύου
- Ανεπαρκής ιχνηλασιμότητα

- Δίκτυο

- Ανεπαρκώς προστατευμένα κανάλια επικοινωνίας (κακή ή καθόλου κρυπτογράφηση)

- Αναξιόπιστος σχεδιασμός δικτύου

 Προσωπικό

- Μη επαρκής διαδικασίες προσλήψεως προσωπικού
- Εσωτερικός κίνδυνος λόγω ανεπαρκούς συνείδησης ασφαλείας

 Φυσική τοποθεσία

- Περιοχές που επλήγησαν από φυσικές καταστροφές, όπως αυτές που επλήγησαν απόσεισμούς ή πλημμύρες
- Διακοπή παροχής ρεύματος

 Οργάνωση

- Μη χρήση τακτικών ανά διαστήματα ελέγχων
- Έλλειψη εφεδρικών σχεδίων
- Ανεπαρκής ασφάλεια

5.5 Αξιολόγηση Κινδύνου Από Την Εταιρεία

Η προσέγγιση της εκάστοτε ναυτιλιακής εταιρείας στην εκτίμηση κινδύνου ξεκινά με μια αξιολόγηση των συστημάτων του πλοίου για να προσδιοριστεί πόσο καλά είναι τεχνολογικά εξοπλισμένα για να χειριστούν τον όγκο των πιθανών απειλών στον κυβερνοχώρο. Η εταιρεία πρέπει να εκτιμήσει τα αποτελέσματα της αξιολόγησης κινδύνου του πλοίου καθώς και:

• Να εντοπίσει, να αξιολογήσει και να διορθώσει τις κρίσιμες λειτουργίες του πλοίου που είναι επιρρεπείς σε κυβερνοεπιθέσεις και

• Να ανιχνεύσει πιθανά περιστατικά στον κυβερνοχώρο και να τα εκτιμήσει στις κρίσιμες λειτουργίες του πλοίου.

5.6 Αξιολόγηση Κινδύνου Από Τρίτους

Στην αλυσίδα εφοδιασμού ενός ναυτιλιακού οργανισμού, η διαχείριση κινδύνων από τρίτους είναι αρκετά σημαντική διότι είναι σε θέση να αποκαλύψει γρήγορα τους κινδύνους στον κυβερνοχώρο, με αποτέλεσμα την στοχευμένη κατανομή πόρων και την ενισχυμένη συνεργασία με τους εταίρους, οδηγώντας τελικά σε σημαντική μείωση αυτών των κινδύνων.
Για να διασφαλιστεί ότι το επίπεδο άμυνας συμβιβάζεται με τη στρατηγική κυβερνοασφάλειας της εταιρείας, είναι επίσης δυνατή η διεξαγωγή δοκιμών διείσδυσης στην κρίσιμη υποδομή των Συστημάτων Πληροφορικής και Επιχειρησιακής Τεχνολογίας.

5.7 Διαχείριση Κινδύνου – Μέτρα τεχνικής προστασίας

Όσο μεγαλύτερη είναι μια ναυτιλιακή επιχείρηση τόσο μεγαλύτερο κίνδυνο παραβίασης της ασφάλειάς της αντιμετωπίζει σε αντίθεση με μια μικρότερη. Είναι λογικό, καθώς σε ένα περιβάλλον λόγω της αύξησης των συσκευών, του προσωπικού και των διαφόρων υποδομών απαιτείται ιδιαίτερος χειρισμός με βάση συγκεκριμένα τεχνολογικά μέτρα ασφαλείας για την αντιμετώπιση πιθανών απειλών στον κυβερνοχώρο. Παρακάτω περιγράφω αναλυτικά ορισμένα τεχνολογικά μέτρα ασφαλείας:

- **Χρήση καταλόγου συστημάτων λογισμικού και συσκευών που επιτρέπονται και που δεν επιτρέπονται**

  Προκειμένου να διασφαλιστεί ότι μόνο εξουσιοδοτημένο λογισμικό είναι εγκατεστημένο και ότι παρέχεται πρόσβαση μόνο σε εξουσιοδοτημένες συσκευές, οι επιχειρήσεις θα πρέπει να διαχειρίζονται και να παρακολουθούν ενεργά όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο καθώς και το λογισμικό που χρησιμοποιούν. Αυτό βοηθάει αρκετά στον γρήγορο εντοπισμό μη

εξουσιοδοτημένων συσκευών και στην αποσύνδεσή τους προτού προκαλέσουν οποιοδήποτε βλάβη. Οι Hackers σκανάρουν συνεχώς για νέα και απροστάτευτα σημεία εισόδου στο δίκτυο ή αναζητούν ευάλωτες εκδόσεις λογισμικού οι οποίες μπορεί να χρησιμοποιηθούν για να προκαλέσουν βλάβη.

- **Επανειλλημένη εκτίμηση των τρωτών σημείων και διόρθωσή τους**

Για να ανακαλύψουν και να διορθώσουν ευπάθειες που ενδέχεται να εκμεταλλευτούν οι χάκερ για να αποκτήσουν πρόσβαση στα δίκτυά τους, όλες οι επιχειρήσεις θα πρέπει συνεχώς να ελέγχουν, να αξιολογούν και να λαμβάνουν τα κατάλληλα μέτρα για τη λήψη νέων πληροφοριών, όπως ενημερώσεις λογισμικού, ενημερώσεις κώδικα, συμβουλές ασφαλείας κ.λπ. για την αποκατάσταση των τρωτών σημείων που θα μπορούσαν να χρησιμοποιήσουν οι Hackers για να διεισδύσουν στα δίκτυά τους.

- **Χρήση διαχειριστικών δικαιωμάτων**

Για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα συστήματα, όλες οι επιχειρήσεις θα πρέπει να χρησιμοποιούν αυτοματοποιημένες λύσεις για την παρακολούθηση της δραστηριότητας ατόμων με τα απαραίτητα δικαιώματα. Οι χάκερ προσπαθούν να παραβιάσουν ή να μαντέψουν τον κωδικό πρόσβασης για έναν χρήστη με πρόσβαση διαχειριστή χρησιμοποιώντας τη μέθοδο Brute Force Attack, τις τακτικές phishing ή άλλους τρόπους, όπως περιγράψαμε προηγουμένως.

- **Προστασία για τα email των επιχειρήσεων και των προγραμμάτων περιήγησης**

Για να μειωθεί η πιθανότητα κυβερνοεπίθεσης εναντίον τους, όλες οι επιχειρήσεις καλούνται να επιβεβαιώσουν την εγκυρότητα μόνο των προγραμμάτων περιήγησης που υποστηρίζονται πλήρως, καθώς και των εργαλείων διαχείρισης email. Λόγω του υψηλού επιπέδου τεχνολογικής πολυπλοκότητας και ευελιξίας τους, τα

προγράμματα περιήγησης ηλεκτρονικού ταχυδρομείου και διαδικτύου είναι δύο από τα πιο δημοφιλή σημεία εισόδου για τους χάκερ. Αυτό τους επιτρέπει να ξεγελούν τους χρήστες να ολοκληρώσουν δραστηριότητες που μπορεί να εισάγουν επιβλαβή κώδικα και να οδηγήσουν στην απώλεια σημαντικών δεδομένων.

- **Προστασία από κακόβουλο λογισμικό (malware)**

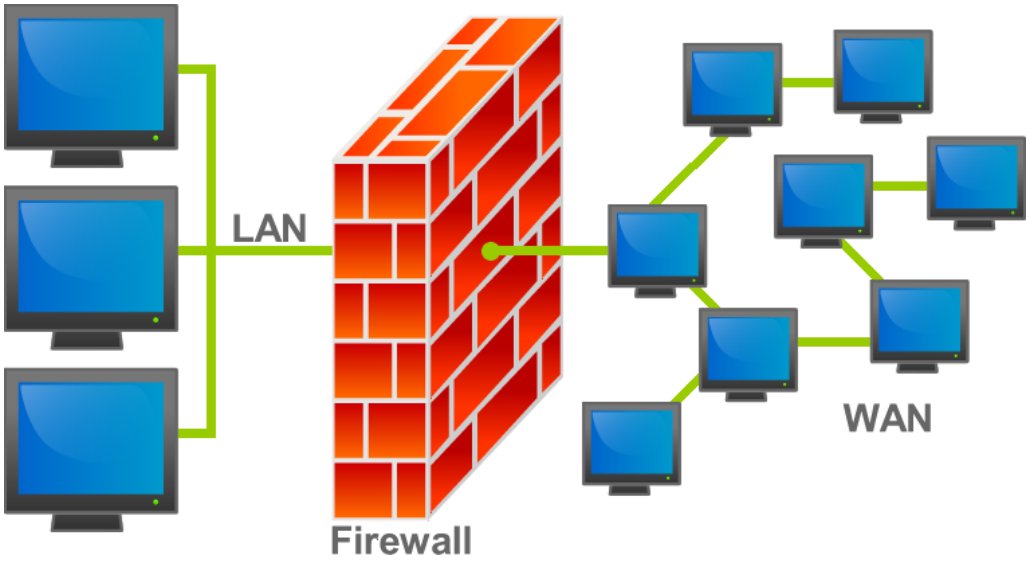
Οι εταιρείες πρέπει να κάνουν τακτικούς ελέγχους για κακόβουλα λογισμικά που μπορούν να επιφέρουν βλάβες μέσα στην επιχείρηση ή στο πλοίο με την βοήθεια χρήσης ***anti-virus, anti-spyware, firewalls*** και λειτουργίες ***host based IPS (HIPS)*** που βασίζονται σε κεντρικούς υπολογιστές.

Firewall

Ως τείχος προστασίας ή Firewall ονομάζεται μια συσκευή ή πρόγραμμα που έχει ρυθμιστεί για να εγκρίνει ή να απορρίπτει πακέτα δεδομένων που μετακινούνται από ένα δίκτυο υπολογιστών σε άλλο. Η κύρια δουλειά ενός τείχους προστασίας είναι να ελέγχει τη ροή δεδομένων μεταξύ δύο δικτύων υπολογιστών. Το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο είναι συνήθως αυτά τα δύο δίκτυα. Ανάμεσα σε δύο δίκτυα με διαφορετικά επίπεδα εμπιστοσύνης, μπαίνει ένα τείχος προστασίας.
Το εταιρικό ή οικιακό δίκτυο έχει το υψηλότερο επίπεδο εμπιστοσύνης, ενώ το Διαδίκτυο έχει χαμηλό επίπεδο εμπιστοσύνης. Μια αποστρατιωτικοποιημένη ζώνη (DMZ) ή ένα περιμετρικό δίκτυο έχουν μέσο βαθμό εμπιστοσύνης. Η εγκατάσταση ενός τείχους προστασίας γίνεται για να χρησιμοποιηθεί ώς άμυνα και να σταματήσει επιθέσεις στο τοπικό δίκτυο. Ένα τείχος προστασίας, ωστόσο, μπορεί να καταλήξει να είναι αναποτελεσματικό εάν δεν έχει ρυθμιστεί σωστά.
Το τείχος προστασίας θα πρέπει να ρυθμιστεί ώστε να απορρίπτει όλες τις συνδέσεις εκτός από αυτές που έχει εξουσιοδοτήσει ο διαχειριστής του δικτύου (προεπιλογή-άρνηση). Ο διαχειριστής δικτύου πρέπει να είναι γνώστης των δικτύων υπολογιστών και να έχει πλήρη κατανόηση των απαιτήσεων του δικτύου προκειμένου να ρυθμίσει σωστά ένα τείχος προστασίας. Δεδομένου ότι πολλοί διαχειριστές δεν διαθέτουν αυτά τα διαπιστευτήρια, ορίζουν την προεπιλεγμένη

ρύθμιση-allow του τείχους προστασίας ώστε να δέχεται όλες τις συνδέσεις εκτός από αυτές που ο διαχειριστής απαγορεύει καθιστώντας το δίκτυο επιρρεπές σε επιθέσεις από εξωτερικούς χρήστες.

Υπάρχουν 3 επίπεδα ασφάλειας. Το block all incoming traffic, το οποίο είναι και το πιο ασφαλές αλλά ο διαχειριστής πρέπει να έχει αρκετές καλές γνώσεις δικτύου, το allow income but block outcome, μεσαίας επιπέδου ασφαλείας που έχουνε τα περισσότερα δίκτυα καθώς και το allow all, στο οποίο όλα τα εξωτερικά δεδομένα μπορούν να εισέλθουν χωρίς κανένα έλεγχο είτε είναι κακόβουλα είτε όχι. Συνιστάται ποτέ μην μπει αυτή η εντολή στο τείχος προστασίας.



(Εικ.11 - , Μοντέλο λειτουργίας Firewall)

Περιγραφή	Το Firewall είναι μία δικτυακή συσκευή ασφαλείας η οποία «φιλτράρει» όλη την εισερχόμενη και εξερχόμενη λειτουργία στο δίκτυο, βασιζόμενο στους προκαθορισμένους κανόνες
Αρχή Λειτουργίας	«Φιλτράρει» την κυκλοφορία στο δίκτυο με βάση τις διευθύνσεις IP και τον αριθμό των ports.
Λειτουργία Διαμόρφωσης	Λειτουργία επιπέδου 3 ή transparent mode
Τοποθέτηση	Στην inline περίμετρο του δικτύου
Κυκλοφοριακοί patterns	Δεν έχουν αναλυθεί
Τοποθεσία σε σχέση με άλλες συσκευές	Είναι η πρώτη γραμμής άμυνας το firewall
Ενέργεια σε ανίχνευση μη εξουσιοδοτημένης κυκλοφορίας	«Μπλοκάρει» την κυκλοφορία
Σχετικές ορολογίες	• Σταθερό φίλτρο πακέτο • Επιτρέπει και «μπλοκάρει την κυκλοφορία

(Είκ.12 - , Χαρακτηριστικά του Firewall)

- **Περιορισμός και έλεγχος των πρωτοκόλλων και υπηρεσιών του Δικτύου**

  Για να μειωθούν τα παράθυρα ευπάθειας που είναι προσβάσιμα στους χάκερ οι οποίοι σαρώνουν εξ αποστάσεως για ελαττωματικές υπηρεσίες δικτύου που θα τους επιτρέψουν να εκμεταλλευτούν τα τρωτά σημεία, οι εταιρείες θα πρέπει να παρακολουθούν και να ρυθμίζουν τη χρήση πρωτοκόλλων και υπηρεσιών σε συσκευές δικτύου.

- **Data Backup**

  Επειδή οι χάκερ συχνά αλλάζουν δεδομένα όταν αποκτούν πρόσβαση στα εταιρικά δίκτυα, καταστρέφοντας ή διαγράφοντας πληροφορίες, οι εταιρείες θα πρέπει να διασφαλίζουν ότι δημιουργούνται τακτικά τα κατάλληλα αντίγραφα ασφαλείας.

- **Προστασία των δεδομένων**

  Η προστασία των δεδομένων επιτυγχάνεται καλύτερα μέσω τεχνικών μεθόδων κρυπτογράφησης ***(AES***,κτλ), για τον μετριασμό του κινδύνου διαφυγής- απώλειας δεδομένων και τη διασφάλιση της ακεραιότητας των ευαίσθητων πληροφοριών από πολλές διαρροές δεδομένων ύστερα από επιθέσεις Hackers.

- **Ελεγχόμενη πρόσβαση (Ασύρματη, κτλ)**

- **Έλεγχος ταυτότητας πολλών παραγόντων**

  Ένας χρήστης επαληθεύεται σε μια υπηρεσία χρησιμοποιώντας διάφορους παράγοντες, οι οποίοι είναι γνωστοί ως έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA). Αυτά τα στοιχεία περιλαμβάνουν συχνά ειδοποιήσεις push, κωδικούς πρόσβασης μίας χρήσης, κλειδιά ασφαλείας, μηνύματα SMS κ.λπ.

- **Καταλληλη εκπαίδευση**

  Κάθε εταιρεία θα πρέπει να προσδιορίζει τις ακριβείς πληροφορίες και οδηγίες που χρειάζονται οι υπάλληλοί της για τη βελτίωση της ασφάλειας, είτε μέσω επίσημης εκπαίδευσης ή σεμιναρίων σε θέματα ασφάλειας, είτε μέσω μιας στρατηγικής για τον εντοπισμό που αφορούν τα κενά ασφαλείας καθώς και την πλήρωσή τους με σχετικές πολιτικές και εκπαιδευτικές πρωτοβουλίες. Οι χάκερ κατασκευάζουν συχνά επιθέσεις που εκμεταλλεύονται το ανθρώπινο στοιχείο, όπως γράφοντας προσεκτικά μηνύματα ηλεκτρονικού "ψαρέματος" (phishing), τα οποία μοιάζουν με κανονικά μηνύματα ηλεκτρονικού ταχυδρομείου, το οποίο ο χρήστης της εταιρείας δεν καταλαβαίνει ότι είναι ψεύτικο με αποτέλεσμα την εισχώρηση του χάκερ.

- **Ασφάλεια λογισμικού εφαρμογών**

  Όλες οι εταιρείες θα πρέπει να ελέγχουν τακτικά ότι χρησιμοποιούν μόνο τις πιο πρόσφατες εκδόσεις και όχι παλαιότερες ή απαρχαιωμένες που αποσκοπούν στην διευκόλυνση των Κυβερνοεπιθέσεων.

- **Αντιμετώπιση και διαχείριση περιστατικών**

  Όλες οι επιχειρήσεις θα πρέπει να δημιουργήσουν και να εφαρμόσουν κατάλληλες διαδικασίες αντιμετώπισης περιστατικών, όπως σχέδια, ρόλοι κ.λπ., μέσω εκπαίδευσης, για την αντιμετώπιση μιας πιθανής επίθεσης στον κυβερνοχώρο.

- **Στρατηγικός σχεδιασμός**

  Είναι μια διαδικασία μιας επιχείρησης που αφορά στον καθορισμό λήψης αποφάσεων σχετικά με την κατανομή τον πόρων ασφαλείας, συμπεριλαμβανομένου του κεφαλαίου και των ανθρώπων. Κάθε ναυτιλιακή επιχείρηση περιέχει ένα στρατηγικό σχέδιο. Στρατηγικό σχέδιο είναι η στρατηγική της εκάστοτε εταιρείας για το που θέλει να φτάσει και να γνωρίζει πού κατευθύνεται. Στη συνέχεια αποφασίζει την διαδρομή για να φτάσει εκεί. Το αποκορύφωμα αυτής της διαδικασίας είναι ένα έγγραφο που αναφέρεται ως «στρατηγικό σχέδιο». Είναι αρκετά σημαντικό να υλοποιηθεί σωστά και με ακρίβεια επειδή οι Hackers μπορούν να εκμεταλλευτούν την ευπάθεια μεταξύ του σχεδιασμού άμυνας του οργανισμού και υλοποίησής του, όπως το χρονικό διάστημα μεταξύ της ανακοίνωσης ενός τρωτού σημείου και να επεμβούν σε αυτό.

5.8 Διαδικαστικά́ μέ́τρα προστασί́ας

Οι έλεγχοι διαδικασίας επικεντρώνονται στον τρόπο με τον οποίο τα μέλη του πληρώματος χρησιμοποιούν τα συστήματα επί του σκάφους. Οι σημαντικές και ευαίσθητες πληροφορίες πρέπει πάντα να διατηρούνται μυστικές και να αντιμετωπίζονται σύμφωνα με τα καθιερωμένα επιχειρηματικά πρότυπα στα σχέδια και τις διαδικασίες του πλοίου. Ακολουθούν ορισμένα παραδείγματα διαδικαστικών προφυλάξεων ασφαλείας με περισσότερες λεπτομέρειες:

- **Η Κατά́ρτιση / εκπαίδευση και η ευαισθητοποί́ηση του προσωπικού**

  Ένα από τα βασικά́ εργαλεί́α για την αποτελεσματική́ διαχεί́ριση και την αντιμετώ́πιση του κινδύ́νου στον κυβερνοχώ́ρο αποτελεί η εκπαίδευση και ευαισθητοποίηση του προσωπικού. Είναι σημαντικό να ληφθεί υπόψη ο αυξανόμενος κίνδυνος μιας νέας απειλής στον κυβερνοχώρο. Η εκπαίδευση και η ευαισθητοποίηση του προσωπικού είναι ζωτικής σημασίας για τη σωστή εκτέλεση και την αποφυγή διαφόρων λαθών, όπως η χρήση αφαιρούμενων μέσων USB για τη μεταφορά δεδομένων μεταξύ συστημάτων χωρίς να λαμβάνονται προφυλάξεις έναντι κακόβουλου λογισμικού. Επιπλέον, το προσωπικό της εταιρείας διαδραματίζει σημαντικό ρόλο στην προστασία των λειτουργικών συστημάτων και των συστημάτων πληροφορικής. Η επιχείρηση (το προσωπικό που βοηθά στη διαχείριση και τη λειτουργία του πλοίου) και οι υπάλληλοι του πλοίου, όπως ο πλοίαρχος και οι αξιωματικοί, θα πρέπει να παρέχουν εκπαίδευση και ευαισθητοποίηση του προσωπικού σε όλα τα επίπεδα ιεραρχίας. Ένα κατάλληλο πρό́γραμμα εκπαί́δευσης και ευαισθητοποί́ησης του προσωπικού θα πρέ́πει να καλύ́πτει τουλά́χιστον τις ακό́λουθες προδιαγραφέ́ς:

1. Οι κίνδυνοι των SPAM μηνυμάτων ηλεκτρονικού ταχυδρομείου και ο τρόπος χειρισμού τους, καθώς και η συζήτηση για πιθανές επιθέσεις στον κυβερνοχώρο, όπως το phishing (να μην κάνετε κλικ σε κακό ιστότοπο κ.λπ.).
2. Τα μέσα κοινωνικής δικτύωσης, τα φόρουμ συνομιλίας και οι διαδικασίες αποθήκευσης αρχείων που βασίζονται στο Google Cloud είναι όλα παραδείγματα

κινδύνων από τη χρήση του Διαδικτύου.

3. Οι προσωπικές συσκευές του προσωπικού (κινητά, υπολογιστής κ.λπ.) ενέχουν κινδύνους λόγω πιθανής έλλειψης μέτρων ασφαλείας, όπως απαρχαιωμένο λογισμικό ή ανεπαρκής προστασία από ιούς (μη χρήση antivirus). Αυτοί οι κίνδυνοι μπορούν να μεταφερθούν στο περιβάλλον του πλοίου.
4. Η χρήση μολυσμένου υλικού στα εταιρικά συστήματα για την εγκατάσταση και τη συντήρηση του λογισμικού μέσω αφαιρούμενων μέσων USB.
5. Όταν το μη εταιρικό προσωπικό όπως οι τεχνικοί κτλ, αφήνονται να εργάζονται στον εξοπλισμό του πλοίου χωρίς την κατάλληλη επίβλεψη, επιφέρει πιθανότητα για κινδύνους.
6. Οι διαδικασίες για την αποτροπή κινδύνων που προκύπτουν κατά τη διάρκεια παραβίασης του υπολογιστή ή του συστήματος όπως: ξαφνικές αλλαγές στο διαθέσιμο χώρο στο δίσκο ή στη μνήμη, απροσδόκητα σφάλματα προγράμματος, συχνές διακοπές λειτουργίας συστήματος, συστήματα/υπολογιστές που δεν ανταποκρίνονται ή αργούν, αλλαγές κωδικού πρόσβασης και μηνύματα ηλεκτρονικού ταχυδρομείου που επιστρέφονται απροσδόκητα ή με ύποπτο χαρακτήρα.
7. Προστασία των πληροφοριών του χρήστη και των κωδικών πρόσβασης όλου του προσωπικού ξεχωριστά.
8. Εφαρμογή σχετικών ρουτινών προληπτικού χαρακτήρα όπως πχ, σάρωση για εύρεση κακόβουλου λογισμικού στα συστήματα με χρήση antivirus.

- **Πρόσβαση για τους επισκέπτες**

Η χρήση υπολογιστών κατά τη διάρκεια του πλοίου θα πρέπει να απαγορεύεται για όλους τους επισκέπτες, συμπεριλαμβανομένων των αρχών, των υπαλλήλων λιμένων και τερματικών σταθμών και εκπροσώπων ιδιοκτητών/μελών. Το δίκτυο του πλοίου θα πρέπει να απαγορεύει τη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητους υπολογιστές Λειτουργικών Συστημάτων Τεχνολογίας. Η πρόσβαση στο δίκτυο επισκεπτών θα πρέπει να οργανώνεται σύμφωνα με τις πολιτικές που ορίζονται από την εταιρεία ή τον χειριστή του πλοίου. Θα πρέπει να χρησιμοποιείται υπολογιστής του χρήστη και μόνον σε μέρη εξουσιοδότησης (Δημόσιο δίκτυο). Τέλος, για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης

θα πρέπει να αποτρέπεται η χρήση αφαιρούμενων μέσων ***USB***.

- **Αναβάθμιση και συντήρηση λογισμικού**

  Μετά από κάποιο χρονικό διάστημα, η υποστήριξη του κατασκευαστή για όλα τα συστήματα πλοίων και τους τύπους λογισμικού που απαιτούν ενημερώσεις λήγει και, ως εκ τούτου, δεν τους παρέχονται πλέον οι απαραίτητες ενημερώσεις κώδικα και αναβαθμίσεις για την αντιμετώπιση τυχόν ευπάθειας. Ο κάθε οργανισμός θα πρέπει να εξετάσει προσεκτικά με τη χρήση της τεχνολογίας το λογισμικό ως μέρος της αξιολόγησης του κινδύνου στον κυβερνοχώρο. Για την έγκαιρη αναβάθμιση του υλικού και του λογισμικού θα πρέπει να δημιουργηθούν κάποιες διαδικασίες, λαμβάνοντας πάντα υπόψη το είδος του πλοίου, την ταχύτητα σύνδεσης στο διαδίκτυο, τη διάρκεια του θαλάσσιου ταξιδιού κ.λπ. Επιπλέον απαιτείται τακτική αναβάθμιση των τειχών προστασίας (firewalls), για την αποτελεσματική αντιμετώπιση του κακόβουλου λογισμικού και ιών.

- **Ενημερώσεις εργαλείων Antivirus**

  Κάθε οργανισμός θα πρέπει να προβαίνει σε τακτικές ενημερώσεις των εργαλείων antivirus για την αποτροπή και αντιμετώπιση πιθανής εισόδου κακόβουλου λογισμικού στα υπολογιστικά συστήματα.

- **Λύσεις απομακρυσμένης πρόσβασης**

  Αφορά τη δημιουργία ορισμένων εξειδικευμένων πρωτοκόλλων για τη διαχείριση της απομακρυσμένης πρόσβασης στα λειτουργικά και πληροφοριακά συστήματα (IT/OT) που είναι ενσωματωμένα στο πλοίο. Μια κυβερνοεπίθεση στο συνδεδεμένο επιχειρησιακό περιβάλλον ενός πλοίου μπορεί να έχει καταστροφικές συνέπειες, θέτοντας σε κίνδυνο το περιβάλλον και την ασφάλεια του πληρώματος, εκτός από την καταστροφή ζωτικής σημασίας υποδομών και υπηρεσιών. Τα βιομηχανικά δίκτυα γίνονται όλο και πιο ψηφιακά συνδεδεμένα, γεγονός που τα εκθέτει σε κινδύνους στον κυβερνοχώρο και τονίζει την ανάγκη για ασφάλεια συστημάτων OT εκτός από τα συστήματα πληροφορικής.

- **Administration Only**

  Η πρόσβαση στα ευαίσθητα δεδομένα του πλοίου ή της επιχείρησης αναφέρεται μόνο στον καθορισμένο διαχειριστή (Admin Only). Στον διαχειριστή επιτρέπεται η πλήρης πρόσβαση στις ρυθμίσεις συστήματος και σε όλα τα δεδομένατου πλοίου. Εάν ένας χρήστης συνδεθεί στα συστήματα υπολογιστή του πλοίου με δικαιώματα διαχειριστή, μπορεί να επιτρέψει την εκμετάλλευση μιας ευπάθειας με αποτέλεσμα την εύκολη είσοδο των χάκερ σε αυτά. Ο ρόλος και τα προνόμια του διαχειριστή θα πρέπει να δίνονται μόνο σε κατάλληλα εκπαιδευμένο προσωπικό σε θέματα που σχετίζονται με την κυβερνοασφάλεια. Τέλος, για την προστασία της πρόσβασης σε πληροφορίες και δεδομένα του πλοίου θα πρέπει να αναπτυχθούν ισχυροί κωδικοί πρόσβασης σύνδεσης. Οι κωδικοί πρόσβασης πρέπει να αποτελούνται από σύμβολα, νούμερα αλλά και από αριθμούς και να αλλάζουν περιοδικά, αποτρέποντας έτσι τον υποψήφιο Hacker να μαντέψει τον κωδικό πρόσβασης μέσω *Brute Force Attack.*

- **Έλεγχοι σε φυσικά και αφαιρούμενα μέσα.**

  Ο κίνδυνος εισαγωγής ιού μέσω αφαιρούμενων μέσων USB θα πρέπει να λαμβάνεται σοβαρά υπόψη κατά τη μεταφορά δεδομένων από μη ελεγχόμενα συστήματα σε ελεγχόμενα συστήματα στο πλοίο. Θα πρέπει να υπάρχουν ορισμένα πρότυπα και διαδικασίες σχετικά με τη χρήση φορητών μέσων, όπως η ανάγκη να σαρωθεί από κακόβουλο λογισμικό από λογισμικό προστασίας από ιούς πριν εισαχθεί σε οποιοδήποτε από τα συστήματα του πλοίου.

- **Τεχνική υποστήριξη από τη στεριά**

  Τα πλοία θα πρέπει να έχουν πρόσβαση σε τεχνική υποστήριξη σε περίπτωση μιας ενδεχόμενης Κυβερνοεπίθεσης.

Κεφάλαιο 6. Αντιμετώπιση περιστατικών κυβερνοεπίθεσης

6.1 Αξιολόγηση κινδύνων και κατάρτιση Σχεδίου Αποτίμησης Επικινδυνότητας

Η επιτυχής αξιολόγηση και ο έλεγχος των απειλών/κινδύνων, αποτελεί ένα από τα σημαντικότερα θεμέλια για την ασφάλεια στον κυβερνοχώρο. Για το σκοπό αυτό είναι απαραίτητο να υπάρχει:

• Η δημιουργία ενός συγκεκριμένου πλαισίου στο οποίο οι επιχειρήσεις μπορούν να προσδιορίζουν τους πόρους πληροφοριών και τις επιχειρηματικές δραστηριότητες που είναι απαραίτητες για αυτές.

• Η θέσπιση ενός συγκεκριμένου πλαισίου στο οποίο οι επιχειρήσεις θα βασιστούν σε αυτό για την αναγνώριση των εσωτερικών και εξωτερικών μεταβλητών που ενδέχεται να επηρεάσουν την ασφάλεια των πόρων των πληροφοριών της επιχείρησης.

• Η δημιουργία μιας στρατηγικής για την αποτελεσματική αντιμετώπιση κινδύνων στον κυβερνοχώρο, με την ταυτόχρονη δημιουργία προφίλ των απειλών (Είδος απειλής, λόγος, αιτία, βαρύτητα, κτλ).

• Αξιολόγηση των τρωτών σημείων και των ευπαθειών που ενδέχεται να εκμεταλλευτούν οι χάκερ για κυβερνοεπιθέσεις, και την δημιουργία ενός σχεδίου έκτακτης ανάγκης.

Σχέδιο έκτακτης ανάγκης

Το σχέδιο Έκτακτης Ανάγκης θα περιλαμβάνει τα ακόλουθα:

- Ορισμούς (όπως αυτοί για τη διαχείριση κρίσεων).

  Θα περιλαμβάνονται όλοι οι ορισμοί που σχετίζονται με τη διαχείριση κρίσεων, έτσι ώστε να μπορεί να χρησιμοποιηθεί η ίδια γλώσσα και να δημιουργηθεί μια κοινή κατανόηση.

- Κριτήρια.

  Τα κριτήρια θα καθορίζουν πότε μια κατάσταση θα χαρακτηρίζεται ως απειλή ή απαιτεί την ενεργοποίηση του σχεδίου έκτακτης ανάγκης.

- Ρόλοι και αρμοδιότητες

  Θα περιλαμβάνει κανόνες στο ποιος κάνει τι με βάση την ιεραρχία. Στα ανώτερα επίπεδα θα υπόκειται προσωπικό αρκετά εκπαιδευμένο ώστε να είναι ικανό σε μια κατάσταση απειλής να συντονίσει σωστά και να μην μεταφέρει τον πανικό στα κατώτερα ιεραρχικά επίπεδα.

- Σχέδια αποκατάστασης από τις καταστροφές των κυβερνοεπιθέσεων και επιχειρηματικής συνέχειας.

  Θα περιλαμβάνει την καταγραφή πληροφοριών σχετικά με τις κυβερνοεπιθέσεις, με την ταυτόχρονη ανάπτυξη Σχεδίων Επιχειρησιακής Συνέχειας και Ανάκτησης αυτών και τέλος τα απαραίτητα μέτρα για την επανέναρξη των τακτικών λειτουργιών.

- Αξιολόγηση, ανάλυση και ανίχνευση κινδύνου/τρωτότητας.

  Θα περιλαμβάνει την αξιολόγηση, ανάλυση και την ανίχνευση τρωτών σημείων ή ευπαθειών και στην επίλυσή τους.

6.2 Λύσεις Έξυπνων Λιμανιών με 5G - Κυβερνοασφάλεια των δικτύων 5ης γενιάς

Η Ευρωπαϊκή Επιτροπή εξέδωσε την Πρόταση Αριθ. 2019 534 προς τα Κράτη Μέλη, τους αρμόδιους φορείς, τους οργανισμούς και άλλα όργανα της Ευρωπαϊκής Ένωσης, καθώς και την Ομάδα Συνεργασίας που έχει καθιερωθεί βάσει της Οδηγίας (ΕΕ) 2016 1148 (Ομάδα Συνεργασίας για την Ασφάλεια των Δικτύων και της Πληροφορίας), στο πλαίσιο της ευρωπαϊκής συντονισμένης συνεργασίας για τη διασφάλιση της κυβερνοασφάλειας των δικτύων 5ης γενιάς (5G). Σκοπός αυτής της πρωτοβουλίας είναι η χρήση έξυπνων λύσεων για τη βελτίωση της λειτουργίας των λιμένων και των συναφών υποδομών, με γνώμονα πάντοτε την ασφάλεια και προστασία του κυβερνοχώρου. Στην πρόταση αναφέρονται λύσεις με την βοήθεια της τεχνολογίας όπως:

6.2.1 Απομακρυσμένος έλεγχος των γερανών

Η νέα τεχνολογία της 5ης γενιάς θα μπορούσε να χρησιμοποιηθεί για την απομακρυσμένη λειτουργία γερανών σε λιμάνια εμπορευματοκιβωτίων, κάτι που θα μπορούσε να είναι πολύ επωφελές καθώς θα εξασφάλιζε διαχείριση σε πραγματικό χρόνο.

6.2.2 Επιτήρηση του χώρου με την χρήση καμερών

Η χρήση σύγχρονων τεχνολογιών της 5ης γενιάς μπορεί να χρησιμοποιηθεί για την επιτήρηση των χώρων με αποτέλεσμα την αύξηση της ασφάλειας. Οι κάμερες με τεχνητή νοημοσύνη στους γερανούς και η αυτόματη μέτρηση φορτίων μπορούν να χρησιμοποιηθούν για την εντοπισμό όλων των εμπορευματοκιβωτίων και έτσι στον διαμερισμό του φόρτου εργασίας. Επιπλέον, η παρακολούθηση του προσωπικού με βάση την τεχνολογία αναγνώρισης προσώπου θα επιτρέπει να διαπιστώνεται η συνεχής εργασιακή ικανότητα του προσωπικού κ.λπ. Ως αποτέλεσμα, οι λειτουργίες του λιμένα γίνονται ακόμη πιο άνετες και πιο εύκολες.

6.2.3 Πλοήγηση εξ αποστάσεως

Στην ναυτιλιακή βιομηχανία, με την χρήση τεχνολογίας 5ης γενιάς μπορούν να χρησιμοποιηθούν τα αυτόνομα ή αλλιώς αυτοματοποιημένα πλοία. Αυτά τα πλοία λειτουργούν χωρίς την ανάγκη ανθρώπινου πληρώματος, καθώς διαχειρίζονται και ελέγχονται εξ αποστάσεως από συστήματα στην στεριά. Υπάρχουν αρκετά πλεονεκτήματα στη χρήση μη επανδρωμένων πλοίων στη ναυτιλία, γεγονός που τονίζει την αξία τους. Η βελτίωση της ασφάλειας με την χρήση αυτόνομων πλοίων εκτοξεύεται στα ύψη αφού αφαιρεί την πιθανότητα ανθρώπινου λάθους, που μπορεί να προκαλέσει ατυχήματα.

6.3 Απώλειες που προκύπτουν από μια κυβερνοεπίθεση

Οι Κυβερνοεπιθέσεις, όπως προαναφέραμε μπορούν να προκαλέσουν σοβαρές και εκτεταμένες ζημιές ανεξάρτητα αν πρόκειται για ναυτιλιακές εταιρείες, είτε στα πλοία, είτε σε κυβερνητικούς οργανισμούς. Ας δούμε μερικές απώλειες που μπορούν να προκαλέσουν:

Χρηματοοικονομικές Απώλειες:

Ισχυρές κυβερνοεπιθέσεις μπορούν να προκαλέσουν τεράστιες οικονομικές ζημιές σε οργανισμούς και εταιρείες ή σε κυβερνητικά ιδρύματα, όπως απώλειες εσόδων, διαρροές εμπιστευτικών δεδομένων, κλοπές χρηματοπιστωτικών καρτών, κ.λπ.

Παραβίαση Προσωπικών Δεδομένων:

Οι συνέπειες των κυβερνοεπιθέσεων μπορούν να οδηγήσουν σε παραβίαση προσωπικών δεδομένων, προκαλώντας τη διαρροή προσωπικών πληροφοριών που μπορεί να χρησιμοποιηθούν για κλοπή ταυτότητας, απάτες, ή άλλες κακόβουλες δραστηριότητες.

Διακοπή Υπηρεσιών:

Διάφοροι τύποι κυβερνοεπιθέσεων είναι σε θέση να προκαλέσουν υπερφόρτωση διάφορων υπηρεσιών, ιστοσελίδων ή κάποιων δικτύων, προκαλώντας έτσι απώλεια εργασίας και παραγωγικότητας. (DDoS Attacks).

Καταστροφή Υποδομών:

Ισχυρές κυβερνοεπιθέσεις μπορούν να προκαλέσουν ζημιά σε ψηφιακές πλατφόρμες ή υποδομές και στα συστήματα ελέγχου, προκαλώντας μαζική καταστροφή και δυσκολία στην επαναφορά.

6.3.1 Καλύψεις για υλικές ζημιές

Όπως προαναφέραμε σε προηγούμενα κεφάλαια, υπάρχουν ήδη ασφαλιστήρια συμβόλαια και ρήτρες (A,B,C) που καλύπτουν όλους τους πιθανούς κλασικούς κινδύνους που μπορεί να προκύψουν σε ένα ταξίδι, όπως η προσάραξη, η σύγκρουση πλοίου, η πυρκαγιά, η απώλεια φορτίου λόγω καιρικών συνθηκών, κτλ, τα οποία είναι μερικά από τα γεγονότα που μπορούν να προκαλέσουν απώλειες ή ζημιές στο πλοίο και στον εξοπλισμό του. Πριν ξεκινήσει το πλοίο, είναι πολύ σημαντικό να υπάρχει ένα ασφαλιστήριο συμβόλαιο για την κάλυψη αυτών των πιθανών κινδύνων.

Όμως ζούμε σε μια ψηφιακή εποχή η οποία συνεχώς ολοένα και επεκτείνεται χάρη στην τεχνολογία, η χρήση της οποίας αποφέρει πολλά πλεονεκτήματα αλλά και ορισμένα μειονεκτήματα όπως η χρήση της για κακό σκοπό, καθιστώντας επομένως πολύ σημαντικό για τις εταιρείες να επαληθεύουν εκ των προτέρων με τους ασφαλιστές τους εάν το συμβόλαιό τους απορροφά και καλύπτει ζημιές και απώλειες από επιθέσεις στον κυβερνοχώρο. Ευτυχώς υπάρχουν σπάνια κενά/ρήτρες μη συμπερίληψης ασφαλιστικής κάλυψης για επιθέσεις που προέρχονται από τον Κυβερνοχώρο. Συνήθως στις περισσότερες εταιρείες καις τα πλοία τους υπάρχει κάλυψη απωλειών κυβερνοεπιθέσεων. Εάν όμως σε μια θαλάσσια πολιτική περιλαμβάνεται ρήτρα εξαίρεσης για επιθέσεις στον κυβερνοχώρο, η εταιρεία ενδέχεται να μην αποζημιωθεί για τυχόν προκύπτουσα απώλεια.

Επομένως, οι ασφαλιστές στη ναυτιλιακή βιομηχανία πρέπει να ρωτούν και να μαθαίνουν σχετικά με τις τακτικές μιας ναυτιλιακής εταιρείας για επιθέσεις στον κυβερνοχώρο, να εξοικειώνονται με τα πρότυπα του κλάδου και να πράττουν αναλόγως.

6.4 Ερωτήσεις αυτό – αξιολόγησης

Κάθε ναυτιλιακή εταιρεία θα πρέπει κάθε χρόνο να αυτό – αξιολογείται για την εύρεση και διόρθωση ευπαθειών στα υπολογιστικά της συστήματα και να στην υλοποίηση πιθανών σεναρίων μιας ενδεχόμενης κυβερνοεπίθεσης. Ενδεικτικές αυτό – ερωτήσεις είναι οι εξής:

- Είναι όλο το λειτουργικό σύστημα της εταιρείας Up to Date;
- Υπάρχουν κάποια σωστά πρωτόκολλα για την αντιμετώπιση των αλλαγών στο λογισμικό;
- Με ποιόν τρόπο αντιμετωπίζονται οι διορθώσεις ασφαλείας για το λογισμικό; Υπάρχει κάποια πολιτική για τη διαχείριση ενημερώσεων κώδικα;
- Οι κωδικοί πρόσβασης Admin και εξουσιοδοτημένων ατόμων χρησιμοποιούνται και ενημερώνονται ανάλογα με τις ανάγκες;
- Υπάρχουν τρόποι που να καθιστούν δυνατόν να εντοπιστούν παραβιάσεις και περιστατικά ασφάλειας στον κυβερνοχώρο;
- Είναι προσβάσιμα ανα πάσα στιγμή και καταγράφονται τα αρχεία ασφαλείας;
- Υπάρχει κάποια στρατηγική αντιμετώπισης πιθανών παραβιάσεων ασφαλείας;
- Οι κωδικοί πρόσβασης διαχειριστή Admin είναι μη προβλέψιμοι από επίθεση μέσω Brute – Force; Επίσης τα δικαιώματα του Admin έχουν περιορισμούς;
- Είναι ενεργή η προστασία του προγράμματος περιήγησης anti-theft και Fire Wall και του ηλεκτρονικού ταχυδρομείου Anti-spam;
- Δίνεται η δυνατότητα κρυπτογράφησης AES;
- Γίνεται τακτική σάρωση συσκευών αποθήκευσης USB στο εταιρικό δίκτυο για αποφυγή κάποιας εισόδου μολυσμένου αρχείου;
- Πώς γίνεται η οριστική διαγραφή δεδομένων από τα PDA που χρησιμοποιούν οι επιχειρήσεις;
- Ελέχγονται τακτικά και πού φυλάσσονται τα αντίγραφα ασφαλείας Security Backups; Τηρούνται οι μονάδες αποθήκευσης Data backups;

Κεφάλαιο 7. Συμπεράσματα

Η ψηφιακή εποχή που ζούμε με την συνεχώς αλματώδη αύξηση της τεχνολογίας έχει επιφέρει μοναδικές ευκαιρίες για συνδεσιμότητα, καινοτομία και πρόοδο, αλλά έχει επίσης αυξήσει την δυνατότητα σε δράστες να διαταράξουν, να κλέψουν και να προκαλέσουν ζημιές σε ευαίσθητες πληροφορίες και κρίσιμες υποδομές. Η ευρεία απειλή των κυβερνοεπιθέσεων και το συνεχώς μεταβαλλόμενο τοπίο της κυβερνοασφάλειας θέτουν σημαντικές προκλήσεις για άτομα, επιχειρήσεις και κυβερνητικούς παράγοντες σε όλο τον κόσμο. Η διπλωματική εργασία μου έχει εξετάσει διάφορες πτυχές των κυβερνοεπιθέσεων και της κυβερνοασφάλειας, καταλήγοντας στα εξής συμπεράσματα:

1) Οι επιθέσεις στον κυβερνοχώρο είναι ευρέως διαδεδομένες:

Στον ψηφιακό συνδεδεμένο κόσμο οι κυβερνοεπιθέσεις αποτελούν μόνιμη απειλή στον κυβερνοχώρο. Από καθημερινές μαζικές παραβιάσεις δεδομένων, επιθέσεις ransomware κατά εταιρειών, επιθέσεις spyware, παραβιάσεις ευαίσθητων προσωπικών πληροφοριών, επιθέσεις άρνησης υπηρεσιών έως απόπειρες phishing που στοχεύουν άτομα για απάτη, το φάσμα όλων αυτών των απειλών στον κυβερνοχώρο συνεχίζει να αυξάνεται. Αυτή η συνεχής ανάπτυξη κυβερνοεγκληματιών απαιτεί προσεκτικά μέτρα για την προστασία των ψηφιακών μας περιουσιακών στοιχείων.

2) Η σημασία της κυβερνοασφάλειας:

Υψίστης σημασίας είναι η εφαρμογή κάποιων ισχυρών μέτρων για την ασφάλεια στον κυβερνοχώρο. Είναι απαραίτητη στον ψηφιακό κόσμο μας η προστασία ευαίσθητων δεδομένων, η πνευματική ιδιοκτησία και η διασφάλιση της αδιάλειπτης λειτουργίας των κρίσιμων υπηρεσιών. Η κυβερνοασφάλεια δεν είναι ευθύνη μόνο ενός ή του τμήματος πληροφορικής, αλλά πρέπει να γίνει κοινή ευθύνη σε όλα τα επίπεδα της κοινωνίας και στον καθένα μα ξεχωριστά.
Στις επιχειρήσεις οι επιθέσεις αυτές προκαλούν τρομακτικές ζημιές και μπορούν να

προκαλέσουν οικονομικές απώλειες, υποβάθμιση της φήμης της εταιρείας, κτλ. Επομένως, όλοι ναυτιλιακοί οργανισμοί πρέπει να υιοθετήσουν κάποιες στρατηγικές ασφαλείας και να επενδύσουν σε τεχνολογίες που μπορούν να ανιχνεύσουν, προλάβουν και αντιμετωπίσουν αποτελεσματικά τις κυβερνοεπιθέσεις.

3) <u>Η συνεχής εξέλιξη της τεχνολογίας απαιτεί συνεχή προσαρμογή και ενίσχυση των μέτρων κυβερνοασφάλειας:</u>

Η συνεχής εξέλιξη της τεχνολογίας είναι ένα αρκετά σημαντικό πλεονέκτημα της σύγχρονης κοινωνίας όμως προκαλεί έντονες επιδράσεις στον τομέα της κυβερνοασφάλειας, καθιστώντας πολύ σημαντική την ανάγκη για συνεχή προσαρμογή και ενίσχυση των μέτρων κυβερνοασφάλειας.
Με την τεχνολογική εξέλιξη, οι κυβερνοεπιθέσεις γίνονται ολοένα και πιο εξεζητημένες και επικίνδυνες. Οι Hacker αναζητούν συνεχώς νέους τρόπους για να επιτύχουν πρόσβαση σε ευαίσθητα δεδομένα και σε ναυτιλιακά συστήματα.
Επιπλέον, η χρήση προηγμένων τεχνολογιών όπως το icloud, το Internet of Things (IoT) και το AI δημιουργούν ευνοικές καταστάσεις για κυβερνοεπιθέσεις.
Τέλος, οι νόμοι και οι κανονισμοί σχετικά με την κυβερνοασφάλεια πρέπει να αλλάζουν συνεχώς για να ανταποκριθούν στις νέες απειλές και τεχνολογίες. Οι επιχειρήσεις και οι κυβερνήσεις πρέπει να είναι σε συνεχή συμμόρφωση με αυτούς τους νόμους.

<u>Μελλοντικές προτάσεις</u>

1) <u>Ενίσχυση της διεθνούς συνεργασίας και της κοινοποίησης πληροφοριών για την αντιμετώπιση παγκόσμιων κυβερνοαπειλών:</u>

Για την αντιμετώπιση παγκόσμιων απειλών στον κυβερνοχώρο και την υποστήριξη της ασφάλειας και της σταθερότητας, η "ενίσχυση της διεθνούς συνεργασίας και της ανταλλαγής πληροφοριών" είναι ένα σύνολο μέτρων και πολιτικών που στοχεύουν στην

προώθηση του συντονισμού μεταξύ διαφορετικών χωρών και διεθνών οργανισμών.

Η κοινή χρήση στρατηγικών εχθρικών οργανισμών και ο συντονισμός μεταξύ ερευνητικών και επιχειρησιακών ομάδων είναι μόνο μερικά στοιχεία της παγκόσμιας συνεργασίας όσον αφορά τους κανονισμούς και τις οδηγίες για την ασφάλεια στον κυβερνοχώρο. Ο συνδυασμός πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο είναι επίσης μια κρίσιμη πτυχή αυτής της διαδικασίας.

Για την καταπολέμηση των απειλών στον κυβερνοχώρο, είναι ζωτικής σημασίας για τις χώρες και τους οργανισμούς να ανταλλάσσουν πληροφορίες, ώστε οι τρέχοντες κίνδυνοι να αναγνωρίζονται και να αντιμετωπίζονται κατάλληλα. Η πράξη της ανταλλαγής πληροφοριών είναι ζωτικής σημασίας για την αντιμετώπιση αυτών των απειλών.

2) <u>Ανάπτυξη προηγμένων τεχνολογιών ανίχνευσης και αποτροπής κυβερνοεπιθέσεων (5G):</u>

Η προστασία του δικτύου με τεχνολογίες 5G και η ασφάλεια στον κυβερνοχώρο είναι μια κρίσιμη πτυχή για τη διαφύλαξη των τηλεπικοινωνιακών υποδομών και την καταπολέμηση των επιθέσεων στον κυβερνοχώρο. Η εφαρμογή προηγμένων τεχνολογιών 5^{ης} γενιάς είναι μια αποτελεσματική προσέγγιση για την επίτευξη αυτού του στόχου. Με τις τεχνολογίες 5^{ης} γενιάς γίνεται έγκαιρος εντοπισμός κυβερνοεπιθέσεων και παραβιάσεων στα δίκτυα και στα συστήματα το οποίο αυτό επιτυγχάνεται με τη χρήση προηγμένων συστημάτων ανίχνευσης εισβολών και ανίχνευσης ανωμαλιών 5^{ης} γενιάς .

3) <u>Προώθηση και επένδυση έρευνας και καινοτομίας για την αντιμετώπιση των νέων κυβερνοαπειλών που εμφανίζονται χρησιμοποιώντας τεχνικά αλλά και διαδικαστικά μέτρα προστασίας</u>

4) Ενίσχυση της ευαισθητοποίησης του κοινού και εκπαίδευση του προσωπικού των οργανισμών σχετικά με τους κυβερνοκινδύνους και τα μέτρα προστασίας:

Η ενίσχυση της ευαισθητοποίησης του κοινού και η εκπαίδευση του προσωπικού των οργανισμών σχετικά με τις κυβερνοεπιθέσεις και τα μέτρα προστασίας είναι ζωτικής σημασίας για την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων. Παρακάτω παρουσιάζονται κάποια βήματα που μπορούν να ληφθούν για την επίτευξη αυτών:

Α) Εκπαίδευση προσωπικού: Η συνεχής εκπαίδευση για την ασφάλεια στον κυβερνοχώρο για το προσωπικό των ναυτιλιακών επιχειρήσεων ή του πληρώματος του πλοίου είναι ζωτικής σημασίας που αφορά την εκπαίδευσή τους σχετικά με τις πιο πρόσφατες απειλές και πρακτικές προστασίας. Πρέπει να δωθεί ιδιαίτερη έμφαση στην εκπαίδευση για να διασφαλίστει ότι το προσωπικό είναι έμπειρο στα βασικά θέματα της κυβερνοασφάλειας.

Β)Σεμινάρια: Πρέπει να οργανωθούν εκπαιδευτικά προγράμματα/σεμινάρια και εκδηλώσεις για την ενημέρωση του ευρύτερου κοινού σχετικά με τους κινδύνους στον κυβερνοχώρο και την πρόταση μέτρων προστασίας.

Γ)Ετοιμότητα: Οι πιθανές επιθέσεις στον κυβερνοχώρο πρέπει να αντιμετωπίζονται με ετοιμότητα. Κάθε οργανισμός πρέπει να αναπτύξει πρωτόκολλα και σχέδια δράσης για τον εντοπισμό κρίσιμων πληροφοριών και συστημάτων για την ασφάλεια.

Τέλος, ο έγκαιρος εντοπισμός απειλών στον κυβερνοχώρο μπορεί να ενισχυθεί με την επένδυση σε τεχνολογίες παρακολούθησης και ανίχνευσης (όπως αναφέραμε πρηγουμένως π.χ 5G). Αυτό θα οδηγήσει σε αύξηση της ασφάλειας και στην αποτροπή επιθέσεων.

Βιβλιογραφία

Ελληνική

- Γεδεών Σαββίνα- Εφραιμία, (2021), *Κυβερνοασφάλεια στη ναυτιλία- εφαρμογή σχετικών κανονισμών σε πλοίο,* Πανεπιστήμιο Δυτικής Αττικής, Σχολή μηχανικών, τμήμα Ναυπηγών μηχανικών.

- Δρούγας, Α., Σαρρή, Α., Κυρανούδη, Π. και Ζήσης, Α., (2019), *Port Cybersecurity*.

- Καβαλλιεράτος, Γ., (2018), *Κυβερνοεπιθέσεις στο cyber-enabled πλοίο, Cyber-attacks against the cyber-enabled ship,* Πανεπιστήμιο Πειραιώς Τμήμα Ψηφιακών Συστημάτων Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων».

- Κουναλάκης, Α., Χαρίτος, Δ., (2022), *Κυβερνοασφάλεια στη Ναυτιλία,* Πανεπιστήμιο Δυτικής Αττικής, Σχολή μηχανικών, τμήμα μηχανικών πληροφορικής.

- Μαργέτη, Γ., Σαλοδημήτρη, Δ., Ψωμά, Σ., (2016), *"Η Σημασία και Προοπτικές της Εμπορικής Ναυτιλίας στην Ανάπτυξη της Ελληνικής Οικονομίας",* Τμήμα Λογιστικής, ΤΕΙ Δυτικής Ελλάδος.

- Μερούση, Β., (2021), *Κυβερνοασφάλεια στην Ναυτιλία: Η χρήση του διαδυκτίου από το πλήρωμα,* Πανεπιστήμιο Αιγαίου, τμήμα ναυτιλίας και επιχειρηματικών υπηρεσιών.

- Χήτα, Π., (2021), *Κυβερνοασφάλεια και Θαλάσσια Ασφάλιση,* Πανεπιστήμιο Πειραιώς, Τμήμα Ναυτιλιακών σπουδών.

Ξένη

- IMO (2021), 'The Guidelines of Cyber Security Onboard Ships'

- Abrams, M., & Weiss, J. (2008), *Malicious Control System Cyber Security Attack Case Study* , Maroochy Water Services, Australia. National Institute of Standards and Technology, Computer Security Division.

- Kapalidis, P., (2020), *Cybersecurity at Sea. In Global Challenges in Maritime Security*, Springer: Berlin/Heidelberg, Germany, pp: 127–143

- Mednikarov, B., Tsonev, Y., Lazarov, A., (2020), *Analysis of Cybersecurity Issues in the Maritime Industry*. Inf. Secur.**,** vol. *47*, pp: 27–43.

- Mileski, J., Clott, C. and Galvao, C.B., (2018), *"Cyberattacks on ships: a wicked problem approach"*, Maritime Business Review, Vol. 3 No. 4, pp. 414-430.

- Jones, K., (2016), *Threats and Impacts in Maritime Cyber Security*, University of Plymouth, School of Engineering, Computing and Mathematics

- Jensen, L., (2015), *Challenges in Maritime Cyber-Resilience*, Technology Innovation Management Review, vol.48, pp: 35-39.

- Simon, L., Bruce, C., (2009), *Cyberattacks: Why, What, Who, and How*, IT Professional maganize, Vol: 11, Issue: 3, pp: 14 – 21.

Διαδικτυακές πηγές

- Isalos, "*The History of Greek Shipping*", (2021), link: https://www.isalos.net/i-elliniki-naftilia/history/

- Katie Chadd, "*The History of Cybersecurity*", (2020), link: https://blog.avast.com/history-of-cybersecurity-avast

- Naftemporiki, *"Ναυτιλία: Η «Μεγάλη Αποσύνδεση» και η κυβερνοασφάλεια*" link: https://www.naftemporiki.gr/maritime/1400716/naytilia-i-megali-aposyndesi-kai-i-kyvernoasfaleia/

- Καπτ. Γ. Γεωργούλη Αξ. Ε.Ν.,*" Κυβερνοεπιθέσεις στη Ναυτιλία: Η Σύγχρονη Απειλή Μπορεί να Περιοριστεί"*, (2018), link: https://www.isalos.net/2018/08/kyvernoepitheseis-sti-naftilia-i-synchroni-apeili-borei- na-perioristei/

- Ελεάνα Χουτέα, *"Πως Μπορεί να θωρακιστεί η Ναυτιλίας Απέναντι στης Κυβερνοαπειλές;"*, (2019), link: https://www.liberal.gr/apopsi/pos-mporei-na-thorakistei-i-nautilia-apenanti-stis- kubernoapeiles/241148

- ESET, "*Types of Cybersecurity Threats*", (2022), link: https://www.eset.com/uk/types-of-cyber-threats/

Άλλες Διαδικτυακές πηγές

- https://el.wikipedia.org/wiki/Κυβερνοεπίθεση
- https://www.consilium.europa.eu/el/policies/cybersecurity/
- https://www.naftemporiki.gr/maritime/1400716/naytilia-i-megali-aposyndesi-kai-i-kyvernoasfaleia/
- https://www.naftikachronika.gr/2022/06/01/kyvernoasfaleia-sti-naftilia-veltistes-praktikes-kai-prosfates-exelixeis/
- https://www.isalos.net/2022/12/cybersecurity-onboard-technologiki-exelixi-kai-antimetopisi-enos-diaforetikou-tomea-michalis-vrettos/
- https://www.eset.com/gr/types-of-cyber-threats/
- https://tictac.gr/cyber-security/