ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

στην

ΝΑΥΤΙΛΙΑ

«Κυβερνοασφάλεια και Θαλάσσια Ασφάλιση»

Πετρούλα Χήτα

Διπλωματική εργασία
που υποβλήθηκε στο Τμήμα Ναυτιλιακών Σπουδών
του Πανεπιστημίου Πειραιώς ως μέρος των
απαιτήσεων για την απόκτηση του Μεταπτυχιακού
Διπλώματος Ειδίκευσης στη Ναυτιλία

Πειραιάς, Αύγουστος 2021

ΔΗΛΩΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

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

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Η παρούσα Διπλωματική Εργασία εγκρίθηκε ομόφωνα από την Τριμελή Εξεταστική Επιτροπή που ορίσθηκε από την ΓΣΕΣ του Τμήματος Ναυτιλιακών Σπουδών Πανεπιστημίου Πειραιώς σύμφωνα με τον Κανονισμό Λειτουργίας του Προγράμματος Μεταπτυχιακών Σπουδών στην Ναυτιλία.

Τα μέλη της Επιτροπής ήταν:

- Ο Επίκουρος Καθηγητής κ. Γεώργιος Δανιήλ (Επιβλέπων Καθηγητής)
- Ο Καθηγητής κ. Γεώργιος Βλάχος
- Ο Επίκουρος Καθηγητής κ. Διονύσης Πολέμης

Η έγκριση της Διπλωματικής Εργασίας από το Τμήμα Ναυτιλιακών Σπουδών του Πανεπιστημίου Πειραιώς δεν υποδηλώνει αποδοχή των γνωμών του συγγραφέα

ΕΥΧΑΡΙΣΤΙΕΣ

Η εκπόνηση της παρούσας διπλωματικής εργασίας επισφραγίζει την ολοκλήρωση των μεταπτυχιακών σπουδών μου στην Ναυτιλία. Η συγγραφής της με βοήθησε να διευρύνω τις γνώσεις μου και να μελετήσω εις βάθος ένα ιδιαίτερα σημαντικό και επίκαιρο ζήτημα. Θα ήθελα, στο σημείο αυτό, να εκφράσω τις θερμότερες ευχαριστίες μου στον επιβλέποντα καθηγητή μου για την καθοδήγηση και επιστημονική του βοήθεια κατά την υλοποίηση της παρούσας εργασίας, καθώς και για το ενδιαφέρον που εξαρχής έδειξε στην ανάπτυξη του παρόντος θέματος. Τέλος, δε θα μπορούσα να μην εκφράσω το μεγαλύτερο ευχαριστώ στην οικογένεια μου για την αμέριστη στήριξη και αγάπη της.

Με εκτίμηση

Πετρούλα Χήτα

Στην οικογένειά μου…

“There are only two types of companies: those that have been hacked and those that will be”

Robert Mueller, FBI Director 2012

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Σε μια εποχή όπου οι κίνδυνοι στον κυβερνοχώρο αποτελούν πραγματική και παρούσα απειλή για τον θαλάσσιο κόσμο, οι πλοιοκτήτες και όλοι οι σχετιζόμενοι με τη ναυτιλία φορείς, καλούνται να βρίσκονται σε εγρήγορση και να θωρακιστούν απέναντι στις κυβερνοεπιθέσεις. Στην προσπάθεια αυτή είναι απαραίτητο να παίξει καταλυτικό ρόλο η θαλάσσια ασφάλιση, καθώς η δυνατότητα ασφάλισης κατά κινδύνων του κυβερνοχώρου, τόσο στη στεριά όσο και στη θάλασσα, δεν αποτελεί μόνο τρόπο κάλυψης της εκάστοτε οικονομικής ζημίας ή απώλειας, αλλά θεωρείται και ως μέσο άμεσης διαχείρισης του συμβάντος.

ABSTRACT

In an era in which cyber-attacks are a reality, the shipping industry is not exempt from a potential disruption in their business. Ship owners and carriers related to shipping have to be cognizant of this threat and must take the appropriate measures to protect their clients and the industry. In this effort, marine insurance has a significant role that protects the client against cyber-attacks on land, as well as, on the sea. The marine insurance benefits cover financial losses and/or costs, but will also be a means of handling the incident in a timely manner.

ΕΙΣΑΓΩΓΗ

Ιούνιος 2017 - Ο δανέζικος κολοσσός A.P. Moller – Maersk ανακοινώνει μέσω του λογαριασμού του στο twitter, ότι το λογισμικό σύστημα της εταιρίας βρέθηκε στο στόχαστρο κυβερνοεπίθεσης, με αποτέλεσμα αυτό να τεθεί εκτός λειτουργίας σε διάφορες περιοχές ανά την υφήλιο, όπου η εταιρία διατηρεί γραφεία. Η μετέπειτα αποκατάσταση της ζημιάς και ο συνολικός αντίκτυπος της στις δραστηριότητες του ομίλου άγγιξε τα 300 εκ. $ και διήρκησε περίπου ένα μήνα σύμφωνα με τα επίσημα στοιχεία της εταιρίας.

Νοέμβριος 2017 - Ο μεγαλύτερος ναυλομεσιτικός οίκος του κόσμου, ο βρετανικός Clarksons, δέχεται επίθεση από χάκερς, οι οποίοι παραβίασαν τα ηλεκτρονικά του συστήματα και αντέγραψαν δεδομένα και αρχεία της εταιρίας. Η κυβερνοεπίθεση αυτή, όπως αποδείχθηκε κατόπιν έρευνας, προήλθε από έναν μοναδικό και απομονωμένο λογαριασμό χρήστη.

Ιούλιος 2018 - Η COSCO Shipping Lines παραλύει από μία κυβερνοεπίθεση που έλαβε χώρα στα γραφεία της στην Αμερική με αποτέλεσμα να σημειωθούν βλάβες και δυσλειτουργίες στο δίκτυο ίντερνετ και τηλεπικοινωνιών της εταιρίας. Παρά το γεγονός ότι το συμβάν επηρέασε μόνο τις εργασίες του τερματικού της σταθμού στο λιμένα του Long Beach, η COSCO αναγκάστηκε να διακόψει τη λειτουργία των συστημάτων της και κατ' επέκταση την επικοινωνία της με άλλες περιοχές, προκειμένου να αποκαταστήσει την υφιστάμενη βλάβη και να ελαχιστοποιήσει τις επιπτώσεις της επίθεσης.

Τα ανωτέρω πραγματικά περιστατικά αποδεικνύουν πέραν πάσης αμφιβολίας πόσο ευάλωτη είναι η ναυτιλιακή βιομηχανία στο σύνολό της και πόσο τρωτό το περιβάλλον της σε μια επικείμενη κυβερνοεπίθεση. Η κυβερνό – απειλή (cyber – threat) αποτελεί τη σύγχρονη μορφή τρομοκρατίας η οποία τα τελευταία χρόνια έχει βάλει στο στόχαστρο τη ναυτιλία, που είναι για πολλούς λόγους, μια βιομηχανία πολύ δελεαστική για τους χάκερς, προκαλώντας στα «θύματα» της τεράστια ζημία τόσο σε οικονομικό επίπεδο όσο και σε επίπεδο φήμης.

Είναι το χρονικό σημείο, όπου όλοι οι σχετιζόμενοι με τη ναυτιλία φορείς πρέπει να κάνουν μια εις βάθος προσπάθεια, προκειμένου να αντιμετωπίσουν επιτυχώς την αυξανόμενη απειλή των κυβερνοεπιθέσεων και με τα κατάλληλα αμυντικά μέτρα να ξεπεράσουν τις «Συμπληγάδες» της σύγχρονης εποχής. Θα μπορούσαν οι ναυτασφαλίσεις ν' αποτελέσουν ένα σημαντικό «εργαλείο» σε αυτήν την προσπάθεια της ναυτιλιακής βιομηχανίας;

Κεφάλαιο 1. Οι κυβερνοεπιθέσεις: Μια σύγχρονη πραγματικότητα

1.1.Γενική επισκόπηση της κυβερνοεπίθεσης

Ως κυβερνοεπίθεση νοείται κάθε κακόβουλη και προμελετημένη απόπειρα, που γίνεται με τη χρήση υπολογιστή και μόνο μέσω διαδικτύου, από έναν άνθρωπο ή οργανισμό[1] με σκοπό να παραβιάσει το πληροφοριακό/λογισμικό σύστημα κάποιου άλλου ανθρώπου ή οργανισμού και να αποκομίσει περιουσιακό ή μη όφελος[2].

Η κυβερνοεπίθεση, ως στοιχειοθετείται, έχει κάποια συγκεκριμένα χαρακτηριστικά που δυσχεραίνουν τη διερεύνηση και κατ' επέκταση την εξιχνίασή της. Ειδικότερα:

- την ταχύτητα, καθώς οι επιθέσεις διαπράττονται σε ελάχιστο χρονικό διάστημα και πολλές φορές χωρίς να γίνονται αντιληπτές από το θύμα
- την ευκολία, γιατί η απόπειρα ή η τέλεση της κάθε πράξης γίνεται μέσω υπολογιστή και στον οικείο χώρο του δράστη
- την ανωνυμία που προσφέρει το διαδίκτυο ως ασπίδα του δράστη
- τον διασυνοριακό χαρακτήρα της πράξης, καθώς μπορεί να διαφέρει ο τόπος τέλεσης της επίθεσης και ο τόπος επέλευσης του αποτελέσματος της
- την έλλειψη επαρκούς καταγραφής, διότι οι τελούμενες κυβερνοεπιθέσεις είναι στην πραγματικότητα περισσότερες από αυτές που τελικά καταγράφονται

Η ανωνυμία που προσφέρει το διαδίκτυο στους χρήστες του καθιστά κάποιες φορές δύσκολο τον εντοπισμό της προέλευσης των κυβερνοεπιθέσεων. Η προστασία της ταυτότητας του ατόμου και η ελευθερία έκφρασης του σε οποιοδήποτε περιβάλλον είναι αναφαίρετα και συνταγματικά κατοχυρωμένα δικαιώματα. Η ελευθερία έκφρασης είναι κατοχυρωμένη στο αρ. 14§1 του Συντάγματος και στο αρ. 10§1 της ΕΣΔΑ ενώ η ανώνυμη διαδικτυακή επικοινωνία και κατ' επέκταση η απόκρυψη της ταυτότητας των χρηστών θεωρείται ως αντικείμενο προστασίας σ' ένα πιο διευρυμένο πλαίσιο των αρ. 9Α του Συντάγματος για την προστασία των προσωπικών δεδομένων και αρ. 19 του Συντάγματος για την προστασία του απορρήτου επικοινωνιών. Παρά το γεγονός ότι αυτή η συνταγματικά κατοχυρωμένη ανωνυμία είναι η ασπίδα προστασίας των δραστών και ένας από τους λόγους που δυσκολεύει

[1]Έχει επικρατήσει διεθνώς να χρησιμοποιείται ο όρος χάκερ· όποιος προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε άλλο σύστημα δεδομένων ή που καθιστά μη διαθέσιμο κάποιο σύστημα, μέσω υπολογιστών και διαδικτύου

[2]Ορισμός από Wikipedia

σε σημαντικό βαθμό την εξιχνίαση των κυβερνοεπιθέσεων, θεωρείται αδύνατη η κατάργησή της, διότι αυτό θα οδηγούσε σε παραβίαση των ατομικών ελευθεριών.

1.1.1. Σύντομη αναφορά στους δράστες μιας κυβερνοεπίθεσης

Ανάλογα με το κίνητρο για την πραγματοποίηση μιας κυβερνοεπίθεσης οι δράστες μπορούν να χωριστούν σε 4 κατηγορίες, ήτοι τους ακτιβιστές, τους εγκληματίες, τους καιροσκόπους και τους τρομοκράτες ή τα κράτη.[3] Στους πρώτους δε, συμπεριλαμβάνονται και οι δυσαρεστημένοι υπάλληλοι μιας επιχείρησης, εταιρίας ή οργανισμού. Τα κίνητρα του κάθε δράστη και ποιος είναι ο πραγματικός σκοπός της επίθεσης που πράττει, διαφέρει ανά κατηγορία, γι' αυτό άλλωστε και τα θύματα μιας κυβερνοεπίθεσης δεν είναι συγκεκριμένα, αλλά μπορεί να είναι μεμονωμένα άτομα, επιχειρήσεις, οργανισμοί, κρατικές υπηρεσίες, υπουργεία, κυβερνήσεις, και κράτη ολόκληρα. Επίσης μπορεί, είτε να είναι ο κύριος στόχος του δράστη και να είναι συγκεκριμένα εξαρχής είτε τυχαία. Η επιλογή εξαρτάται από τα κίνητρα και την πρόθεση που έχει ο δράστης ώστε να εκμεταλλεύεται κάθε φορά τα τρωτά σημεία του κυβερνοχώρου. Η υποκλοπή προσωπικών δεδομένων, στρατηγικών σχεδίων, οικονομικών πληροφοριών, κωδικών, η τέλεση απατών, η στρατιωτική και επιστημονική κατασκοπεία με τα αντίστοιχα οικονομικά, πολιτικά, στρατιωτικά οφέλη που προσπορίζει ο δράστης μιας κυβερνοεπίθεσης είναι οι αιτίες που τέτοιου είδους επιθέσεις έχουν αυξηθεί ραγδαία. Η συνήθης πρακτική των δραστών είναι ν' αποκρυπτογραφούν τα ευαίσθητα δεδομένα και αρχεία των θυμάτων τους και στη συνέχεια να τους ζητούν λύτρα. Πάνω από το 50% των επιθέσεων στον κυβερνοχώρο έχουν ως αποτέλεσμα την περιουσιακή ζημία των θυμάτων και αν μάλιστα, το θύμα δεν είναι μεμονωμένος χρήστης, αλλά εταιρία, τότε η ζημία επεκτείνεται και στη φήμη της.

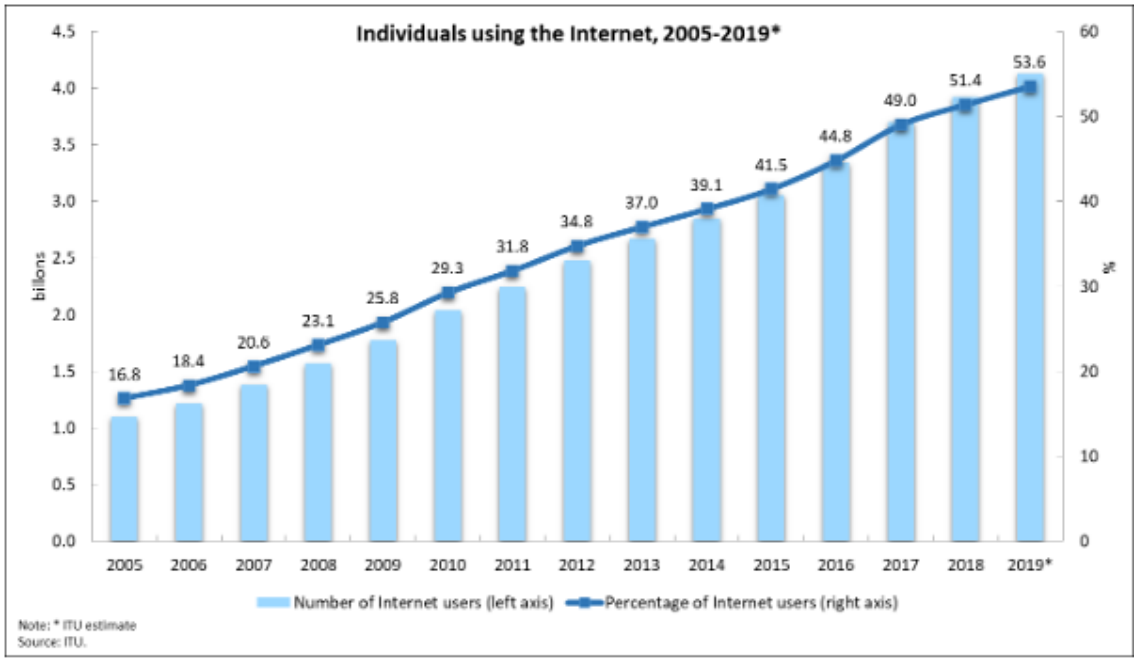
Επιπλέον, αξίζει να γίνει μία μικρή αναφορά στο ότι ο κυβερνοχώρος, όπως αποδεικνύεται από τα αμέτρητα περιστατικά που έχουν λάβει χώρα, αποτελεί το νέο πεδίο δράσης διακρατικών συγκρούσεων. Κρατικά χρηματοδοτούμενες επιθέσεις εντός του κυβερνοχώρου συνιστούν μία νέα μορφή πολέμου. Τα κίνητρα μίας τέτοιας επίθεσης είναι καθαρά πολιτικά και ο στόχος τους είναι πρόδηλος· αποσκοπεί στην υπονόμευση της ακεραιότητας, της ασφάλειας και της οικονομικής ανταγωνιστικότητας του βαλλόμενου κράτους, επιφέροντας συγχρόνως ενδεχόμενο κίνδυνο σύγκρουσης. Οι κυβερνοεπιθέσεις μεταξύ των κρατών κερδίζουν συνεχώς έδαφος και έχουν αποκτήσει διεθνικό χαρακτήρα, γιατί δύναται να

[3] The Guidelines on Cyber Security Onboard Ships (2017)

επιφέρουν το ίδιο αποτέλεσμα με μία ένοπλη επίθεση, ήτοι την πρόκληση ζημίας στο αντίπαλο κράτος, αλλά αυτό να γίνει ευκολότερα, ταχύτερα και οικονομικότερα. Βεβαίως, όπως είναι λογικό, μία τέτοια δράση - επίθεση προκαλεί και την αντίστοιχη αντίδραση – αντεπίθεση του βαλλόμενου κράτους με ότι αυτό συνεπάγεται για τις μεταξύ των κρατών σχέσεις. Για το λόγο αυτό, το κύριο μέλημα των κρατών πρέπει να είναι ένας ανοιχτός, ασφαλής και σταθερός κυβερνοχώρος, η επίτευξη του οποίου θα πραγματοποιηθεί μέσω της ενίσχυσης της διεθνούς συνεργασίας και της ειρηνικής διευθέτησης των διεθνών διαφορών στον κυβερνοχώρο.

1.1.2. Οι πιο συνηθισμένες μορφές κυβερνοεπιθέσεων

Σε μία εποχή που στον κυβερνοχώρο είναι συνδεδεμένοι 4 δισεκατομμύρια χρήστες, όλοι μας είμαστε εν δυνάμει θύματα μιας κυβερνοεπίθεσης. Σύμφωνα μάλιστα με εκτιμήσεις της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU)[4], μέχρι το τέλος του 2019, το 53,6% του παγκόσμιου πληθυσμού έκανε χρήση του διαδικτύου αυξάνοντας τους μεμονωμένους χρήστες κατά ~215% σε σχέση με το 2005.



Πηγή: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Ωστόσο, το ζήτημα που τίθεται είναι το κατά πόσο είμαστε ή όχι προετοιμασμένοι να αντιμετωπίσουμε μια τέτοια επίθεση. Αξίζει δε, να σημειωθεί ότι, παρά την καταγραφή 17 εκατομμυρίων κυβερνοεπιθέσεων σε εβδομαδιαία βάση, το 90% των εταιριών δεν είναι

[4] Οργανισμός των Ηνωμένων Εθνών που ειδικεύεται στις τεχνολογίες πληροφοριών και επικοινωνιών

ακόμα έτοιμο και κατάλληλα προετοιμασμένο να αντιμετωπίσει αποτελεσματικά μια ενδεχόμενη επίθεση. Αυτό οφείλεται και στο γεγονός ότι τα είδη των κυβερνοεπιθέσεων συνεχώς μεταλλάσσονται, το οποίο συμβαίνει γιατί οι δράστες εκμεταλλευόμενοι το διαρκώς εξελισσόμενο τεχνολογικό περιβάλλον δημιουργούν νέες μορφές επιθέσεων ή «τελειοποιούν» τις ήδη υπάρχουσες. Οι τέσσερις πιο γνωστές και συνηθισμένες μορφές επιθέσεων, η συνοπτική αναφορά των οποίων θα βοηθήσει στην κατανόηση του τρόπου με τον οποίο πραγματοποιούνται οι κυβερνοεπιθέσεις, είναι το Ransomware, το Phishing, το Wi-Fi και το DDoS.

Ransomware: είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει ευαίσθητα προσωπικά δεδομένα του θύματος ή του απαγορεύει την πρόσβασή του σε αυτά ζητώντας του συγχρόνως λύτρα. Εξάλλου, η ονομασία του συγκεκριμένου λογισμικού προέρχεται από τη λέξη ransom που σημαίνει λύτρα, καθιστώντας σαφές σε τι ακριβώς αποσκοπεί η συγκεκριμένη επίθεση. Το ransomware λειτουργεί με την κρυπτογράφηση των αρχείων του θύματος.

Phishing: τρόπος εξαπάτησης των χρηστών του διαδικτύου, ο οποίος γίνεται με τον τρόπο που υποδηλώνει η ίδια η ονομασία που δόθηκε σε αυτό το είδος επίθεσης. Οι εισβολείς βασίζονται στην άγνοια και την ευπιστία των χρηστών και μιμούμενοι μία υπαρκτή και αξιόπιστη οντότητα ή υπηρεσία, όπως κάποιο χρηματοπιστωτικό ίδρυμα, συνήθως μέσω του ηλεκτρονικού ταχυδρομείου εκμαιεύουν - ψαρεύουν από το θύμα ευαίσθητες προσωπικές πληροφορίες, όπως τα στοιχεία του τραπεζικού λογαριασμού του. Στη συνέχεια, οι πληροφορίες αυτές χρησιμοποιούνται για εκβιασμό, για άδειασμα των λογαριασμών ή πωλούνται από τους δράστες σε τρίτους. Και σε αυτού του είδους την επίθεση το κίνητρο του δράστη είναι οικονομικό.

Wi-Fi: η επίθεση αυτή πραγματοποιείται μέσω του δικτύου Wi-Fi. Όταν ο δράστης συνδεθεί σε συσκευή που είναι συνδεδεμένη σε Wi-Fi τότε έχει πρόσβαση σε οποιαδήποτε συσκευή είναι συνδεδεμένη στο ίδιο δίκτυο. Με αυτόν τον τρόπο ο χάκερ έχει πρόσβαση, όχι μόνο στις ιστοσελίδες που επισκέπτεται το θύμα, αλλά και σε προσωπικές του πληροφορίες, όπως κωδικούς πρόσβασης σε σελίδες κοινωνικής δικτύωσης ή σε τραπεζικούς λογαριασμούς, τις οποίες είναι δυνατόν το θύμα να έχει πληκτρολογήσει σε αυτές. Επίσης είναι πιθανό ο δράστης να εισαγάγει μέσω του Wi-Fi κακόβουλο λογισμικό στον υπολογιστή ή στο κινητό του θύματος.

DDoS: η κατανεμημένη άρνηση υπηρεσιών (Distributed Denial of Service) είναι μία κυβερνοεπίθεση που στοχεύσει να καταστήσει μία πηγή ηλεκτρονικού συστήματος, όπως μία ιστοσελίδα, μη διαθέσιμη στους χρήστες της. Για να επιτευχθεί αυτού του είδους η επίθεση

είναι αναγκαία η χρησιμοποίηση πολλών υπολογιστών, συνδέσεων ίντερνετ και η μαζική αποστολή δεδομένων προκειμένου να «πλημμυρίσει» ο στόχος και να οδηγηθεί στην προσωρινή ή μη κατάρρευσή της.

Οι κυβερνοεπιθέσεις δεν είναι ένα μακρινό σενάριο επιστημονικής φαντασίας, αλλά είναι ένα υπαρκτό πρόβλημα, που συμβαδίζει με την εξέλιξη της τεχνολογίας, της πληροφορικής, των τηλεπικοινωνιών και του διαδικτύου, και το οποίο με το πέρασμα του χρόνου αλλάζει μορφές, μεταλλάσσεται και προσαρμόζεται σε διαφορετικό κάθε φορά τεχνολογικό υπόβαθρο. Οι χωρίς πρόσωπο δράστες κινούνται σ' έναν κόσμο, ο οποίος είναι δύσκολο να οριοθετηθεί αυξάνοντας καθημερινά τη λίστα με τα θύματά τους. Κάποια από αυτά είναι μεμονωμένοι χρήστες του διαδικτύου ενώ άλλα μπορεί να είναι ολόκληροι κλάδοι της παγκόσμιας οικονομίας, όπως η ναυτιλιακή βιομηχανία.

1.2 Οι κυβερνοεπιθέσεις στη ναυτιλιακή βιομηχανία

Η παγκόσμια ναυτιλιακή βιομηχανία στο σύνολο του εύρους της δραστηριότητάς της είναι άκρως διασυνδεδεμένη με την τεχνολογία, προκειμένου να ανταπεξέλθει στις απαιτήσεις της αγοράς και τις προκλήσεις της εποχής. Έχει εισέλθει στο νέο, ψηφιακό κόσμο με την υιοθέτηση αναδυόμενων τεχνολογιών, που αποτελούν πλέον αναπόσπαστο κομμάτι της. Όλες οι εργασίες που αφορούν τον τομέα της ναυτιλίας, η πολυπλοκότητα των οποίων είναι αδιαμφισβήτητη, πραγματοποιούνται και συνδέονται μεταξύ τους μέσω ψηφιακών συστημάτων. Οι ναυτιλιακές επιχειρήσεις και η διεκπεραίωση πληθώρας καθημερινών δραστηριοτήτων της ναυτιλιακής βιομηχανίας βασίζονται σε συστήματα του κυβερνοχώρου.

Τα συστήματα εντοπισμού της θέσης των πλοίων (GPS – Global Position System[5]), οι ηλεκτρονικές φορτωτικές (e – bills of lading), η ηλεκτρονική πλοήγηση των πλοίων με τα ηλεκτρονικά συστήματα χαρτών (ECDIS – Electronic Chart Display and Information System[6]), η παρακολούθηση του φορτίου, η θέση και η κίνηση των πλοίων σε πραγματικό χρόνο μέσω του AIS (Automatic Identification System[7]), η επικοινωνία, η ανταλλαγή

[5]Το παγκόσμιο σύστημα Στιγματοθέτησης ή θεσιθεσίας είναι το δορυφορικό σύστημα εντοπισμού γεωγραφικής θέσης, ακινήτου ή κινητού χρήστη με μεγάλη ακρίβεια

[6] Ηλεκτρονικό σύστημα πλοήγησης που πληροί τους κανονισμούς του IMO και χρησιμοποιείται ως εναλλακτική στην πλοήγηση με παραδοσιακούς χάρτες. Παρέχει ποικιλία πληροφοριών σε πραγματικό χρόνο (βλ. IMO Resolution A.817 (19) κεφ. 2 § 2.1)

[7] Σύστημα ειδικά σχεδιασμένο ώστε να παρέχει αυτόματα και σε πραγματικό χρόνο πληροφορίες, που αφορούν το πλοίο, σε άλλα πλοία και στις παράκτιες αρχές (Regulation 19 of SOLAS κεφ. V)

μηνυμάτων ηλεκτρονικού ταχυδρομείου και η τήρηση αρχείων και δεδομένων, δηλαδή όλες οι λειτουργίες, από τις πιο πολύπλοκες μέχρι τις πιο απλές, εξαρτώνται από αξιόπιστα και ασφαλή συστήματα. Είναι αδιαμφισβήτητο ότι και οι λειτουργίες των πλοίων, είναι πλέον άρρηκτα συνδεδεμένες με τον κυβερνοχώρο. Επομένως, είναι λογικό τα περιστατικά επιθέσεων και απειλών, που αφορούν την ασφάλεια τους, να αυξάνονται όσο εξελίσσεται η τεχνολογία και οι επιθέσεις των χάκερς γίνονται πιο περίπλοκες.

Με 50.000 πλοία όλων των κατηγοριών που βρίσκονται στη θάλασσα ή σε κάποιο λιμάνι ανά πάσα χρονική στιγμή, η ναυτιλιακή βιομηχανία είναι εκτεθειμένη σε μεγάλο βαθμό στις κυβερνοεπιθέσεις.

Ωστόσο, οι επιθέσεις, όπως προκύπτει και από τα εκατοντάδες πραγματικά περιστατικά που έχουν λάβει χώρα, ο αριθμός των οποίων θα ήταν υπερδιπλάσιος, αν δημοσιοποιούνταν όλα τα γεγονότα, δε πραγματοποιούνται μόνο στο πλοία μιας εταιρίας, αλλά και στην ίδια την εταιρία. Εξάλλου το πλοίο, συμπεριλαμβανομένου του φορτίου που μεταφέρει, και η εταιρία με τη βάση δεδομένων που έχει, αποτελούν τους μεγαλύτερους στόχους μιας κυβερνοεπίθεσης με ανυπολόγιστες συνέπειες σε όλα τα επίπεδα.

Μέχρι πριν από μερικά χρόνια η κυβερνοασφάλεια δεν αποτελούσε κάποιο ιδιαίτερο ζήτημα για τα πλοία, καθώς οι δραστηριότητες τους δε συνδέονταν με τον «έξω κόσμο». Με την εξέλιξη όμως της τεχνολογίας και τη σύνδεση όλων των δραστηριοτήτων τους με αυτήν, τα πλοία δεν είναι πλέον μία ξεχωριστή μονάδα αλλά συνδέονται με τον παγκόσμιο διαδικτυακό ιστό, γεγονός που τα κάνει ευπαθή σε κάθε είδους απειλή ή επίθεση μέσω του κυβερνοχώρου. Ακόμα και η λειτουργία ώθησης του πλοίου, μέσω των κύριων και βοηθητικών συστημάτων του, μία λειτουργία που εκ πρώτης όψεως δε φαίνεται να σχετίζεται καθόλου με υπολογιστές, βασίζεται πλέον, αποκλειστικά στη σωστή χρήση αυτών, προκειμένου να λειτουργήσουν αποδοτικά. Γενικά οι λειτουργίες του πλοίου, που συνδέονται με την ασφαλή πλοήγησή του, τον εντοπισμό της θέσης του, την κίνησή του σε πραγματικό χρόνο και την παρακολούθηση του φορτίου, είναι αυτές οι λειτουργίες, που μπορούν να προσβληθούν πιο εύκολα από μια επίθεση, λόγω του ότι είναι άρρηκτα συνδεδεμένες και εξαρτημένες με τον κυβερνοχώρο.

Χαρακτηριστικό παράδειγμα του ανωτέρω, είναι το πόσο εύκολα μπορεί να προσβληθεί από μια κυβερνοεπίθεση το AIS, το οποίο σύμφωνα με τον κανονισμό 19 του SOLAS κεφ. 5, είναι υποχρεωτικό να χρησιμοποιείται από α) όλα τα πλοία με χωρητικότητα ίσης ή μεγαλύτερης των 300 τόνων, που εκτελούν διεθνή δρομολόγια, β) όλα τα φορτηγά πλοία με χωρητικότητα ίσης ή μεγαλύτερης των 500 τόνων, ανεξάρτητα από το αν εκτελούν ή όχι διεθνή δρομολόγια, και γ) όλα τα επιβατηγά πλοία ανεξαρτήτως μεγέθους. Το κενό

ασφαλείας και την ευαισθησία της τεχνολογίας του AIS σε μία ενδεχόμενη κυβερνοεπίθεση εντόπισαν δύο ερευνητές του προγράμματος «Forward Looking Threat Research» της εταιρίας ασφαλείας Trend Micro, ο Kyle Wilhoit και Dr. Marco Baltuzzi, σε συνεργασία με τον ανεξάρτητο ερευνητή, Alessandro Pasta. Τα πειράματα που πραγματοποίησαν απέδειξαν ότι, οι βασικοί πάροχοι του AIS, οι οποίοι συλλέγουν τις πληροφορίες και τις διανέμουν, παρουσιάζουν ελαττώματα, με αποτέλεσμα να επιτρέπεται στους εισβολείς να παραβιάζουν τα συστήματα και να εισάγουν μη έγκυρα δεδομένα ή να τροποποιούν κατά το δοκούν τα ήδη υπάρχοντα. Τα δεδομένα αυτά μπορεί να σχετίζονται με τη θέση, την πορεία, το φορτίο, τη σημαία και το όνομα του πλοίου. Επιπλέον οι χάκερς, εξαιτίας των ευπαθειών του συστήματος, μπορούν να δημιουργήσουν ψεύτικα πλοία, τοποθετώντας τα στο χάρτη, να υποκλέψουν τις συνομιλίες των πλοίων, να εκπέμψουν ψεύτικους συναγερμούς SOS ή σύγκρουσης και να απενεργοποιήσουν προσωρινά τη λειτουργία του AIS σε κάθε πλοίο. Αυτό οφείλεται κυρίως στο γεγονός ότι το πρωτόκολλο του AIS σχεδιάστηκε χωρίς να ληφθούν υπόψη κάποιοι σημαντικοί παράγοντες ασφαλείας. Η πραγματοποίηση της έρευνας σε ειδικά διαμορφωμένα εργαστήρια με συγκεκριμένο ραδιοεξοπλισμό προκάλεσε ιδιαίτερη ανησυχία στους επιστήμονες για την ευκολία με την οποία μπορούν οι χάκερς να πραγματοποιήσουν ανάλογες επιθέσεις, ικανές να προκαλέσουν μεγάλη οικονομική ζημία στις εταιρίες, χρησιμοποιώντας ως μέσο, έναν τροποποιημένο ασύρματο πομποδέκτη, με κόστος αγοράς 150 €. Κατόπιν τούτων, γίνεται εύκολα αντιληπτό ότι ένα σύστημα, όπως το AIS, το οποίο δημιουργήθηκε προς διευκόλυνση της ναυτιλίας και χρησιμοποιείται για τη διάδοση χρήσιμων πληροφοριών σε πραγματικό χρόνο, αφήνει πολλά παραθυράκια στους χάκερς για να εκμεταλλευτούν τις όποιες αδυναμίες του καθιστώντας το μη λειτουργικό. Τα αποτελέσματα της ανωτέρω έρευνας παρουσιάστηκαν για πρώτη φορά στη διεθνή συνδιάσκεψη ασφαλείας Hack In The Box στην Κουάλα Λουμπούρ τον Οκτώβριο του 2014 ενώ η λεπτομερής έκθεση δημοσιοποιήθηκε τον Δεκέμβριο του 2014[8].

Με λίγα λόγια, η δυσκολία αναγνώρισης των κινδύνων που εγκυμονεί η χρήση της τεχνολογίας, η αδιαμφισβήτητη εξάρτηση της ναυτιλίας από αυτήν και η μη εις βάθος γνώση επί του θέματος και κατ' επέκταση η μη ορθή λήψη προληπτικών μέτρων, καθιστούν τη ναυτιλιακή βιομηχανία αναμφίβολα ευάλωτη, ένα εύκολο θύμα κυβερνοεπιθέσεων.

1.3 Η στοιχειοθέτηση μιας κυβερνοεπίθεσης

[8] A Trend Micro research paper: A Security Evaluation of AIS

Πέρα από το αναφερθέν γενικό πλαίσιο των κυβερνοεπιθέσεων στη ναυτιλιακή βιομηχανία, θα ήταν χρήσιμο για την πλήρη κατανόηση του εύρους και της ποικιλομορφίας τους, να αναλυθούν τα επιμέρους στοιχεία που στοιχειοθετούν μια κυβερνοεπίθεση, ήτοι τα προφίλ των δραστών, τα είδη και τα στάδια μιας επίθεσης και ο στόχος της ή άλλως τα τρωτά σημεία που εκτίθενται στον κίνδυνο.

1.3.1 Τα πρόσωπα των δραστών

Δύσκολα μπορεί να πιστέψει κάποιος ότι οι χάκερς με το πάτημα ενός πλήκτρου μπορούν να εισχωρήσουν στα συστήματα επιχειρήσεων προκαλώντας σε αυτές ανυπολόγιστη οικονομική ζημία. Και όμως, η τεράστια δύναμη τους, που παραδόξως βρίσκεται στην άκρη των δαχτύλων τους, πηγάζει από τη δυνατότητά πρόσβασής τους στην πληροφορία, η οποία αποτελεί σημαντικό πλεονέκτημα για όποιον την έχει.

Όπως αναφέρθηκε και ανωτέρω, οι δράστες των κυβερνοεπιθέσεων διαφέρουν ανάλογα με το κίνητρο και τον σκοπό της επίθεσης. Ο κάτωθι πίνακας αποδίδει επιγραμματικά και κατανοητά ποιες μπορεί να είναι οι πιθανές συνέπειες μιας κυβερνοεπίθεσης, τόσο στην ναυτιλιακή εταιρία όσο και στα πλοία που αυτή διαχειρίζεται, σε αντιστοιχία με το πρόσωπο που τελεί την επίθεση, το οποίο, όπως είναι αναμενόμενο, εκμεταλλεύεται τις ευπάθειες του κυβερνοχώρου.

Κατηγορία Δράστη	**Κίνητρο**	**Αντικείμενο**
Ακτιβιστές	Αναστάτωση της λειτουργίας Βλάβη της φήμης	Καταστροφή των δεδομένων Δημοσιοποίηση σημαντικών αρχείων Προσοχή των ΜΜΕ
Εγκληματίες	Οικονομικό όφελος Εμπορική κατασκοπεία Βιομηχανική κατασκοπεία	Πώληση κλεμμένων δεδομένων Εξαγορά κλεμμένων δεδομένων Εξαγορά λειτουργικότητας συστήματος Απάτη στη μεταφορά φορτίου
Καιροσκόποι	Πρόκληση	Πρόσβαση στις άμυνες της κυβερνοασφάλειας Οικονομικό όφελος

Κράτη ή Τρομοκράτες	Πολιτικό όφελος Κατασκοπεία	Γνώση Διαταραχή στην οικονομία και στο εθνικό οικοδόμημα

Πηγή: *The Guidelines on Cyber Security Onboard Ships (2017)*

Οι ανωτέρω κατηγορίες δραστών έχουν την ικανότητα, τις δεξιότητες, αλλά και τα κατάλληλα μέσα, ώστε να απειλήσουν και τελικά να πλήξουν την ασφάλεια του πλοίου και τη διαχειριστική ικανότητα της εταιρίας, ολοκληρώνοντας την αποστολή τους. Δέον να υπογραμμιστεί ότι κάθε εταιρία, ανάλογα με το αντικείμενο δραστηριοτήτων της, βρίσκεται στο στόχαστρο διαφορετικής κατηγορίας δραστών. Για παράδειγμα μια διαχειρίστρια εταιρία τάνκερ είναι πολύ πιθανό να δεχτεί περισσότερες απειλές από περιβαλλοντολόγους ακτιβιστές παρά από κάποια άλλη κατηγορία δραστών.

Επιπρόσθετα, ιδιαίτερη προσοχή πρέπει να δοθεί στον ανθρώπινο παράγοντα μιας ναυτιλιακής εταιρίας δηλαδή στο προσωπικό της και αυτό διότι, το ανθρωπινό λάθος έχει υπάρξει η αιτία για πολλά καταγεγραμμένα ατυχήματα. Επομένως και στη συγκεκριμένη περίπτωση, το προσωπικό της εταιρίας, συμπεριλαμβανομένων των υπαλλήλων στα γραφεία αλλά και του πληρώματος, μπορεί ανά πάσα στιγμή να θέσει σε κίνδυνο τα συστήματα, που συνδέονται με τον κυβερνοχώρο. Εξάλλου, είναι αποδεκτό, ότι η εσωτερική απειλή αποτελεί την μεγαλύτερη κυβερνοαπειλή σε μια ναυτιλιακή εταιρία. Η εκ των έσω κυβερνοεπίθεση μπορεί να προκληθεί με δύο τρόπους, είτε ακούσια είτε σκόπιμα.

Η χωρίς πρόθεση, προκαλείται από τα άτομα, τα οποία μπορεί να κάνουν κάποιο λάθος κατά τη διαχείριση του συστήματος Information Technologies (IT) ή Operational Technologies (OT), ή από άτομα, τα οποία δεν έχουν το απαιτούμενο γνωστικό υπόβαθρο ή δεν έχουν λάβει την κατάλληλη εκπαίδευση, όσον αφορά τους κυβερνοκινδύνους και τις κυβερνοεπιθέσεις γενικότερα, ή δε σέβονται και δεν τηρούν τα υποχρεωτικά μέτρα προστασίας. Η εκπαίδευση του εργατικού δυναμικού μιας εταιρίας είναι η κορωνίδα των τρόπων αντιμετώπισης των κυβερνοαπειλών και των κυβερνοεπιθέσεων, καθώς το προσωπικό μιας εταιρίας πρέπει να είναι σε θέση ώστε να αναγνωρίζει του κινδύνους στην κυβερνοασφάλεια, να τους εντοπίζει και να προσπαθεί με κάθε τρόπο να μετριάσει τον επικείμενο κίνδυνο. Από αυτό συνάγεται ότι το ανθρώπινο δυναμικό μιας εταιρίας, από τον υπάλληλο στα γραφεία που εισάγει το κακόβουλο λογισμικό μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου (spear – fishing) μέχρι κάποιο μέλος του πληρώματος που δεν κάνει σωστή χρήση του κινητού τηλεφώνου του, με μηδαμινή ή ελάχιστη εκπαίδευση μπορεί ν’ αφήσει μια ολόκληρη εταιρία εκτεθειμένη σ’ έναν κυβερνοκίνδυνο με ό,τι αυτό συνεπάγεται.

Η εκούσια κυβερνοαπειλή προκαλείται από έναν υπάλληλο, ο οποίος μπορεί να έχει εκδικητικές τάσεις απέναντι στην εταιρία, σε κάποιον ανώτερό του ή συνάδελφό του, μπορεί να καθοδηγείται από συναισθήματα μίσους ή θυμού, από κάποια πολιτική ή θρησκευτική ιδεολογία ή ν' απειλείται από κάποιον τρίτο για να πράξει αυτού του είδους τις ενέργειες κατά της εταιρίας. Η με πρόθεση έκθεση της εταιρίας ή του πλοίου σε κάποιον κυβερνοκίνδυνο και η επερχόμενη κυβερνοεπίθεση προκαλεί πολύ μεγάλη ζημία και εν συνεχεία βλάπτει την εταιρία και το πλοίο.

Όπως έχει αναφέρει χαρακτηριστικά και ο Edward Snowden[9], ο μεγαλύτερος κίνδυνος που υπάρχει στον κυβερνοχώρο και που έχει ν' αντιμετωπίσει μια εταιρία, η οποία λειτουργεί στο σύγχρονο διασυνδεδεμένο κόσμο, είναι ο άνθρωπος.

1.3.2 Τα είδη μιας κυβερνοεπίθεσης

Τα είδη των κυβερνοεπιθέσεων σε μια ναυτιλιακή εταιρία ή σ' ένα πλοίο, καθώς και τα μέσα που χρησιμοποιεί ο δράστης για την υλοποίηση του σκοπού του, διαφέρουν ανάλογα με το αν η εταιρία ή το πλοίο αποτελούν τον στόχο του δράστη εξαρχής ή ένα τυχαίο θύμα.

Ειδικότερα, οι δράστες στις στοχευμένες επιθέσεις χρησιμοποιούν συγκεκριμένα εργαλεία και τεχνικές ειδικά διαμορφωμένα για την εταιρία ή το πλοίο, στα οποία αποβλέπουν. Μάλιστα, οι επιθέσεις που λαμβάνουν χώρα είναι πιο εξεζητημένες. Μερικά παραδείγματα αυτών, των εξειδικευμένων εργαλείων, που χρησιμοποιούνται σε τέτοιου είδους επιθέσεις, είναι τα εξής:

Brute Force: Επίθεση κατά την οποία ο εισβολέας χρησιμοποιεί πολλούς και διαφορετικούς συνδυασμούς κωδικών πρόσβασης, τους οποίους ελέγχει συστηματικά και εξετάζει τους πιο πιθανούς μέχρι να βρει τον σωστό.

Social Engineering: Εισβολείς προσπαθούν να χειραγωγήσουν άτομα, τα οποία ανήκουν στο ανθρώπινο δυναμικό της εταιρίας ή είναι μέλη του πληρώματος του πλοίου, ώστε να σπάσουν τις διαδικασίες ασφαλείας που ακολουθεί η εταιρία. Η χειραγώγηση αυτή πραγματοποιείται συνήθως μέσω των κοινωνικών δικτύων.

Denial of Service: Πλημμυρίζοντας ένα δίκτυο με δεδομένα, αποτρέπει τους νόμιμους και εξουσιοδοτημένους χρήστες από το να έχουν πρόσβαση σε πληροφορίες.

[9] Αμερικανός διαχειριστής συστημάτων, ο οποίος εργαζόταν για την National Security Agency (NSA) και την Central Intelligence Agency (CIA) των ΗΠΑ. Το 2013 διοχέτευσε στον τύπο απόρρητες πληροφορίες για μια σειρά από μυστικά προγράμματα παρακολουθήσεων της NSA.

Subverting the supply chain: Επίθεση σε εταιρία ή σε πλοίο, μέσω του εξοπλισμού, του λογισμικού ή των υποστηρικτών υπηρεσιών, που παραδίδονται στην εταιρία ή στο πλοίο στο πλαίσιο λειτουργίας της εφοδιαστικής αλυσίδας.

Spear Phishing: Λειτουργεί σαν το ηλεκτρονικό ψάρεμα (phising), αλλά στοχοποιούνται συγκεκριμένα άτομα, που λαμβάνουν προσωπικά emails, τα οποία περιέχουν κακόβουλο λογισμικό ή συνδέσμους, οι οποίοι παραπέμπουν σε κακόβουλο λογισμικό.

Αντίθετα με τα ανωτέρω, οι δράστες, όταν δεν έχουν συγκεκριμένο στόχο, συνήθως χρησιμοποιούν εργαλεία και τεχνικές διαθέσιμα στο διαδίκτυο, τα οποία είναι ικανά να εντοπίσουν, ανακαλύψουν και στη συνέχεια, να εκμεταλλευτούν τις όποιες ευπάθειες έχει η εταιρία ή το πλοίο. Μερικά παραδείγματα των εργαλείων, που χρησιμοποιούνται σε τέτοιες περιπτώσεις είναι τα εξής:

Scanning*:* Ανιχνεύει τις ευπάθειες ενός συστήματος ή τους δυνατούς τρόπους διείσδυσης στο σύστημα ώστε να τα εκμεταλλευτεί αργότερα.

Water Holing*:* Οι δράστες δημιουργούν μία ψεύτικη ιστοσελίδα ή εισχωρούν σε μία ήδη υφιστάμενη προσπαθώντας να εκμεταλλευτούν τους επισκέπτες της.

Malware*:* Κακόβουλο λογισμικό, το οποίο είναι ειδικά σχεδιασμένο ώστε να εισχωρεί και να καταστρέφει τον υπολογιστή του θύματος εν αγνοία του. Υπάρχουν πολλοί τύποι κακόβουλου λογισμικού, ο καθένας εκ των οποίων λειτουργεί διαφορετικά και χρησιμοποιείται ανάλογα με τον στόχο της επίθεσης. Κάποιοι από τους πιο γνωστούς τύπους malware είναι το worm, το trojan, το virus και το ransomware.

Phishing: Οι δράστες αποστέλλουν αληθοφανή μηνύματα ηλεκτρονικού ταχυδρομείου σε πιθανούς στόχους, μη προαποφασισμένους, ζητώντας τους την καταχώρηση των ευαίσθητων και προσωπικών τους δεδομένων, όπως κωδικών πρόσβασης. Επίσης, τα μηνύματα δύναται να περιλαμβάνουν κάποιον σύνδεσμο, ο οποίος να παραπέμπει τους παραλήπτες σε κάποια ψεύτικη ιστοσελίδα, ειδικά διαμορφωμένη, προς εξυπηρέτηση του σκοπού των εισβολέων.

Σύμφωνα με την "θαλάσσια επισκόπηση κυβερνοασφάλειας" του IHS Markit για το έτος 2020, το ηλεκτρονικό ψάρεμα (phising) αναγνωρίστηκε ως ο κύριος τύπος κυβερνοεπίθεσης, που βίωσε η ναυτιλιακή βιομηχανία, σε ποσοστό 68%, ακολούθησε το spear phising με 41% ενώ οι επιθέσεις με κακόβουλα προγράμματα (malware) ήταν ο τρίτος πιο κοινός τύπος επίθεσης στον κυβερνοχώρο σε ποσοστό 33%. Τα στοιχεία αυτά που παρατίθενται αφορούν το χρονικό διάστημα των τελευταίων 12 μηνών.

Το πρόβλημα ωστόσο, είναι ότι η εφευρετικότητα των εισβολέων δεν εξαντλείται μόνο στα ανωτέρω αναπτυχθέντα εργαλεία, αλλά δυστυχώς, τα είδη των κυβερνοεπιθέσεων, ο

αριθμός των εργαλείων και η πολυπλοκότητα των τεχνικών, που χρησιμοποιούν, συνεχώς εξελίσσονται.

1.3.3 Τα στάδια μιας κυβερνοεπίθεσης

Έχει παρατηρηθεί ότι οι στοχευμένες κυβερνοεπιθέσεις, από την προετοιμασία μιας επίθεσης μέχρι την πραγματοποίησή της, λαμβάνουν χώρα σε τέσσερα στάδια.

Στο πρώτο στάδιο, κατά την προετοιμασία της κυβερνοεπίθεσης, ο εισβολέας προσπαθεί να βρει, μέσω δημοσιεύσεων, εγγράφων, κοινωνικών μέσων και ιστοσελίδων, όσες περισσότερες πληροφορίες είναι διαθέσιμες για την εταιρία, το πλοίο ή τον συγκεκριμένο υπάλληλο που θέλει να στοχεύσει. Επιπλέον, με επισταμένη παρακολούθηση του στόχου του, συλλέγει πραγματικά και επίσημα δεδομένα, τα οποία αποστέλλονται από τα γραφεία της ναυτιλιακής εταιρίας στο πλοίο και το αντίστροφο, συμπληρώνοντας έτι περαιτέρω τις πληροφορίες που έχει ήδη συγκεντρώσει. Αυτή η πρώτη επαφή του θύτη και του θύματος είναι θεμελιώδης για να στεφθεί με επιτυχία η προαποφασισμένη κυβερνοεπίθεση. Γι' αυτό τον λόγο, ο δράστης πρέπει να μελετήσει προσεχτικά τον στόχο του, συνολικά, αλλά και κάθε επιμέρους στοιχείο του, όπως το ανθρώπινο δυναμικό, χωριστά, και να μάθει όσα περισσότερα μπορεί για αυτόν, ώστε να είναι σε θέση στη συνέχεια να προσδιορίσει με ακρίβεια τα τρωτά του σημεία. Αυτό το στάδιο, το οποίο μπορεί να διαρκέσει για αρκετά μεγάλο χρονικό διάστημα, χαρακτηρίζεται ως το στάδιο της παρακολούθησης/αναγνώρισης του στόχου (Survey/reconnaissance).

Στο δεύτερο στάδιο, οι εισβολείς επιχειρούν με διάφορους τρόπους να αποκτήσουν πρόσβαση στα συστήματα και τα δεδομένα της εταιρίας και του πλοίου. Αυτό μπορεί να επιτευχθεί με παραπλανητικές ή ψεύτικες ιστοσελίδες, με αποστολή κακόβουλου λογισμικού μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ακόμα και μέσω των διαδικτυακών υπηρεσιών της εταιρίας. Οι μέθοδοι είναι πάρα πολλές και ο κάθε εισβολέας επιλέγει τον τρόπο με τον οποίο θα εισχωρήσει στην εταιρία ή το πλοίο. Το δεύτερο στάδιο ονομάζεται παράδοση (Delivery).

Στο τρίτο στάδιο πραγματοποιείται η παραβίαση του ευάλωτου συστήματος της εταιρίας ή του πλοίου. Ωστόσο, η έκταση της παραβίασης και το μέγεθος της προκληθείσας ζημίας εξαρτώνται από το πόσο ευαίσθητα είναι τα αυτά συστήματα, αλλά και από τη μέθοδο που επέλεξε ο εισβολέας, κατά το δεύτερο στάδιο της επίθεσης, για να εισχωρήσει σε αυτά. Μετά την παραβίαση και ανάλογα με το τι ακριβώς έχει παραβιαστεί, ο εισβολέας μπορεί να προκαλέσει αλλαγές στα συστήματα της εταιρίας, οι οποίες είτε μπορεί να γίνουν αντιληπτές

είτε όχι. Σε αυτό το στάδιο ο εισβολέας μπορεί να έχει πρόσβαση σε ευαίσθητα δεδομένα όπως στην ονομαστική λίστα του πληρώματος, των επιβατών, των επισκεπτών, να αποκτήσει πλήρη έλεγχο σε κάποιο από τα συστήματα, όπως στο σύστημα διαχείρισης των μηχανημάτων και να προσπαθήσει να τροποποιήσει πληροφορίες σημαντικές για το σύστημα πλοήγησης. Το τρίτο στάδιο επομένως, είναι αυτό της παραβίασης (Breach).

Στο τέταρτο στάδιο, ο εισβολέας χρησιμοποιεί, ως εργαλείο, το παραβιασμένο σύστημα του τρίτου σταδίου, ώστε μέσω αυτού να επιτεθεί και σε αλλά συστήματα του στόχου λιγότερο ευάλωτα. Σε αυτή τη φάση δηλαδή, ο δράστης προσπαθεί να διατηρήσει την πρόσβασή του στο σύστημα εγκαθιστώντας εργαλεία που θα του το επιτρέψουν, να εκτελέσει καινούργιες επιθέσεις σ' αυτό, να δημιουργήσει το κατάλληλο περιβάλλον, το οποίο θα μπορέσει να υποστηρίξει μια καινούργια επίθεση και να ανακαλύψει γειτονικά συστήματα με τη μέθοδο της σάρωσης ή της χαρτογράφησης δικτύου, τα οποία θα γίνουν ο επόμενος στόχος του. Το στάδιο αυτό έχει πάρει την ονομασία του από την τεχνική της περιστροφής, γιατί ο εισβολέας χρησιμοποιώντας ως βάση την παραβίαση που πραγματοποίησε στο προηγούμενο στάδιο, εκτελεί και άλλες δραστηριότητες (Pivot).

1.3.4 Το αντικείμενο μιας κυβερνοεπίθεσης (προσδιορισμός των τρωτών σημείων)

Μία εταιρία και ένα πλοίο έχουν συστήματα και ακολουθούν διαδικασίες, τα περισσότερα εκ των οποίων είναι δελεαστικά για έναν επίδοξο εισβολέα και κάποιες φορές αρκετά ευάλωτα, κάνοντας πιο εύκολο το έργο του.

Είναι απαραίτητο μια ναυτιλιακή εταιρία να αξιολογεί τα συστήματα που έχει και να γνωρίζει ακριβώς το πόσο ανθεκτικά είναι ή όχι σε μια ενδεχόμενη κυβερνοαπειλή ώστε με βάση αυτά να αναπτύσσει κάθε φορά μια ρεαλιστική στρατηγική αντιμετώπισης των κυβερνοκινδύνων. Είναι προφανές ότι τα συστήματα που είναι συνδεδεμένα σε μη ελεγμένα διαδίκτυα ή απευθείας στο διαδίκτυο είναι περισσότερο ευάλωτα σε εξωτερικούς κυβερνοκινδύνους απ' ότι τα αυτόνομα συστήματα. Για το λόγο αυτό, πρέπει να δοθεί ιδιαίτερη προσοχή στα συστήματα του πλοίου, τα οποία ενδέχεται να είναι συνδεδεμένα σε κάποιο μη ασφαλές δίκτυο, καθιστώντας τα αυτομάτως ευάλωτα και εκτεθειμένα σε κυβερνοκινδύνους. Επομένως, ένα από τα ακόλουθα συστήματα, που υπάρχουν στα πλοία, σε συνδυασμό με την έλλειψη εκπαίδευσης των χειριστών τους, μπορεί οποιαδήποτε χρονική στιγμή να αποτελέσει την αρχή μιας κυβερνοεπίθεσης και αυτό διότι αυτά τα συστήματα είναι ψηφιοποιημένα και κάποια από αυτά μάλιστα, συνδεδεμένα στο διαδίκτυο. Τέτοια

συστήματα είναι τα συστήματα γέφυρας, διαχείρισης φορτίου, ελέγχου πρόσβασης, ώθησης και διαχείρισης μηχανημάτων, εξυπηρέτησης και διαχείρισης επιβατών και επικοινωνίας.

Όπως έχει αναφερθεί και ανωτέρω, η ναυτιλιακή βιομηχανία έχει αφήσει στο παρελθόν κάθε τι που λογίζεται ως παραδοσιακή ναυτιλία και έχει υιοθετήσει μηχανισμούς, οι οποίοι βελτιώνουν την αποδοτικότητά της και τις λειτουργίες της σ' έναν κόσμο, όπου τα πάντα λειτουργούν με ψηφιακή μέσα. Από αυτή την αλλαγή, δε θα μπορούσε να λείπει η ψηφιακή αλληλεπίδραση μεταξύ πλοίου και ακτής/εταιρίας. Αυτό σημαίνει ότι τα πλοία, λόγω των ψηφιοποιημένων μέσων που χρησιμοποιούνται πλέον, γίνονται ολοένα και περισσότερο ένα αναπόσπαστο μέρος των διαδικασιών, που πραγματοποιούνται στην ακτή. Αυτό, όπως είναι λογικό άλλωστε, δίνει τροφή στους δράστες των κυβερνοεπιθέσεων, οι οποίοι βρίσκουν όλο και περισσότερα πεδία δράσης.

Επιπρόσθετα, έχουν παρατηρηθεί στα πλοία κάποιες γενικές ευπάθειες που οδηγούν στην τέλεση μιας κυβερνοεπίθεσης. Απαρχαιωμένα γενικά και μη λειτουργικά συστήματα, ληγμένο ή ανεπαρκές λογισμικό προστασίας από ιούς, ανεπαρκής έλεγχος κατά την πρόσβαση τρίτων μερών, όπως παρόχων υπηρεσιών, υπολογιστές συνδεδεμένοι σε μη ελεγμένα διαδίκτυα, ανεπαρκή ασφάλεια, η οποία περιλαμβάνει τη μη σωστή διαχείριση του δικτύου, των λογαριασμών και των κωδικών πρόσβασης κυρίως από αμέλεια των διαχειριστών. Οι ευπάθειες των συστημάτων παρουσιάζονται, όπως είναι λογικό, πολύ λιγότερο στα νεότευκτα πλοία.

Γενικά τα πλοία, έχουν καταστεί πιο ευάλωτα στο σύνολό τους σε σχέση με τη ναυτιλιακή εταιρία, εξαιτίας της άμεσης εξάρτησής τους από ψηφιακά μέσα και της συνδεσιμότητα τους με τα συστήματα της ακτής.

Από όλα τα ανωτέρω καταδεικνύεται χωρίς αμφιβολία ότι η ναυτιλιακή βιομηχανία είναι εκτεθειμένη σε μεγάλο βαθμό στους κυβερνοκινδύνους, λόγω της αυξημένης ψηφιοποίησης που έχει υποστεί τα τελευταία χρόνια σε συνδυασμό με την έλλειψη νομικής προστασίας και ασφαλιστικής κάλυψης. Σε αυτά δε, συνηγορεί και το γεγονός της μέχρι και σήμερα υποτιμήσης του κινδύνου και των συνεπειών μιας τέτοιας επίθεσης.

Κεφάλαιο 2. Η κυβερνοασφάλεια στη Ναυτιλία

2.1 Υποθέσεις κυβερνοεπιθέσεων στη ναυτιλία - Cases

Τα κάτωθι πραγματικά περιστατικά κυβερνοεπιθέσεων, που έλαβαν χώρα, έκρουσαν τον κώδωνα του κινδύνου στον κόσμο της ναυτιλίας και έδωσαν το έναυσμα στους διεθνείς ναυτιλιακούς οργανισμούς και στους νομοθέτες να σχεδιάσουν και στη συνέχεια να υιοθετήσουν νομοθετήματα και γενικούς κανονισμούς που αφορούν στην προστασία όσων εμπλέκονται σε μια κυβερνοεπίθεση. Είναι σημαντικό, κάθε πλοιοκτήτης να αντιμετωπίζει τις επιθέσεις σα να συνέβησαν στον ίδιο και όχι σα σενάριο επιστημονικής φαντασίας, αδύνατο να «γυριστεί» στην δική του εταιρία ή πλοίο. Μόνο έχοντας αυτή τη νοοτροπία, ορίζοντας δηλαδή το πρόβλημα στις κανονικές του διαστάσεις, αλλά και με τη συνεργασία όλων των μερών της εφοδιαστικής αλυσίδας και όχι με μεμονωμένες προσπάθειες, θα μπορέσει η ναυτιλιακή βιομηχανία, αν όχι να αντιμετωπίσει άρδην το πρόβλημα των κυβερνοεπιθέσεων, τότε σίγουρα να το περιορίσει σε σημαντικό βαθμό.

2.1.1Λιμάνι της Αμβέρσας – Port of Antwerp[10]

Το λιμάνι της Αμβέρσας υπήρξε θύμα κυβερνοεπίθεσης, η οποία ξεκίνησε το 2011 και διήρκησε για χρονική περίοδο άνω των δύο ετών. Η συγκεκριμένη κυβερνοεπίθεση βρήκε έρεισμα στο σύστημα ηλεκτρονικής απελευθέρωσης των εμπορευματοκιβωτίων, γνωστό ως ERS, το οποίο χρησιμοποιήθηκε για πρώτη φορά στο λιμάνι της Αμβέρσας το 2005. Στην πράξη το ERS λειτουργούσε ως εξής· κάποιοι μεταφορείς, αντί φορτωτικών, έστελναν, μέσω emails, μοναδικούς ηλεκτρονικούς αριθμούς στους παραλήπτη, πράκτορα, αλλά και στον τερματικό λιμένα (pin codes), που αντιστοιχούσαν σε συγκεκριμένα εμπορευματοκιβώτια, και ήτο απαραίτητοι για την παραλαβή των εν λόγω εμπορευματοκιβωτίων από τις αποθήκες του τερματικού. Το 2011 μια ομάδα εισβολέων κατάφερε να παραβιάσει αυτό το σύστημα διαχείρισης των εμπορευματοκιβωτίων και να αποκτήσει πρόσβαση σε δεδομένα, τα οποία παρείχαν στους δράστες πληροφορίες σχετικά με την ακριβή θέση και την ασφάλεια των εμπορευματοκιβωτίων στο λιμάνι. Αυτό τους έδωσε τη δυνατότητα να κρύβουν μεταξύ των νόμιμων φορτίων λαθραία ναρκωτικά και όπλα και να τα διακινούν παράνομα στη χώρα. Οι

[10] Νομολογία για τη συγκεκριμένη υπόθεση παρατίθεται στο σκεπτικό της απόφασης του Εφετείου στην υπόθεση Glencore International AG κατά MSC Mediterranean Shipping Co SA [2017] EWCA Civ 365

αρχές αντιλήφθηκαν το λαθρεμπόριο, τον τρόπο που αυτό είχε στηθεί και την παραβίαση του κυβερνοχώρου, όταν οι δράστες, εξαιτίας του ότι δρούσαν ανενόχλητοι για μεγάλο χρονικό διάστημα, υπερεκτίμησαν τις δυνάμεις τους και αφαίρεσαν ολόκληρα εμπορευματοκιβώτια από τον τερματικό σταθμό της Αμβέρσας. Ανάλογες επιθέσεις πραγματοποιήθηκαν το έτος 2018 στα λιμάνια της Βαρκελώνης και του Σαν Ντιέγκο. Η υπόθεση αυτή, κατέδειξε ότι, τα μέτρα ασφαλείας που υπήρχαν στον κυβερνοχώρο του λιμανιού ήταν ανεπαρκή δημιουργώντας ένα περιβάλλον ευάλωτο, η παραβίαση του κυβερνοχώρου είχε ως απώτερο σκοπό την διάπραξη εγκλημάτων του κοινού ποινικού δικαίου και τέλος, κατέστησε σαφή την αναγκαιότητα για την άμεση θέσπιση μέτρων προστασίας του κυβερνοχώρου.

2.1.2BW Group

Μέσα σε διάστημα μικρότερο του ενός μήνα από την κυβερνοεπίθεση που δέχτηκε ο δανέζικος ναυτιλιακός κολοσσός Maersk, ακόμα μία εταιρία, η BW Group, έπεσε θύμα επιτήδειων χάκερς. Συγκεκριμένα, παραβιάστηκαν οι υπολογιστές στα γραφεία της εταιρίας στη Σιγκαπούρη με αποτέλεσμα η επικοινωνία της εταιρίας με τον έξω κόσμο να διακοπεί και να περιοριστεί μόνο σε μηνύματα ηλεκτρονικού ταχυδρομείου με παραλήπτες τους πελάτες και το πλήρωμα των πλοίων. Έγινε γνωστό από τον εκπρόσωπο της εταιρίας ότι η επίθεση αυτή δεν οφειλόταν σε κάποιο ransomware, ωστόσο δεν διευκρινίστηκε, αν κατά την κυβερνοεπίθεση εκλάπησαν οικονομικά στοιχεία ή δεδομένα της BW. Στη συνέχεια και όπως ήταν αναμενόμενο, το χρονικό διάστημα που ακολούθησε την επίθεση, η εταιρία προσπάθησε να λάβει τα κατάλληλα μέτρα προκειμένου να αποφευχθεί οποιαδήποτε παρόμοια κατάσταση στο μέλλον και να καλύψει τα υφιστάμενα κενά στο σύστημα κυβερνοασφάλειας της εταιρίας.

2.1.3 Clarkson PLC

Στις 29 Νοεμβρίου 2017 ο βρετανικός ναυλομεσιτικός οίκος, Clarkson PLC, με επίσημο δελτίο τύπου[11] επιβεβαίωσε μη εξουσιοδοτημένη πρόσβαση στο σύστημα υπολογιστών της εταιρίας στο Ηνωμένο Βασίλειο. Η παραβίαση που πραγματοποιήθηκε συνίστατο στην κλοπή των προσωπικών δεδομένων των πελατών, τα οποία περιελάμβαναν ημερομηνίες γέννησης,

[11] https://www.clarksons.com/media/1129201/notice_of_cyber_security_incident.pdf

στοιχεία διαβατηρίων, λογαριασμούς τραπεζών κλπ και στην απαίτηση καταβολής λύτρων για τη μη δημοσιοποίηση αυτών των δεδομένων. Μάλιστα, μετά από έρευνα των αρχών διαπιστώθηκε ότι η παραβίαση των συστημάτων προήλθε από ένα μοναδικό και απομονωμένο λογαριασμό χρήστη, ο οποίος στη συνέχεια απενεργοποιήθηκε. Το παράδοξο είναι ότι η παραβίαση των συστημάτων με την αντίστοιχη υποκλοπή των προσωπικών δεδομένων έγινε αντιληπτή στις 7 Νοεμβρίου 2017 ενώ αυτή συνέβαινε για χρονικό διάστημα 6 μηνών, ήτοι από τις 31 Μαΐου 2017 μέχρι τις 4 Νοέμβριου του ίδιου έτους.

Μετά την κυβερνοεπίθεση, η Clarkson PLC έκανε κάθε δυνατή προσπάθεια από πλευρά της για την ορθή διαχείριση της επίθεσης, προσπαθώντας συγχρόνως και να μην επηρεαστούν οι λειτουργίες της, αλλά και να προστατεύσει τους πελάτες της. Επίσης, φρόντισε για τη λήψη επιπρόσθετων μέτρων ασφάλειας προκειμένου να αποφευχθούν παρόμοια περιστατικά στο μέλλον και μελέτησε την επίθεση εις βάθος ώστε να ενισχύσει την κυβερνοασφάλεια της.

Το περιστατικό που συνέβη στον ναυλομεσιτικό οίκο καταδεικνύει ότι το ζήτημα των κυβερνοεπιθέσεων και της κυβερνοασφάλειας δεν αφορά μόνο τα πλοία, τα λιμάνια και τις ναυτιλιακές εταιρίες με τη στενή έννοια, αλλά επηρεάζει όλο το φάσμα της ναυτιλίας και της ναυτιλιακής οικονομίας (πλοία, ναυτιλιακές εταιρίες, λιμάνια, μεσίτες, ασφαλιστές, προμηθευτές και ναυλωτές) υπογραμμίζοντας ότι η αντιμετώπιση των κυβερνοεπιθέσεων και η εξεύρεση προληπτικών μέτρων προστασίας καθίστανται πιο επίκαιρες και αναγκαίες από ποτέ.

2.1.4 Cosco US

Στις 24 Ιουλίου 2018, οι δράστες των κυβερνοεπιθέσεων αύξησαν τη λίστα των θυμάτων τους, προσθέτοντας σε αυτήν, την Cosco Shipping Lines, καθώς παραβιάστηκαν οι λειτουργίες της εταιρίας στις Ηνωμένες Πολιτείες. Η εταιρία με ανακοίνωση, που ανήρτησε στη σελίδα της στο Facebook την επόμενη ημέρα της επίθεσης, ενημέρωσε τους πελάτες της ότι λόγω της επακόλουθης κατάρρευσης του δικτύου, τα συστήματα του τηλεφώνου υπολειτουργούσαν και η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου δε διεξαγόταν ομαλά στην ευρύτερη περιοχή που πραγματοποιήθηκε η επίθεση. Μάλιστα, για λόγους προστασίας, πρόληψης και περιορισμού της ζημιάς μόνο στις επιχειρήσεις της στην Αμερική, αναγκαστικά διέκοψε τη σύνδεση με τις υπόλοιπες περιοχές, ώστε να μην επηρεαστούν και τα δικά τους συστήματα από την επίθεση και επέλθει μια γενικευμένη κατάρρευση όλων των λειτουργιών. Επίσης, συνέπεια της συγκεκριμένης επίθεσης θεωρείτο και η περιορισμένης έκτασης δυσλειτουργία των εργασιών του τερματικού της, Pier J, στο λιμάνι του Long Beach.

Υπογραμμίστηκε δε από την εταιρία, πως όλα τα πλοία της λειτουργούν κανονικά χωρίς να έχουν επηρεαστεί από την επίθεση. Ο τρόπος που επανήλθε η εταιρία μετά το περιστατικό αποδεικνύει πως η Cosco βρισκόταν σε ετοιμότητα, είχε μελετήσει διεξοδικά την κυβερνοεπίθεση, που συνέβη στην Mærsk ένα χρόνο πριν, και προσπάθησε λαμβάνοντας τα κατάλληλα μέσα να ελαχιστοποιήσει τον κίνδυνο. Γι' αυτό το λόγο άλλωστε, κατέφερε να επαναφέρει όλες τις διαδικασίες της στην ομαλότητα και να επανέλθει σχεδόν στην κανονικότητα μία βδομάδα μετά το συμβάν. Σε αυτό βέβαια, συνέβαλε και το γεγονός ότι η συγκεκριμένη επίθεση δεν ήταν τόσο μεγάλη, επιβλαβής και επιζήμια όσο αυτή της δανέζικης εταιρίας Mærsk.

2.1.5 A.P. Møller – Mærsk

Το πιο γνωστό περιστατικό κυβερνοεπίθεσης στην ιστορία της ναυτιλίας έλαβε χώρα στις 27 Ιουνίου 2017 όταν η δανέζικων συμφερόντων εταιρία Mærsk «χτυπήθηκε» από ένα είδος κακόβουλου λογισμικού με την ονομασία NotPetya[12]. Η επίθεση στην εταιρία θεωρήθηκε ως παράπλευρη απώλεια στο πλαίσιο μια γενικευμένης κυβερνοεπίθεσης, η οποία εκ του αποτελέσματος απέδειξε ότι ακόμα και κάτω από αυτές τις συνθήκες, οι συνέπειες μιας κυβερνοεπίθεσης μπορεί να είναι ανυπολόγιστες. Συγκεκριμένα, η επίθεση επηρέασε όλες τις λειτουργίες της Mærsk σε παγκόσμιο επίπεδο, καθώς και τα τερματικά, τα οποία διαχειρίζεται, αφού 17 τερματικά της παραβιάστηκαν, δύο στο λιμάνι του Ρότερνταμ και 15 σε άλλα λιμάνια στον κόσμο. Τα τερματικά, λόγω των προβλημάτων που αντιμετώπιζε το πληροφορικό σύστημα της εταιρίας, υπολειτουργούσαν και μάλιστα κάποια από τα φορτία δεν παραδόθηκαν στους σωστούς προορισμούς. Τα πλοία της Mærsk μεταφέρουν περίπου το 20% του παγκόσμιου εμπορίου σε εμπορευματοκιβώτια, οπότε μπορεί να γίνει εύκολα αντιληπτή η δυσκολία που έχει να αντιμετωπίσει μία εταιρία τέτοιου βεληνεκούς, και ο αντίκτυπος που αναμενόμενα θα έχει στις δραστηριότητές της, όταν προσπαθεί να λειτουργήσει με παραβιασμένο σύστημα IT. Για την επαναφορά της εταιρίας στην προτεραία της κατάσταση χρειάστηκε να επαναγκαταστήσουν 4.000 καινούργιους servers, 45.000 νέους υπολογιστές και 2.500 εφαρμογές. Η ολική επανεγκατάσταση ολοκληρώθηκε μέσα σε 10 ημέρες, ενώ κάτι αντίστοιχο υπό φυσιολογικές συνθήκες χρειάζεται περίπου 6 μήνες.

[12] Κακόβουλο λογισμικό το οποίο εμποδίζει την πρόσβαση των ανθρώπων στα προσωπικά τους δεδομένα, μέχρι να καταβληθούν λύτρα $300 σε κρυπτονόμισμα (bitcoin)

Ο Jim Hagemann Snabe, πρόεδρος της A.P. Møller – Mærsk, ως ένας εκ των ομιλητών στο παγκόσμιο οικονομικό φόρουμ του 2017, μοιράστηκε τις σκέψεις του σχετικά με την κυβερνοασφάλεια και τα συμπεράσματα στα οποία κατέληξε ο ίδιος μέσα από την εμπειρία που βίωσε η εταιρία του.

1. Η συγκεκριμένη κυβερνοεπίθεση κατέδειξε ότι όλες οι εταιρίες, ανεξάρτητα από το μέγεθος και τη φήμη τους, υστερούν σε θέματα κυβερνοασφάλειας. Επομένως, το ζήτημα της κυβερνοασφάλειας, όχι μόνο πρέπει να είναι η πρώτη προτεραιότητα κάθε εταιρίας, αλλά και ν' αποτελεί ένα ανταγωνιστικό πλεονέκτημα για όσες την έχουν.

2. Από την πρώτη στιγμή του περιστατικού, η Mærsk, χωρίς να φοβηθεί για τον αντίκτυπο που μπορεί να έχει στη φήμη της, δημοσιοποίησε, μέσω του λογαριασμού της στο twitter, το περιστατικό της επίθεσης και ενημέρωνε σε τακτά χρονικά διαστήματα για τα βήματα της αποκατάστασης που ακολουθούσε, ώστε αυτό το γεγονός ν' αποτελέσει πηγή γνώσης για τις υπόλοιπες εταιρίες.[13] Όπως τόνισε και ο κ. Jim Hagemann Snabe, η εταιρία μέσω της δημοσιοποίησης της επίθεσης που υπέστη, προσπάθησε να μεταλαμπαδεύσει την εμπειρία της για να κατανοήσουν άπαντες το μέγεθος του προβλήματος, γιατί καμία εταιρία δεν πρέπει να αντιμετωπίζει με αφέλεια το ζήτημα της κυβερνοασφάλειας, καθώς όπως αποδείχθηκε, η πρόληψη είναι σημαντικότερη ακόμα και από την εκ των υστέρων άμεση αντίδραση σε μια κυβερνοεπίθεση!

Η επίθεση στην Mærsk κατέδειξε την ανάγκη προσαρμογής των εταιριών σε νέα δεδομένα, γιατί, όπως χαρακτηριστικά ανέφερε ο William P. Doyle[14] "Από τη στιγμή που η Mærsk έπεσε θύμα κυβερνοεπίθεσης, κάτι ανάλογο μπορεί να συμβεί σε οποιονδήποτε". Μάλιστα, η δημοσιοποίηση όλων των δεδομένων της επίθεσης από την A.P. Møller – Mærsk, θεωρήθηκε το πρώτο βήμα στην αλλαγή νοοτροπίας των εταιριών στο πως αντιλαμβάνονται τη φύση και τον αντίκτυπο του κυβερνοκίνδυνο. Σήμερα, όλες οι εταιρίες δείχνουν επισταμένη προσοχή στο ζήτημα της κυβερνοασφάλειας και εν όψει μάλιστα της έναρξης ισχύος του κανονισμού - MSC.428(98)[15], που επιβάλλει ο IMO από 1η Ιανουαρίου 2021 σε

[13] Η νομοθεσία που διέπει τη ναυτιλία δεν καθιστά αναγκαία τη δημοσιοποίηση περιστατικών που λαμβάνουν χώρα στον κυβερνοχώρο, σε αντίθεση με το νομικό πλαίσιο των αερομεταφορών, το οποίο καθιστά υποχρεωτική την αναφορά τέτοιων περιστατικών, ως μέτρο πρόληψης, προκειμένου να ανιχνεύονται παρόμοιοι κίνδυνοι, ικανοί να βλάψουν την ασφάλεια τους, όπως αυτό αναπτύσσεται εντός του Ευρωπαϊκού Κανονιστικού Πλαισίου (Regulation (EU) 2018/1139 και Regulation (EU) No 376/2014).

[14] τ. Επίτροπος του Ομοσπονδιακού Ναυτιλιακού Οργανισμού (Federal Maritime Organization).

[15]Οι εταιρείες πρέπει να αποδείξουν ότι η ασφάλεια στον κυβερνοχώρο αποτελεί αναπόσπαστο μέρος του συστήματος διαχείρισης της ασφάλειας τους, το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου

όλα τα πλοία στα οποία εφαρμόζεται ο ISM, έχουν ξεκινήσει να εισάγουν στη λειτουργία τους και αντίστοιχα μέτρα πρόληψης.

Επιπλέον, η συγκεκριμένη επίθεση στάθηκε η αφορμή για τη γέννηση πλήθος ερωτημάτων, σχετικά με την ασφαλιστική κάλυψη ή μη τέτοιων περιστατικών και με το ποιες ακριβώς είναι οι απορρέουσες από μια τέτοια επίθεση υποχρεώσεις των εμπλεκόμενων μερών. Μέχρι σήμερα, τα υφιστάμενα παραδοσιακά ασφαλιστικά προϊόντα δεν καλύπτουν τους κίνδυνους που προκαλούνται από κυβερνοεπιθέσεις και επομένως, η επικρατούσα κατάσταση, κατέστησε αναγκαία τη δημιουργία ενός καινούργιου προϊόντος στις ναυτασφαλίσεις, το οποίο γίνεται όλο και πιο απαραίτητο στις ναυτιλιακές εταιρίες.

2.2 Η ισχύουσα ρύθμιση για την κυβερνοασφάλεια από διεθνή όργανα

Υπό το πρίσμα της πρωτοφανούς κατάστασης που βιώνει η ναυτιλιακή βιομηχανία με την συνεχή αυξητική τάση των κυβερνοεπιθέσεων, η διεθνής ναυτιλιακή κοινότητα βρίσκεται σε διαρκή εγρήγορση για την έκδοση κατευθυντήριων οδών, συστάσεων και οδηγιών, οι οποίες θ’ αποτελέσουν τη βάση μελλοντικών διεθνών συνθηκών που θα ρυθμίζουν το ζήτημα της ασφάλειας στον κυβερνοχώρο. Εξάλλου, όπως είναι αναμενόμενο, η επικρατούσα κατάσταση, οι συνθήκες που συνεχώς αλλάζουν, τα νέα δεδομένα που προκύπτουν, η αέναη απειλή των κυβερνοεπιθέσεων και τα ερωτήματα που ανακύπτουν ως προς τον τρόπο αντιμετώπισης τους, γεννούν την ανάγκη για διεθνή και ενιαία ρύθμιση του ζητήματος.

2.2.1 IMO Guidelines – Ολοκληρωμένοι και χρήσιμοι οδηγοί από τον IMO

Οι κατευθυντήριες οδηγίες που εξεδόθησαν από τον IMO αποδεικνύουν πως η ναυτιλιακή βιομηχανία, παρά την χαλαρότητα με την οποία αντιμετώπισε αρχικά το ζήτημα των

συμμόρφωσης (DOC) και συγκεκριμένα από την 1η Ιανουαρίου 2021. Το πιστοποιητικό DOC εκδίδεται για την εταιρεία, μετά την διενέργεια αρχικής επιθεώρησης, από την αρμόδια αρχή ή εξουσιοδοτημένο οργανισμό, για να διαπιστωθεί η πλήρης συμμόρφωση της με τον ISM Code για το Σύστημα Ασφαλούς Διαχείρισης (ΣΑΔ/ΣΜΑ) το οποίο λειτουργεί και εφαρμόζεται για τρεις τουλάχιστον μήνες τόσο από την εταιρεία όσο και από κάθε τύπο πλοίου της εταιρείας. Η ισχύς του DOC είναι πέντε έτη και κατά την διάρκεια ισχύος του διενεργούνται ετήσιες επιθεωρήσεις κάθε 12 μήνες +03 μήνες από την επετειακή ημερομηνία λήξης του πιστοποιητικού. Για την ανανέωση του πιστοποιητικού DOC μετά τη λήξη του διενεργείται νέος έλεγχος και παύει να ισχύει, όταν δεν έχει γίνει μία από τις προβλεπόμενες υποχρεωτικές επιθεωρήσεις ή σε περίπτωση που έχει διαπιστωθεί σημαντική απόκλιση από τις απαιτήσεις του ISM Code. Το Document of Compliance ανήκει στα οριστικά ναυτιλιακά έγγραφα. (βλ. σημειώσεις στη «Λειτουργική Διαχείριση Πλοίου» - Α. Γκατζόλη)

κυβερνοεπιθέσεων, πλέον στέκεται με καχυποψία απέναντι στον αόρατο κίνδυνο και προσπαθεί με κάθε τρόπο να οργανωθεί και φυσικά να προστατευθεί από αυτόν. Ειδικότερα, τον Ιούνιο του 2016 ο ΙΜΟ δημοσίευσε το " *Interim Guidelines on Maritime Cyber Risk Management.*"[16] Όπως αναπτύσσεται στο ίδιο το κείμενο και συγκεκριμένα στο εισαγωγικό σημείωμα, ο σκοπός του είναι σαφής· να παράσχει συστάσεις αναφορικά με τη διαχείριση των κινδύνων στον κυβερνοχώρο ώστε να προφυλάξει τη ναυτιλία από τρέχουσες και μελλοντικές απειλές.

Οι προπαρασκευαστικές αυτές οδηγίες αντικαταστάθηκαν από ένα ολοκληρωμένο σχέδιο επιπρόσθετων οδηγιών, το "*Guidelines on Maritime Cyber Risk Management* "[17], το οποίο εξεδόθη από τον ΙΜΟ στις 5 Ιουλίου 2017. Τονίζοντας το πόσο αναγκαία είναι η τεχνολογία για την ορθή λειτουργία συστημάτων, τα οποία σχετίζονται με την ασφαλή ναυσιπλοΐα και την προστασία του θαλάσσιου περιβάλλοντος, ο ΙΜΟ προσπάθησε να αναδείξει τη σημασία και την αναγκαιότητα για επαρκή και αποτελεσματική διαχείριση του κυβερνοκινδύνου από τις εταιρίες, το λεγόμενο δηλαδή cyber risk management[18]. Σκοπός του ΙΜΟ είναι να δώσει ένα γενικό πλαίσιο και όχι να προτείνει συγκεκριμένους τρόπους εφαρμογής των οδηγιών αυτών, καθώς κάθε εταιρία έχει διαφορετικές ανάγκες και θα πρέπει να ορίσει η ίδια τα μέτρα που θα λάβει, προκειμένου να διαχειριστεί τους κινδύνους και να διασφαλίσει την κυβερνοασφάλεια της.

Στην τελική διαμόρφωση του "*Guidelines on Maritime Cyber Risk Management*", όπως αναφέρεται στο προοίμιό του, έπαιξε καθοριστικό ρόλο εκτός από το MSC.1/Circ.1526 και το έγγραφο με τίτλο"*Measures to Enhance Maritime Security*"[19], που υποβλήθηκε από τις Ηνωμένες Πολιτείες της Αμερικής στις 4 Απριλίου 2017 κατά την 98^{η} συνεδρίαση της Επιτροπής Θαλάσσιας Ασφάλειας.

Το ανωτέρω έγγραφο, αφού επισημαίνει ότι η ανεπαρκής κυβερνοασφάλεια μπορεί να θέσει σε κίνδυνο την ασφάλεια του πλοίου, συστήνει ως τρόπο αντιμετώπισης μία ολιστική διαχείριση κινδύνων, η οποία να περιλαμβάνει συν των υπολοίπων κινδύνων και τους κινδύνους στον κυβερνοχώρο. Επομένως, προτείνει να ενσωματωθεί η διαχείριση των

[16] MSC.1/Circ.1526

[17] MSC-FAL.1/Circ.3

[18] Cyber risk management: the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level by taking into consideration the costs and benefits of actions taken by stakeholders (βλ. The Guidelines on Cyber Security on board ships Version 3 – Annex 4: Glossary)

[19] MSC 98/5/2

κινδύνων στον κυβερνοχώρο στο ήδη υπάρχον σύστημα ασφαλείας του πλοίου και της εταιρίας, και αυτό γιατί οι συγκεκριμένοι κίνδυνοι θεωρούνται λειτουργικοί, αφού επιδρούν στη βιωσιμότητα της εκάστοτε επιχείρησης, και ως τέτοιοι πρέπει να αντιμετωπίζονται. Με βάση αυτό, η αξιολόγηση και η διαχείριση των κυβερνοκινδύνων θα πρέπει να γίνεται σύμφωνα με όσα ορίζει ο Διεθνής Κώδικας Διαχείρισης Ασφάλειας (International Safety Management Code– ISM)[20].

Το MSC 98/5/2, το MSC.1/Circ.1526 και το MSC-FAL.1/Circ.3 έθεσαν γερά θεμέλια για την ενίσχυση της κυβερνοασφάλειας και η συμβολή τους θα μπορούσε να χαρακτηριστεί από τη ναυτιλιακή βιομηχανία ως το πρώτο βήμα στην αντιμετώπιση των κυβερνοεπιθέσεων.

2.2.2 Ο Διεθνής Κώδικας Ασφαλούς Διαχείρισης (ISM Code)

Λαμβάνοντας υπόψη το MSC-FAL.1/Circ.3 και το MSC.1/Circ.1526, η Επιτροπή Θαλάσσιας ασφάλειας υιοθέτησε στις 16 Ιουνίου 2017 το ψήφισμα MSC.428(98) υπό τον τίτλο " *Maritime Cyber Risk Management in Safety Management Systems*". Το συγκεκριμένο ψήφισμα ορίζει ότι η διαχείριση των κινδύνων στον κυβερνοχώρο πρέπει να γίνεται σύμφωνα με τους στόχους και τις απαιτήσεις του Διεθνούς Κώδικα Διαχείρισης της Ασφάλειας (ISM code) και να ενσωματώνεται στα ήδη υπάρχοντα σύστημα ασφαλούς διαχείρισης (Safety Management Systems – SMS), καθιστώντας το τελευταίο υποχρεωτικό για όλες τις ναυτιλιακές εταιρίες. Το ψήφισμα απαιτεί από τις εταιρίες να αποδείξουν ότι η ασφάλεια στον κυβερνοχώρο αποτελεί αναπόσπαστο μέρος του συστήματος διαχείρισης της ασφάλειας τους, το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης (DOC) που θα λάβει χώρα από την 1η Ιανουαρίου 2021 και έπειτα. Μετά την 1η Ιανουαρίου 2021, σε περίπτωση ελέγχου στα λιμάνια, τα πλοία που δεν έχουν συμμορφωθεί με το ανωτέρω ψήφισμα, αντιμετωπίζουν κυρώσεις και μπορεί ακόμα και να κρατηθούν.

Για να συμμορφωθεί με τις οδηγίες του IMO και να πράξει ό,τι ορίζει το ψήφισμα, κάθε εταιρία θα πρέπει να κινηθεί σε τρεις κατευθύνσεις και να πραγματοποιήσει σωρευτικά τα κάτωθι:

1. Να ορίσει ρόλους, αρμοδιότητες και ευθύνες στα μέλη του προσωπικού, είτε αυτά βρίσκονται στη ξηρά είτε σε πλοία. Με λίγα λόγια, να τους εκπαιδεύσει, ώστε να είναι εξοικειωμένοι με τους κινδύνους στον κυβερνοχώρο και να γνωρίζουν τι ακριβώς θα πρέπει να πράξουν όταν βρεθούν αντιμέτωποι με μια κυβερνοαπειλή. Όπως προβλέπονται και

[20] https://safety4sea.com/wp-content/uploads/ISM-Code/ISM%20Code%202015%20with%20cover.pdf

ακολουθούνται συγκεκριμένες διαδικασίες σε περιπτώσεις έκτακτης ανάγκης[21] πχ σε περίπτωση σύγκρουσης ή πυρκαγιάς, και κάθε μέλος του προσωπικού της εταιρείας ή του πλοίου γνωρίζει ακριβώς τις ενέργειες που πρέπει να πράξει ή να αποφύγει, έτσι και στη συγκεκριμένη περίπτωση το πλήρωμα πρέπει να είναι κατάλληλα προετοιμασμένο και εκπαιδευμένο προκειμένου να αντιμετωπίσει μια κυβερνοεπίθεση. Μία έρευνα που πραγματοποιήθηκε το 2018 κατέδειξε την ανάγκη ευαισθητοποίησης των μελών του πληρώματος, καθώς, παρά το γεγονός, ότι το 47% των ερωτηθέντων απάντησαν ότι βρέθηκαν κάποια στιγμή σε πλοίο, το οποίο έγινε στόχος επίθεσης στον κυβερνοχώρο, μόνο το 15% εξ αυτών είχε λάβει οποιαδήποτε μορφή εκπαίδευσης σχετικά με την ασφάλεια του κυβερνοχώρου, ποσοστό ιδιαίτερα μικρό. Επομένως, είναι απαραίτητο να γίνει κατανοητό ότι η κυβερνοασφάλεια δεν είναι απλώς ζήτημα του IT τμήματος μιας εταιρίας, αλλά θα πρέπει να θεωρείται μέρος της συνολικής ασφάλειας του πλοίου, αναπόσπαστο κομμάτι της αξιοπλοΐας του και της συνέχειας των λειτουργιών της εταιρίας και ως τέτοια θα πρέπει να αντιμετωπίζεται. Άρα είναι απολύτως σημαντική, τόσο η ενημέρωση και η εκπαίδευση όλων των εμπλεκομένων προσώπων, η οποία ξεκινάει από τα στελέχη της ανώτερης διοίκησης και φτάνει μέχρι το πλήρωμα του πλοίου, όσο και ο σωστός σχεδιασμός, που θα εξασφαλίσει ετοιμότητα στην αντιμετώπιση και διαχείριση μιας κρίσης. Αυτά δύναται να επιτευχθούν μέσω κατάλληλων προγραμμάτων κατάρτισης και ευαισθητοποίησης του προσωπικού

2. Να προσδιορίσει με ακρίβεια ποια είναι τα πιο ευαίσθητα συστήματα ενός πλοίου, τα οποία αν προσβληθούν από κάποιον κυβερνοκίνδυνο, θα διαταράξουν τις λειτουργίες του.

3. Να είναι σε θέση να εκτιμήσει το μέγεθος του κινδύνου και να διαμορφώσει ένα σχέδιο έκτακτης ανάγκης (real time monitoring response) για να μειωθεί όσο γίνεται ο αντίκτυπος της επίθεσης. Αν πραγματοποιηθεί μία κυβερνοεπίθεση, η εταιρία πρέπει να έχει οργανωθεί με τέτοιο τρόπο ώστε να μην «παραλύσει»! Πρέπει να έχει εφαρμόσει τέτοια τεχνικά και διαδικαστικά μέτρα, τα οποία θα της διασφαλίσουν τη συνέχεια των εργασιών της σε περίπτωση που συμβεί κάποιο αναπάντεχο περιστατικό.

Γενικά, η ομαλή ενσωμάτωση των μέτρων στο υπάρχον Σύστημα Διαχείρισης Ασφάλειας είναι μια σημαντική εργασία που απαιτεί χρόνο και μεγάλο κεφάλαιο για να ολοκληρωθεί αποτελεσματικά.

Ιδιαίτερο ενδιαφέρον θα έχει να δούμε πως η θαλάσσια ασφάλιση θα αντιμετωπίσει στο μέλλον το ζήτημα του νέου ψηφίσματος και της ενσωμάτωσης του στο SMS, καθώς γεννάται

[21] βλ. την 8η ενότητα του ISM code " EMERGENCY PREPAREDNESS"

μια σειρά διαδοχικών ερωτημάτων. Για παράδειγμα, μια ασφαλιστική εταιρία θα ασφαλίσει ένα πλοίο, το οποίο διαχειρίζεται ανεπαρκώς τους κυβερνοκινδύνους; Μια εταιρία, η οποία δεν έχει εκπαιδεύσει κατάλληλα το πλήρωμά της όσον αφορά το ζήτημα της κυβερνοασφάλειας, θα μπορεί ν' ασφαλίσει το πλοίο της; Και αν παρόλα αυτά υποθέσουμε ότι ασφαλίζεται το συγκεκριμένο πλοίο και πραγματοποιείται μια κυβερνοεπίθεση και τελικά διαπιστώνεται ότι το σύστημα διαχείρισης των κυβερνοκινδύνων που ακολουθούνταν ήταν ελλιπές, τι θα γίνει όσον αφορά την προκληθείσα ζημία;

2.2.3 The Guidelines on Cyber Security Onboard Ships

Το *"Guidelines on Maritime Cyber Risk Management"* στην ενότητα 4 παραπέμπει τους χρήστες, που αναζητούν επιπρόσθετες και πιο λεπτομερείς οδηγίες σχετικά με τη διαχείριση των κυβερνοκινδύνων, σε επιπλέον εγχειρίδια ώστε να εμβαθύνουν περισσότερο στο εν λόγω ζήτημα. Ένας πολύ χρήσιμος οδηγός είναι το "*The Guidelines on Cyber Security Onboard Ships*".

Οι σημαντικότεροι διεθνείς οργανισμοί της ναυτιλίας ένωσαν τις δυνάμεις τους και επανεξέδωσαν το 2017 την 3η έκδοση του "*The Guidelines on Cyber Security Onboard Ships*", το οποίο συμβαδίζει πάντα με τις οδηγίες του IMO. Σκοπός του είναι, αναλύοντας όλα τα δεδομένα και παρέχοντας στους αναγνώστες του μια πλήρη εικόνα για το τι ακριβώς είναι ο κίνδυνος στον κυβερνοχώρο, να βοηθήσει τις εταιρίες ν' αναπτύξουν το καταλληλότερο γι' αυτές cyber risk management. Το "*The Guidelines on Cyber Security Onboard Ships*", το οποίο έχει γίνει ευρέως αποδεκτό από τον IMO, τους εφοπλιστές και τους νηογνώμονες, αναφέρεται κυρίως στον τρόπο διαχείρισης των κυβερνοκινδύνων στα πλοία. Οι οδηγίες που δίνει το συγκεκριμένο κείμενο έχουν κατ' εξοχήν συμβουλευτικό χαρακτήρα και σε καμία περίπτωση δεν υποχρεώνεται κάποιος να τις ενστερνιστεί και να συμμορφωθεί με αυτές.

Όλος ο οδηγός βασίζεται στη σωστή ανάπτυξη, εφαρμογή και διατήρηση του cyber risk management, το οποίο είναι το τρέχον ζήτημα που απασχολεί τις εταιρίες. Γι' αυτό το λόγο, στην αρχή παρουσιάζει τα βήματα που πρέπει να γίνουν για να επιτευχθεί μια, όσο γίνεται, πιο ολοκληρωμένη διαχείριση των κυβερνοκινδύνων. Σύμφωνα με τον οδηγό τα βήματα είναι τα εξής: προσδιορισμός των κινδύνων, προσδιορισμός των τρωτών σημείων, εκτίμηση της έκθεσης σε κίνδυνο, ανάπτυξη μέτρων προστασίας και ενίσχυσης, δημιουργία σχεδίων για ελαχιστοποίηση των κυβερνοκινδύνων σε μια ενδεχόμενη απειλή και τέλος σχεδιασμός

απόκρισης και ανάρρωσης από ενδεχόμενα περιστατικά που κλονίζουν την κυβερνοασφάλεια.

Αυτό που μετατρέπει όμως, το "*The Guidelines on Cyber Security Onboard Ships*" από έναν απλό οδηγό σ' ένα πραγματικά χρήσιμο εργαλείο για όποιον θέλει να κατανοήσει το πολύπλοκο ζήτημα των κυβερνοεπιθέσεων είναι ότι προσδιορίζει τα είδη των κυβερνοεπιθέσεων, τα είδη των δραστών και τα κίνητρά τους, τα συστήματα που μπορούν εύκολα να προσβληθούν από έναν κυβερνοκίνδυνο και τέλος, κατονομάζει τους στόχους μιας κυβερνοεπίθεσης προσδιορίζοντας συγχρόνως τις ζημιές και τις απώλειες που μπορεί αυτή να προκαλέσει. Αυτές οι πληροφορίες μπορούν να φανούν πολύ χρήσιμες και στη θαλάσσια ασφάλιση για τη σωστή εκτίμηση των κινδύνων (risk assessment).

Τέλος, να σημειωθεί ότι το "*The Guidelines on Cyber Security Onboard Ships*" έχει μεγάλη αξία και για έναν ακόμη λόγο· είναι το πρώτο κείμενο που συντάχθηκε από φορείς της ναυτιλίας, οι οποίοι αντιπροσωπεύουν όσους ασχολούνται με τη ναυτιλία σε επαγγελματικό επίπεδο. Δείχνει επομένως, με ποιον τρόπο σκοπεύει ν' αντιδράσει η βιομηχανία της ναυτιλίας απέναντι σ' αυτούς τους κινδύνους.

Τον Οκτώβριου του 2020 το Διεθνές Ναυτιλιακό Επιμελητήριο (International Chamber of Shipping – ICS) και η BIMCO σε συνεργασία με τον εκδοτικό οίκο Witherby εξέδωσαν το " *Cyber Security Workbook for On Board Ship Use*", ως μια πιο επικαιροποιημένη έκδοση του προηγούμενου εγχειριδίου. Η ψηφιακή επανάσταση και η στοχοποίηση των πλοίων από τους χάκερς έχει κάνει πιο επιτακτική από ποτέ την ανάγκη της ουσιαστικής κατανόησης από τα πληρώματα τι είναι πραγματικά ο κίνδυνος στον κυβερνοχώρο αλλά και με ποιον τρόπο και σε ποιο χρονικό σημείο μπορεί να γίνει μια κυβερνοεπίθεση. Επομένως, ο συγκεκριμένος οδηγός σχεδιάστηκε, σαν υποστηρικτικό εργαλείο, με σκοπό να παράσχει στον πλοίαρχο, τους αξιωματικούς, τον υπεύθυνο ασφαλείας και τα λοιπά μέλη του πληρώματος, τις πρακτικές δεξιότητες για τον εντοπισμό των κινδύνων και για την προστασία των ευάλωτων συστημάτων του πλοίου. Επίσης, παρουσιάζει ποιος είναι ο καλύτερος τρόπος ανίχνευσης, ανταπόκρισης και ανάκαμψης στην περίπτωση μιας κυβερνοεπίθεσης. Το " *Cyber Security Workbook for On Board Ship Use*" έχει σκοπό να αποτελέσει έναν χρήσιμο, πρακτικό και κατανοητό οδηγό για όλη τη ναυτιλιακή κοινότητα εν όψει της επικείμενης εφαρμογής του ψηφίσματος MSC.428(98).

2.2.4 ISO/IEC 27001 standard on Information technology

Ένα άλλο εργαλείο στο οποίο παραπέμπει ο ΙΜΟ μέσω των οδηγιών του είναι το "*ISO/IEC 27001 standard on Information technology"* το οποίο δημοσιεύθηκε από το Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization – ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnica Commission – IEC). Το *ISO/IEC27001*θέτει τα προαπαιτούμενα για ένα πρότυπο σύστημα διαχείρισης ασφάλειας των πληροφοριών (Information Security Management System – ISMS). Το ISMS είναι ένας τρόπος για να διαχειρίζονται οι εταιρίες ευαίσθητα προσωπικά δεδομένα, όπως πληροφορίες των υπαλλήλων και εμπιστευτικές πληροφορίες που έχουν δοθεί σε τρίτα μέρη, και συγχρόνως να εγγυώνται για την ασφάλειά τους.

Αυτά τα πρότυπα είναι σημαντικά και χρήσιμα για τις ναυτιλιακές εταιρίες και τα πλοία, αφού με αυτόν τον τρόπο θα μπορέσουν να διατηρήσουν ασφαλείς τις πληροφορίες π.χ. προσωπικά δεδομένα υπαλλήλων, πληρωμάτων και επιβατών.

2.2.5 Ο Ευρωπαϊκός Κανονισμός για την Προστασία Προσωπικών Δεδομένων – General Data Protection Regulation (GDPR)[22]

Μέσα στα όρια της Ευρωπαϊκής Ένωσης, οι εταιρίες είναι υποχρεωμένες, πλην των ανωτέρω οδηγιών, να συμμορφώνονται στο πλαίσιο της κυβερνοασφάλειας και μ' έναν επιπλέον κανονισμό, το πολυσυζητημένο GDPR. Το GDPR, η εφαρμογή του οποίου τέθηκε σε ισχύ για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου του 2018, αφορά την προστασία και την επεξεργασία προσωπικών δεδομένων. Το GDPR επηρεάζει και τη ναυτιλία, καθώς πλοιοκτήτες και εφοπλιστές είναι υποχρεωμένοι να συμμορφωθούν με τον Κανονισμό, που αυστηροποιεί το πλαίσιο νομιμότητας της επεξεργασίας προσωπικών δεδομένων με τον τρόπο που ορίζεται στα άρθρα του, διαφορετικά κινδυνεύουν να αντιμετωπίσουν την επιβολή ιδιαίτερα αυστηρών διοικητικών προστίμων[23]. Επομένως, είναι αναγκασμένοι να συγκεντρώνουν και να τηρούν στα αρχεία τους τα προσωπικά δεδομένα των

[22] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016

[23] Άρ.83 §5 του 2016/679 Ευρωπαϊκού Κανονισμού «*Παραβάσεις των ακόλουθων διατάξεων επισύρουν, σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 20.000.000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο*».

υπαλλήλων τους με ιδιαίτερη προσοχή, χωρίς να τα επεξεργάζονται και χωρίς να τα γνωστοποιούν σε τρίτους άνευ της συγκατάθεσής τους. Με τον όρο προσωπικά δεδομένα νοείται κάθε προσωπική πληροφορία, η οποία μπορεί να οδηγήσει με ακρίβεια, είτε άμεσα είτε έμμεσα, στην ταυτοποίηση του προσώπου.

Μεγαλύτερη ευθύνη απέναντι στον GDPR φέρουν οι ναυτιλιακές εταιρίες κρουαζιέρας, οι οποίες συγκεντρώνουν και αποθηκεύουν προσωπικά δεδομένα εκατοντάδων επιβατών. Τα στοιχεία αυτά, τα οποία αποθηκεύονται ηλεκτρονικά στη βάση δεδομένων της εκάστοτε εταιρίας, μπορεί να περιλαμβάνουν αριθμό ταυτότητας / διαβατηρίου, ημερομηνία γέννησης, διεύθυνση κατοικίας, ιστορικό ασθενείας, και αριθμούς τραπεζικών καρτών προκειμένου να ολοκληρωθεί μια κράτηση. Η αποθήκευσή τους κατ' αυτόν τον τρόπο, αμέσως τα καθιστά έναν εν δυνάμει στόχο κυβερνοεπίθεσης. Επιτήδειοι χάκερς ανά πάσα χρονική στιγμή μπορούν ν' αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα αρχεία της εταιρίας και να υποκλέψουν αυτά τα δεδομένα με ό, τι αυτό συνεπάγεται, κακή δημοσιότητα για την εταιρία, δικαστικές διαμάχες με αντικείμενο αξιώσεις αποζημίωσης, αναζήτηση ποινικών ευθυνών, πρόστιμα κ.α Από τα ανωτέρω προκύπτει σαφής σύνδεση της κυβερνοασφάλειας με το GDPR τονίζοντας για μια ακόμη φορά την αναγκαιότητα της ενσωμάτωσής της στα συστήματα ασφαλείας.

Δέον να προστεθεί ότι η εναρμόνιση με τον Ευρωπαϊκό Κανονισμό για το GDPR και οι κυρώσεις που επιφέρει σε περίπτωση μη συμμόρφωσης με αυτόν, αφορούν κάθε εταιρία, ανεξάρτητα από το αν η έδρα της δε βρίσκεται σε έδαφος κράτους – μέλους της ΕΕ, εφόσον τα προσωπικά δεδομένα που συλλέγει αφορούν ευρωπαίο πολίτη. Αυτό σημαίνει ότι δεν πρέπει να υπάρχει εφησυχασμός και κάθε εταιρία πρέπει να είναι προσεχτική για την ασφαλή φύλαξη και διατήρηση προσωπικών δεδομένων στα αρχεία της.

Ωστόσο, η εφαρμογή και η ισχύς των ανωτέρω οδηγιών δεν έχει επιφέρει ακόμα κάποια ουσιαστική λύση. Το πρόβλημα των κινδύνων στον κυβερνοχώρο εξακολουθεί να υφίσταται, γιατί, τόσο η νομοθεσία όσο και το νομικό καθεστώς που διέπει τη θαλάσσια ασφάλιση, δυσκολεύονται στην πραγματικότητα να συμβαδίσουν με τις εξελίξεις στην τεχνολογία που επηρεάζουν κατά κόρον τη ναυτιλιακή βιομηχανία. Μέχρι στιγμής δεν υφίσταται κάποια διεθνής συνθήκη στο πλαίσιο της οποίας να περιλαμβάνεται η κυβερνοασφάλεια και κατ' επέκταση δεν υπάρχει και υποχρεωτική ασφαλιστική κάλυψη για τις κυβερνοεπιθέσεις.

Κεφάλαιο 3. Η Θαλάσσια Ασφάλιση

3.1 Οι κυβερνοεπιθέσεις μια νέα πρόκληση για τη θαλάσσια ασφάλιση

Έχει καταστεί σαφές ότι το ζήτημα των κυβερνοεπιθέσεων έχει θορυβήσει τη ναυτιλιακή βιομηχανία και η κυβερνοασφάλεια αποτελεί θέμα πρωτίστης σημασίας για όλες τις εταιρίες του κλάδου. Όπως είναι λογικά επόμενο, το συγκεκριμένο ζήτημα και η αντιμετώπισή του έχει προκαλέσει έντονη ανησυχία και στις αποκλειστικά υπεύθυνες, για κάθε είδους ζημία ή απώλεια, εταιρίες, ήτοι τις ασφαλιστικές εταιρίες, αντασφαλιστικές και τα P&I clubs.

Στο πλαίσιο αυτό, αρχικά θα πρέπει να διευκρινίσουμε ότι οι ασφαλιστές προκειμένου να είναι σε θέση να προτείνουν εργαλεία για την αντιμετώπιση των κυβερνοκινδύνων, αυτή τη στιγμή εργάζονται στην κατεύθυνση του να κατανοήσουν καλύτερα τι είναι ο κυβερνοκίνδυνος. Πώς ορίζεται όμως, από τον κλάδο των ναυτασφαλίσεων, ο κυβερνοκίνδυνος; Χρήσιμο προς τούτο εργαλείο, είναι οι ορισμοί που έχουν δοθεί κατά καιρούς για τις κυβερνοεπιθέσεις και τους κυβερνοκινδύνους από τα διάφορα P&I Clubs και τους ναυτιλιακούς οργανισμούς, οι σημαντικότεροι εκ των οποίων παρατίθενται κάτωθι[24]:

NORTH P&I club: Κυβερνοκίνδυνος μπορεί να είναι η αποτυχία ενός δέκτη GPS που βρίσκεται στο πλοίο, λόγω κάποιας βλάβης του εξοπλισμού, η οποίο μπορεί να επεκταθεί και στα λοιπά συστήματα του πλοίου με αποτέλεσμα να μη μπορεί αυτό να λειτουργήσει σωστά ή ακόμα και να καταληφθεί από κακόβουλα τρίτα μέρη (πειρατεία).[25]

UK P&I club: Ο κίνδυνος στον κυβερνοχώρο ορίζεται ως ο κίνδυνος της απώλειας ή της ζημίας ή της διακοπής πρόσβασης στα ηλεκτρονικά συστήματα και στα τεχνολογικά δίκτυα.[26]

JAPAN P&I club: Ο κίνδυνος στον κυβερνοχώρο ορίζεται ως πιθανός παράγοντας, ο οποίος μπορεί να προκαλέσει προβλήματα ή να επηρεάσει το σύστημα IT και που μπορεί ακόμη και να προκαλέσει, εκτός από δυσλειτουργία στην εκτέλεση των καθηκόντων και οικονομική καταστροφή στην εταιρία. Ο κυβερνοκίνδυνος πηγάζει τόσο από εξωτερικούς όσο και από εσωτερικούς παράγοντες. [27]

[24] Σε ελεύθερη μετάφραση από την αγγλική στην ελληνική γλώσσα

[25] βλ. Cyber Risks in Shipping – The North of England P&I Association (July 2017)

[26] βλ. Cyber Risks and P&I insurance – UK P&I club Q&A document (March 2018)

[27] βλ. P&I Loss Prevention Bulletin – Japan P&I club (Vol.42, May 2018)

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL: Κυβερνοεπίθεση είναι κάθε είδος επιθετικού τεχνάσματος, που στοχεύει στα IT και OT συστήματα, στα δίκτυα υπολογιστών ή στις προσωπικές συσκευές των υπαλλήλων και επιδιώκει να καταστρέψει ή να αποκτήσει πρόσβαση στα συστήματα και τα δεδομένα της εταιρίας και του πλοίου. [28]

Για μία εις βάθος κατανόηση των κυβερνοκινδύνων, συμπληρωματικά των ανωτέρω, θα πρέπει να αναφερθούν και οι επιπτώσεις μιας κυβερνοεπίθεσης προκειμένου να προσδιοριστεί το ακριβές πλαίσιο στο οποίο θα πρέπει να κινηθεί η αγορά των ναυτασφαλίσεων αλλά και το αντικείμενο που θα ασφαλίσει. Οι επιπτώσεις των κινδύνων στον κυβερνοχώρο, αν και δε θα έπρεπε, πολύ συχνά υποτιμούνται. Όπως προκύπτει, το φάσμα των πιθανών απωλειών ή ζημιών που επακολουθούν ενός συμβάντος στον κυβερνοχώρο είναι ευρύ και μπορεί να περιλαμβάνει πέρα από τις προφανείς ζημίες, όπως είναι η απώλεια των δεδομένων και η προσωρινή διακοπή των λειτουργιών μιας εταιρίας, και πιο δυσδιάκριτες, οι οποίες σχετίζονται με σωματικούς τραυματισμούς του εργατικού δυναμικού αλλά και με τη δυσφήμιση των εταιριών, απότοκη της επίθεσης. Είναι πολύ σημαντικό να αναλυθούν και να κωδικοποιηθούν οι επιπτώσεις μιας κυβερνοεπίθεσης, γιατί ό,τι πλήττεται είναι τελικά αυτό που ασφαλίζεται, δηλαδή το αντικείμενο της ασφαλιστικής κάλυψης.

3.2 Η Θαλάσσια Ασφαλιστική πράξη 1906 / Marine Insurance Act 1906

Από την ανάλυση αυτού του ζητήματος δε θα μπορούσε να λείπει και μία αναφορά στην πρώτη νομοθεσία που εφαρμόστηκε ποτέ στη θαλάσσια ασφάλιση και συγκεκριμένα στη Marine Insurance Act 1906[29], η οποία έθεσε τις βασικές αρχές για τη θαλάσσια ασφάλιση σε όλο τον κόσμο. Η μεγαλύτερη πρόκληση που τίθεται επί του ζητήματος είναι εάν οι κυβερνοκίνδυνοι και η κυβερνοασφάλεια θα μπορούσαν να συμμορφωθούν με τις αρχές και του κανόνες της MIA 1906, εάν δηλαδή μπορεί η θαλάσσια ασφάλιση να ενσωματώσει τον κυβερνοκίνδυνο στους λοιπούς θαλάσσιους κινδύνους και να τον αντιμετωπίσει ως τέτοιον. Μόνο καινοτόμες τροποποιήσεις στις ήδη υπάρχουσες ασφαλιστικές πράξεις, θα μπορέσουν ν' αλλάξουν ριζικά τον τρόπο που αντιμετωπίζει η θαλάσσια ασφάλιση τις κυβερνοεπιθέσεις.

[28] βλ. The Guidelines on Cyber Security on board ships Version 3 – Annex 4: Glossary

[29] Η Marine Insurance Act που τέθηκε σε ισχύ την 1η Ιανουαρίου του 1907, δεν έφτιαξε νέους νόμους ,αλλά κωδικοποίησε τις ήδη υπάρχουσες νομικές αποφάσεις που είχαν καταγραφεί μέχρι τότε

Αρχικά, για να κατανοήσουμε τη θαλάσσια ασφάλιση, θα πρέπει να γίνει μια αναφορά στην ενότητα 1 της MIA 1906 στην οποία ορίζεται η θαλάσσια ασφάλιση. Σύμφωνα με την οποία «*Ένα συμβόλαιο θαλάσσιας ασφάλισης είναι ένα συμβόλαιο με το οποίο ο ασφαλιστής αναλαμβάνει να αποζημιώσει τον ασφαλισμένο, με τον τρόπο και στο βαθμό που έχει συμφωνηθεί, έναντι των θαλάσσιων απωλειών, δηλαδή των ζημιών που λαμβάνουν χώρα κατά τη θαλάσσια περιπέτεια*». Αυτό που μένει να εξετάσουμε είναι κατά πόσο μπορεί να «διευρυνθεί» το συμβόλαιο θαλάσσιας ασφάλισης ώστε να περιλάβει και τους κινδύνους στον κυβερνοχώρο.

Στο πολύ σημαντικό άρθρο 5 της Marine Insurance Act προσδιορίζεται το ασφαλιστικό συμφέρον, πρώτα με γενικούς όρους και στη συνέχεια με πιο συγκεκριμένους. Αναλυτικότερα «*σύμφωνα με τις διατάξεις της παρούσας νομοθετικής πράξης, ασφαλιστικό συμφέρον έχει οποιοσδήποτε έχει συμφέρον πάνω σε μία θαλάσσια αποστολή*» (αρ. 5 §1). Προκύπτει ότι το ασφαλιστικό συμφέρον ταυτίζεται με το οικονομικό συμφέρον που έχει κάποιος στην περιουσία που ασφαλίζεται, στο βαθμό που, αν η περιουσία μείνει ανασφάλιστη, υποστεί ζημία ή καταστραφεί ολοσχερώς, ο ιδιοκτήτης θα πρέπει να βρει τα χρήματα από ιδίους πόρους προκειμένου να αποκαταστήσει ή αντικαταστήσει τη ζημία. Ουσιαστικά δεν ασφαλίζεται το πράγμα αλλά η οικονομική σχέση ενός προσώπου προς ένα αγαθό, η οποία συνιστά και το ασφαλιστικό συμφέρον. Παρομοίως, κάποιος μπορεί να ευθύνεται και για ζημία που προκλήθηκε στην περιουσία κάποιου άλλου[30]. Στη συνέχεια στην § 2 διευκρινίζει «*ένα πρόσωπο έχει συμφέρον στη θαλάσσια αποστολή όταν βρίσκεται σε νόμιμη ή καλής πίστεως σχέση προς την αποστολή ή την ασφαλιστέα υπό κίνδυνο περιουσία και συνεπώς μπορεί να ευνοηθεί από την ασφαλή ή οφειλόμενη άφιξη της ασφαλιστέας περιουσίας ή να ζημιωθεί από την απώλεια, βλάβη ή κράτηση αυτής ή μπορεί να προκληθεί ευθύνη του σε σχέση μ' αυτήν*». Πρακτικά αυτό σημαίνει ότι τα άτομα, τα οποία έχουν νόμιμη ή καλής πίστεως σχέση με τη θαλάσσια αποστολή ή με την οποιαδήποτε ασφαλισμένη περιουσία που βρίσκεται σε κίνδυνο, μπορούν να χωριστούν σε 3 κύριες κατηγορίες: *α.* ο ιδιοκτήτης της ασφαλισμένης περιουσίας είτε αφορά πλοίο, είτε φορτίο, είτε ναύλο, *β.* άτομα που έχουν δανείσει χρήματα για την ασφάλεια του πλοίου ή του φορτίου και *γ.* οι ίδιοι οι ασφαλιστές[31]. Ωστόσο, υπάρχουν και άλλα πρόσωπα τα οποία έχουν βεβαίως ασφαλιστικό συμφέρον, αλλά

[30] βλ. The Principles of Insurable Interest (MIA 1906, sections 4-15) – Marine Insurance (2015) by Institute of Chartered Shipbrokers

[31] βλ. "Law of Marine Insurance" by Susan Hodges (*chapter 2* "Insurable Interest")

δεν περιλαμβάνονται στην ΜΙΑ, όπως οι ναυτικοί πράκτορες. Γενικά, κάθε πρόσωπο που έχει όφελος (κέρδος) από την θαλάσσια αποστολή έχει και ασφαλιστικό συμφέρον.

Συνοψίζοντας, το ασφαλιστικό συμφέρον ή άλλως insurable interest αποτελεί απαραίτητη προϋπόθεση για την κατάρτιση έγκυρης σύμβασης στη θαλάσσια ασφάλιση και πρέπει σωρευτικά να συγκεντρώνει τρία (3) χαρακτηριστικά. Είναι απαραίτητο να είναι: *οικονομικά αποτιμητό*, καθώς θα πρέπει να υπάρχει δυνατότητα οικονομικής αποτίμησης του συμφέροντος, όπως προκύπτει από το αποζημιωτικό χαρακτήρα της σύμβασης ασφάλισης, *νόμιμο*, γιατί εάν το συμφέρον έχει παράνομο ή ανήθικο χαρακτήρα η ασφαλιστική σύμβαση θεωρείται άκυρη και *πραγματικό*, δηλαδή το ασφαλιστικό συμφέρον θα πρέπει να είναι πραγματικό και να μπορεί να αποδειχθεί[32].

3.3 Οι βασικές αρχές που εφαρμόζονται στη θαλάσσια ασφάλιση

Υπάρχουν κάποιες βασικές αρχές που εφαρμόζονται πάντα σε μια σύμβαση θαλάσσιας ασφάλισης και πρέπει να λαμβάνονται σοβαρά υπόψη και από τα δύο συμβαλλόμενα μέρη. Αυτές είναι: η αρχή της καλής πίστης, η θεωρία της εγγύτερης αιτίας και οι εγγυήσεις.

3.3.1 Η αρχή της υπέρτατης καλής πίστης (Utmost Good Faith)

Όλα τα συμβόλαια της θαλάσσιας ασφάλισης βασίζονται στην αρχή της υπέρτατης καλής πίστης ή άλλως της utmost good faith, καθώς η βιομηχανία των θαλάσσιων ασφαλίσεων αναγνωρίζει το δόγμα της *uberrimae fidei.* Η Marine Insurance Act 1906 εκφράζει με σαφήνεια τις ευθύνες που ανατίθενται στα συμβαλλόμενα μέρη ως προς την τήρηση της υπέρτατης καλής πίστης (utmost good faith). Συγκεκριμένα στο αρ. 17 της πράξης αναφέρεται *"Ένα συμβόλαιο θαλάσσιας ασφάλισης είναι ένα συμβόλαιο που βασίζεται στην υπέρτατη καλή πίστη και στην περίπτωση που ένα από τα συμβαλλόμενα μέρη δεν την ασπάζεται, τότε πρέπει και το έτερο μέρος να μην τηρήσει το συμβόλαιο*"[33]. Η αρχή εφαρμόζεται σε όλα τα συμβόλαια θαλάσσιας ασφάλισης ανεξάρτητα από τον κίνδυνο και το αντικείμενο της ασφάλισης τονίζοντας την ανάγκη για ειλικρίνεια και εμπιστοσύνη μεταξύ

[32] βλ. Σημειώσεις στις Ναυτασφαλίσεις – Γ. Δανιήλ

[33] Παρατίθεται η αγγλική διατύπωση του αρ. 17 της ΜΙΑ 1906: "A contract of marine insurance is a contract based upon the utmost good faith, and, if the utmost good faith be not observed by either party, the contract may be avoided by the other party''

των συμβαλλομένων μερών και επιβάλλεται να υπάρχει όχι μόνο κατά την διάρκεια των διαπραγματεύσεων για τη σύναψη μιας σύμβασης, άλλα και σε όλη την διάρκεια ισχύος της, στην ερμηνεία της και στην εκτέλεσή της μέχρι την λήξη της. Η ΜΙΑ 1906 θέτει το βάρος της τήρησης της ανωτέρω αρχής και στα δύο μέρη του συμβολαίου δικαίως και ισομερώς, αν και στην πράξη, αυτό πέφτει περισσότερο στον ασφαλισμένο. Εάν ο ασφαλισμένος παραβιάσει την αρχή της υπέρτατης πίστης, τότε ο ασφαλιστής μπορεί να αθετήσει το συμβόλαιο και να μην τηρήσει τις απορρέουσες από αυτό υποχρεώσεις του. Αυτό σημαίνει ότι ο ασφαλιστής συμπεριφέρεται σα να μην είχε αποδεχτεί ποτέ από την πλευρά του το ασφαλιστήριο συμβόλαιο και συνεπεία τούτου, αρνείται να πληρώσει όλες τις αξιώσεις ανεξάρτητα από το αν απορρέουν ή όχι από την παραβίαση της αρχής ταύτης.

Το ότι το βάρος της υπέρτατης καλής πίστης σ' ένα ασφαλιστήριο συμβόλαιο το έχει κυρίως ο λήπτης της ασφάλισης, σημαίνει ότι έχει την υποχρέωση να αποκαλύπτει και να μην αποκρύπτει στον ασφαλιστή του, πριν την ολοκλήρωση του συμβολαίου, όλα εκείνα τα ουσιώδη στοιχεία, τα οποία, αφού τα λάβει υπόψη του ο ασφαλιστής, θα προβεί ή μη στη σύναψη της ασφαλιστικής σύμβασης[34]. Το βασικό κριτήριο για την απόφαση του ασφαλιστή, είναι πως θα αντιδρούσε ένας συνετός ασφαλιστής αναφορικά με τη σύναψη ή μη της σύμβασης ασφάλισης, εάν είχε την σωστή πληροφόρηση.

Η αρχή της υπέρτατης καλής πίστης έχει ιδιαίτερη σημασία για τον ασφαλιστή, αφού υπερασπίζεται τα δικαιώματά του έναντι του ασφαλισμένου· ο ασφαλισμένος έχει πολλές παραπάνω πληροφορίες από τον ασφαλιστή, πριν την υπογραφή του συμβολαίου, αναφορικά με τον κίνδυνο, με αποτέλεσμα ο ασφαλιστής να βασίζεται αποκλειστικά στις πληροφορίες που του δίνει ο λήπτης της ασφάλισης για να προβεί στην οριστικοποίηση και την υπογραφή της σύμβασης. Επομένως, οι πληροφορίες πρέπει να είναι αληθείς και να βασίζονται στην εμπιστοσύνη μεταξύ των συμβαλλομένων μερών, η οποία χτίζεται και ενισχύεται χάρη στην αρχή της utmost good faith, η οποία επιβάλλει και στα δύο μέρη τον υψηλότερο βαθμό εντιμότητας.

Δέον να εξεταστεί πως μπορεί να εφαρμοστή η αρχή της υπέρτατης καλής πίστης στο πλαίσιο της κυβερνοασφάλειας και της θαλάσσιας ασφάλισης. Αρχικά, ένας ασφαλισμένος είναι πολύ δύσκολο να γνωρίζει τα στοιχεία που χρειάζονται για την κυβερνοασφάλεια προκειμένου να ενημερώσει τον ασφαλιστή, ως οφείλει, για να προβεί ο τελευταίος στη

[34] Με την τροποποίηση που επέφεραν οι νέες διατάξεις της Marine Insurance Act 2015, στο άρθρο 21 § 2 του Νόμου καταργούνται ουσιαστικά τα αρ. 18, 19 και 20 της ΜΙΑ 1906. Η νέα πράξη τροποποιεί το καθήκον της υπέρτατης καλής πίστης και εισάγει το καθήκον της Δίκαιης Παρουσίασης του κινδύνου, το οποίο επιφέρει τα ίδια αποτελέσματα.

σύναψη της σύμβασης. Οι σχετικές με την κυβερνοασφάλεια πληροφορίες που υποχρεούται βάσει της αρχής της υπέρτατης καλής πίστης, ο ασφαλισμένος να παραχωρήσει στον ασφαλιστή αφορούν κάθε ηλεκτρονικό σύστημα, ηλεκτρονική συσκευή, συσκευή επικοινωνίας, πλοήγησης και οποιαδήποτε άλλη πληροφορία σχετίζεται με τη λειτουργία αυτών. Ωστόσο, αυτό δημιουργεί δύο προβλήματα.

Το πρώτο είναι, αν οι ασφαλισμένοι είναι σε θέση να γνωρίζουν με ακρίβεια ότι αφορά την κυβερνοασφάλεια προκειμένου να μπορέσουν να μεταφέρουν σωστά την πληροφορία στο έτερο συμβαλλόμενο μέρος. Πέρα από το γεγονός ότι ο κυβερνοχώρος είναι μια σύνθετη έννοια και δυσνόητη στους πιο πολλούς, οι περισσότερες εταιρίες δεν έχουν συγκεκριμένο τμήμα ασφαλείας με προσωπικό κατηρτισμένο[35] και εξοικειωμένο στο συγκεκριμένο αντικείμενο, με αποτέλεσμα όλα τα στοιχεία που δίνουν οι μη αρμόδιοι στους ασφαλιστές τους να είναι κάπως θολά. Κανείς δεν έχει τις γνώσεις και την εκπαίδευση που χρειάζεται ώστε να είναι έμπειρος και να γνωρίζει την ακριβή λειτουργία κάθε λογισμικού προγράμματος και κάθε ηλεκτρονικού συστήματος που υπάρχει στα πλοία, καθιστώντας ακόμα πιο πολύπλοκη στο ζήτημα της κυβερνοασφάλειας την απορρέουσα από την αρχή της υπέρτατης καλής πίστης υποχρέωση των ασφαλισμένων για παροχή ουσιωδών πληροφοριών εξαρχής. Το δεύτερο πρόβλημα είναι ότι αυτό που έχουν να αντιμετωπίσουν οι ασφαλιστές σχετικά με τις πολύπλοκες πληροφορίες που τους δίνονται για τη σύναψη σύμβασης είναι ένα ιδιαίτερα δύσκολο έργο, μία πρόκληση που πρέπει να ξεπεράσουν.

Με το ψήφισμα MSC.428(98), το οποίο θα τεθεί άμεσα σε ισχύ, οι λήπτες της ασφάλισης, θα πρέπει να γνωρίζουν και το σχέδιο διαχείρισης της κυβερνοασφάλειας που θα εφαρμόσουν για να ενημερώσουν στη συνέχεια και τους ασφαλιστές τους. Γενικά, η εφαρμογή του εν λόγω ψηφίσματος θα αλλάξει τον χάρτη της θαλάσσιας ασφάλισης στο ζήτημα των κυβερνοκινδύνων.

3.3.2 Η θεωρία της εγγύτερης αιτίας (Causa Proxima)

Ένα συμβόλαιο θαλάσσιας ασφάλισης καλύπτει μόνο συγκεκριμένους κίνδυνους για τους οποίους ασφαλίζεται το αντικείμενο της ασφάλισης, οι οποίοι αναφέρονται στο περιεχόμενό του. Όπως είναι λογικό, εάν το αντικείμενο της ασφάλισης υποστεί ζημία ή απώλεια, η οποία

[35] Η εμφάνιση της τηλεργασίας λόγω της πανδημίας, Covid- 19, και της επιτάχυνσης του ψηφιακού μετασχηματισμού, αύξησε σημαντικά τη ζήτηση στον τομέα της κυβερνοασφάλειας σε όλους τους κλάδους. Πρόσφατη μελέτη του Οργανισμού Πιστοποίησης Ασφάλειας, ICS, κατέδειξε ότι οι κενές θέσεις εργασίας σε επαγγελματίες κυβερνοασφάλειας ξεπέρασαν τα 4 εκατομμύρια κατά το προηγούμενο έτος.

προκλήθηκε από έναν ή περισσότερους κινδύνους που περιέχονται στο ασφαλιστήριο συμβόλαιο, τότε ο ασφαλιστής υποχρεούται να αποζημιώσει τον ασφαλισμένο. Αντιθέτως, εάν η ζημία ή η απώλεια είναι το αποτέλεσμα ενός κινδύνου, που δεν περιλαμβάνεται σε αυτό, τότε ο ασφαλιστής δεν έχει καμία υποχρέωση έναντι του ασφαλισμένου για κάλυψη της ζημίας. Προκειμένου να θεμελιωθεί η ευθύνη των ασφαλιστών και η αντίστοιχη υποχρέωση προς αποζημίωση πρέπει να υπάρχει αιτιώδης συνάφεια μεταξύ της επέλευσης της ζημίας και του ζημιογόνου γεγονότος που έλαβε χώρα ή άλλως να υπάρχει η σχέση αιτίου – αιτιατού.

Το πρόσωπο που αξιώνει την αποζημίωση, ήτοι ο ασφαλισμένος, είναι αυτό που φέρει το βάρος της απόδειξης. Πρέπει ν' αποδείξει ότι η αιτία της απώλειας οφείλεται αποκλειστικά σε έναν από τους ασφαλισμένους κινδύνους. Ωστόσο, δεν είναι πολύ εύκολο να εντοπιστεί η πραγματική αιτία που προκάλεσε το περιστατικό για το οποίο εγείρεται αξίωση αποζημίωσης, καθώς αυτό, μπορεί να είναι αποτέλεσμα διαδοχικών συμβάντων και όχι μιας μεμονωμένης ενέργειας. Για παράδειγμα, μια απώλεια μπορεί να οφείλεται σε δύο οριοθετημένους και ξεχωριστούς κινδύνους· ο ένας από αυτούς μπορεί να περιλαμβάνεται στο ασφαλιστήριο συμβόλαιο και ο άλλος όχι. Επομένως, πρέπει να διαπιστωθεί με σαφήνεια ποιος από τους δύο κινδύνους είναι η αιτία που οδήγησε στο υπό αξίωση αποτέλεσμα, ώστε στη συνέχεια, τα συμβαλλόμενα μέρη να μπορέσουν να εξακριβώσουν, εάν αυτός ο κίνδυνος, περιλαμβάνεται ή όχι στο συναφθέν συμβόλαιο. Εξάλλου, τα περισσότερα ατυχήματα που συμβαίνουν στη θάλασσα προκαλούνται από ένα συνδυασμό αιτιών. Επίσης, δέον να αναφερθεί ότι στη θεωρία της εγγύτερης αιτίας για να καθοριστεί η ευθύνη του ασφαλιστή πρέπει να εξεταστεί η άμεση και όχι η απομακρυσμένη αιτία, δηλαδή "causa proxima non remota spectator". Η έννοια της εγγύτητας κρίνεται με βάση το γεγονός που είχε την καθοριστικής σημασίας επίδραση στην δημιουργία του αποτελέσματος και όχι με βάση τη χρονική σειρά που συνέβησαν.

Το δίπτυχο, αίτιο –αιτιατό και η μεταξύ τους αιτιώδης σχέση, αποτυπώνεται στη θαλάσσια ασφάλιση στο αρ. 55 § 1 της Μ.Ι.Α 1906 όπου μ' έναν κάπως επαναλαμβανόμενο τρόπο αναφέρει ότι *ο ασφαλιστής είναι υπεύθυνος για οποιαδήποτε απώλεια προκαλείται άμεσα απο ασφαλισμένο κίνδυνο και δεν είναι υπεύθυνος για απώλεια που προκαλείται από έναν μη ασφαλισμένο κίνδυνο*[36]. Το συγκεκριμένο άρθρο διατυπώνει την αρχή της εγγύτερης αιτίας

[36] Παρατίθεται η αγγλική διατύπωση του αρ. 55§1 της MIA 1906 " "Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against, but, subject as aforesaid, he is not liable for any loss which is not proximately caused by a peril insured against."

"*proximately caused*", αλλά δεν προσδιορίζει τον τρόπο για την εύρεσή της. Κάποιες φορές η πραγματική/εγγύτερη αιτία είναι εμφανής και άρρηκτα συνδεδεμένη με το αιτιατό/αποτέλεσμα, άλλες πάλι δεν είναι τόσο εύκολο να βρεθεί η αιτιώδης σχέση ενός περιστατικού και ενός κινδύνου, δυσκολεύοντας πολύ το έργο των ασφαλιστών. Ο ασφαλιστής πάντως, εκπίπτει της υποχρέωσής τους για καταβολή αποζημίωσης εφόσον η εγγύτερη αιτία είναι αποτέλεσμα κακόβουλης συμπεριφοράς του ασφαλισμένου.

Δυσκολία στην εφαρμογή της θεωρίας της εγγύτερης αιτίας παρουσιάζεται και στην θαλάσσια ασφάλιση των κυβερνοκινδύνων. Αρχικά, είναι πολύ απαιτητικό να προσδιοριστεί με ακρίβεια σε μια κυβερνοεπίθεση ποια είναι η εγγύτερη αιτία που οδήγησε σ' αυτήν, αφού πολλές φορές είναι δύσκολο ακόμα και να αντιληφθεί κάποιος ότι ένα περιστατικό κυβερνοεπίθεσης έλαβε χώρα. Ακόμα, όμως και να γίνει μάρτυρας ενός περιστατικού κυβερνοεπίθεσης, είναι σχεδόν αδύνατο να οδηγηθεί στην ακριβή αιτία που προκάλεσε το περιστατικό. Επίσης, η θαλάσσια ασφάλιση στην περίπτωση των κυβερνοεπιθέσεων βρίσκεται αντιμέτωπη με πολλά παράλληλα περιστατικά, τα οποία λαμβάνουν χώρα ανά πάσα χρονική στιγμή, με αποτέλεσμα να μη μπορεί να βρει με ποια πράξη συνδέεται το αποτέλεσμα, δηλαδή την αιτιώδη σχέση.

3.3.3 Εγγυήσεις (Warranties)

Οι εγγυήσεις, αν και δεν ανήκουν στις αρχές, τοποθετούνται σε αυτό το κεφάλαιο, γιατί κατέχουν μία σημαντική θέση σε κάθε είδους ασφάλιση, πολύ περισσότερο στη θαλάσσια ασφάλιση. Οι εγγυήσεις αναφέρονται πάντα σ' έναν όρο του ασφαλιστηρίου συμβολαίου, ο οποίος, αν αθετηθεί, θα επιφέρει συγκεκριμένες νομικές συνέπειες. Με την εγγύηση ο ασφαλισμένος αναλαμβάνει ορισμένες υποχρεώσεις προς τις οποίες πρέπει να συμμορφωθεί μέσα σ' ένα προκαθορισμένο χρονικό διάστημα και η απορρέουσα, από το ασφαλιστήριο συμβόλαιο, ευθύνη του ασφαλιστή εξαρτάται από τη συμμόρφωση του ασφαλισμένου με αυτές τις υποχρεώσεις.

Η Marine Insurance Act 1906 αναφέρεται στις εγγυήσεις στα άρθρα 33 – 41. Συγκεκριμένα στο άρθρο 33 § 1 της MIA 1906 *η εγγύηση ορίζεται ως μια υποσχετική εγγύηση του ασφαλισμένου προς τον ασφαλιστή, ο οποίος αναλαμβάνει να πράξει ή όχι κάτι, ή να εκπληρώσει ορισμένους όρους ή μέσω της οποίας δέχεται ή αρνείται την ύπαρξη μιας κατάστασης πραγμάτων.* Η αναγραφή εγγυήσεων στο συμβόλαιο εξασφαλίζει τον ασφαλιστή και συγχρόνως βοηθάει τον λήπτη της ασφάλισης να επιτύχει καλύτερο ασφάλιστρο. Εάν η εγγύηση αθετηθεί, ο ασφαλιστής από εκείνη τη χρονική στιγμή της αθέτησης, απαλλάσσεται

των ευθυνών του έναντι του ασφαλισμένου και παύει η ισχύς του συμβολαίου. Εξακολουθεί να ευθύνεται όμως, για κάθε ζημία ή απώλεια, η οποία προκλήθηκε πριν από την αθέτηση της "υποσχετικής εγγύησης". Αυτή η οριστική και αυτόματη παύση της ισχύς του συμβολαίου και των υποχρεώσεων των ασφαλιστών έχει τροποποιηθεί ελαφρώς με την Marine Insurance Act 2015, η οποία ορίζει στο αρ. 10 ότι η αθέτηση μιας εγγύησης απλώς αναστέλλει προσωρινά την ισχύ του συμβολαίου, το οποίο μπορεί να τεθεί εκ νέου σε ισχύ, εάν η αθέτηση, που οδήγησε στην παύση του, θεραπευτεί.

Υπάρχουν δυο ειδών εγγυήσεις· αυτές που αναφέρονται στο συμβόλαιο και ονομάζονται ρητές εγγυήσεις (expressed warranties) και οι απαράβατες εγγυήσεις (implied warranties), οι οποίες προβλέπονται από την Marine Insurance Act 1906. Οι ρητές εγγυήσεις δεν είναι πάντα οι ίδιες, αλλά διαφοροποιούνται σε κάθε νέο συμβόλαιο ανάλογα με αυτά που θέλουν να ορίσουν τα συμβαλλόμενα μέρη. Επίσης, σε αντίθεση με τις ρητές εγγυήσεις, οι απαράβατες είναι πάντα οι ίδιες, υποχρεωτικές και ποτέ δεν αναγράφονται στο συμβόλαιο. Οι απαράβατες εγγυήσεις είναι: ο υποχρεωτικός όρος Αξιοπλοΐας (warranty of seaworthiness), ο υποχρεωτικός όρος λιμενικότητας (warranty of port worthiness), ο υποχρεωτικός όρος ικανότητας φορτίου (warranty of cargo worthiness) και ο υποχρεωτικός όρος νομιμότητας (warranty of legality)[37].

Η κυβερνοασφάλεια, είτε άμεσα είτε έμμεσα, μπορεί να αποτελέσει το κύριο ζήτημα πολλών ασφαλιστικών εγγυήσεων. Χαρακτηριστικό παράδειγμα το άρθρο 39 της MIA 1906, το οποίο απαιτεί να υπάγονται συγκεκριμένες εγγυήσεις στις πολιτικές ταξιδιών. Η απαράβατη εγγύηση, η οποία αναφέρεται στο ανωτέρω άρθρο, ορίζει συγκεκριμένα ότι ένα πλοίο πρέπει να είναι αξιόπλοο και κατάλληλο για πλου κατά την έναρξη κάθε ταξιδιού. Η αξιοπλοΐα του πλοίου ορίζεται στο αρ. 39 § 4 όπου σύμφωνα με το οποίο " *ένα πλοίο θεωρείται ότι είναι αξιόπλοο όταν είναι ικανό από κάθε άποψη να αντιμετωπίσει τους συνηθισμένους θαλάσσιους κινδύνους του ασφαλισμένου ταξιδιού*". Η αξιοπλοΐα ενός πλοίου εξαρτάται, όχι μόνο από το ίδιο το πλοίο, αλλά και από την ύπαρξη των απαραίτητων για ασφαλή ναυσιπλοΐα μηχανημάτων, εξαρτημάτων και επάνδρωσης του πλοίου με το κατάλληλο πλήρωμα. Η κυβερνοασφάλεια ενός πλοίου θεωρείται αναπόσπαστο κομμάτι της αξιοπλοΐας του. Αν όμως αυτή είναι ανεπαρκής, επηρεάζοντας τελικά την αξιοπλοΐα του πλοίου, οι ασφαλιστές θα καλύψουν την όποια ζημία προκύψει λόγω της συμβατικής τους υποχρέωσης ή θα θεωρηθεί ότι αθετήθηκε η συγκεκριμένη απαράβατη εγγύηση κάνοντας

[37] βλ. για περαιτέρω ανάλυση των απαράβατων εγγυήσεων τα κεφάλαια 3 και 4 του "Warranties in Marine Insurance" by Baris Soyer, 2nd edition.

τους να απέχουν από οποιαδήποτε ευθύνη έναντι του ασφαλισμένου. Το πρόβλημα που ανακύπτει σ' αυτήν την περίπτωση είναι ότι δεν είναι καθόλου απλό γι' αυτούς να αποδείξουν ότι ο ασφαλισμένος είχε γνώση της έλλειψης αξιοπλοΐας πριν το πλοίο ξεκινήσει τη "*θαλάσσια περιπέτειά*" του.

Όπως αναφέρθηκε ανωτέρω, η αξιοπλοΐα ενός πλοίου, και κατά συνέπεια η τήρηση αυτής της απαράβατης εγγύησης, εξαρτάται και από το σύνολο των μηχανημάτων και των εξαρτημάτων που βρίσκονται επί του πλοίου. Από τη σκοπιά της κυβερνοασφάλειας όμως, όταν ένα πλοίο είναι εξοπλισμένο με ηλεκτρονικά συστήματα, τότε αυτό μπορεί να γίνει εύκολα στόχος μιας κυβερνοεπίθεσης, αφού οι ηλεκτρονικές συσκευές αποτελούν εκ των ουκ άνευ το αντικείμενο μιας τέτοιας επίθεσης. Επομένως, το καθήκον του ασφαλισμένου να παρέχει ένα αξιόπλοο πλοίο για την τήρηση της συμβατικής του υποχρέωσης, πηγάζει και συγχρόνως ταυτίζεται με το καθήκον του να παρέχει ένα ασφαλές από κινδύνους στον κυβερνοχώρο πλοίο με προσαρτημένο εξοπλισμό προστατευμένο από κυβερνοεπιθέσεις. Συνεπάγεται ότι η κυβερνοασφάλεια δεν προστατεύει μόνο το πλοίο από τους κινδύνους στον κυβερνοχώρο, αλλά είναι και αυτή που, σε περίπτωση που συμβεί μία αιφνίδια επίθεση, θα προστατεύσει τον ασφαλισμένο έναντι του ασφαλιστή. Οπότε, η αξιοπλοΐα μπορεί να σχετιστεί ως ένα βαθμό με την κυβερνοασφάλεια.

3.4 Οι απώλειες και οι ζημίες μιας κυβερνοεπίθεσης

Οι απώλειες και οι ζημίες που προκαλεί μια κυβερνοεπίθεση είναι τις περισσότερες φορές ανυπολόγιστες. Η κλίμακα των απωλειών μπορεί να είναι σημαντική, ειδικά εάν ένα περιστατικό προκαλέσει ζημία σε πλοία, λιμενικές υποδομές ή άλλα φυσικά περιουσιακά στοιχεία, διότι μέσα από τη στοχευόμενη επίθεση διαταράσσεται συγχρόνως και η γενικότερη ροή των λειτουργιών της ναυτιλίας. Επίσης, μια επίθεση μπορεί να οδηγήσει σε οικονομική και περιουσιακή καταστροφή, αλλά και σε λιγότερο προφανείς επιπτώσεις, που είναι δύσκολο κάποιος να τις συνδυάσει με μια κυβερνοεπίθεση, όπως είναι η σύγκρουση, η απώλεια ζωής, ο τραυματισμός, η πειρατεία, το ναυάγιο και η περιβαλλοντική καταστροφή.

Για παράδειγμα, υπάρχουν πάρα πολλά ηλεκτρονικά συστήματα διαχείρισης ενός πλοίου, όπως το σύστημα πλοήγησης, τα οποία οι δράστες μπορούν να τα ελέγξουν με παρεμβολές ή με αποστολή ψευδών δεδομένων, και τελικά να οδηγήσουν τα πλοία όπου αυτοί θέλουν προκείμενου να τα κατάσχουν και να ζητήσουν λύτρα (πειρατεία). Σομαλοί πειρατές με τη βοήθεια ενός χάκερ κατάφεραν να διεισδύσουν στα ηλεκτρονικά συστήματα μιας ναυτιλιακής εταιρείας προκειμένου να εντοπίζουν τα πλοία που διέρχονται από τον Κόλπο

του Άντεν με σκοπό την πειρατεία των πλοίων αλλά και των φορτίων τους. Γι' αυτό το λόγο, είναι σύνηθες η ναυτιλιακή βιομηχανία, αλλά και αυτή των θαλάσσιων ασφαλίσεων, να εξετάζουν ανάλογα περιστατικά που συμβαίνουν στον κυβερνοχώρο και ως ζητήματα πειρατείας.

Δέον να υπογραμμιστεί ότι σε μια κυβερνοεπίθεση υπάρχουν και κάποιες σημαντικές επιπτώσεις, οι οποίες δεν είναι πάντα οφθαλμοφανείς. Στις 28.09.2020, η γαλλική εταιρία CMA CGM υπέστη παραβίαση στο σύστημα ασφαλείας της, η οποία την ανάγκασε να διακόψει την εξωτερική πρόσβαση στο δίκτυό της προκειμένου να σταματήσει την περαιτέρω εξάπλωση του κακόβουλου λογισμικού. Δύο βδομάδες μετά την επίθεση, η CMA CGM με μήνυμα ηλεκτρονικού ταχυδρομείου που απέστειλε, ενημέρωσε για την επαναφορά των λειτουργιών της στην κανονικότητα. Στις 30.09.2020 ο ΙΜΟ έπεσε θύμα κυβερνοεπίθεσης, η οποία δημιούργησε σημαντικά προβλήματα εισόδου στην ιστοσελίδα του ΙΜΟ, καθώς και στις διαδικτυακές του υπηρεσίες. Σήμερα, 2 σχεδόν μήνες μετά την επίθεση και παρά την προσπάθειας που κατέβαλαν οι ειδικοί, η ιστοσελίδα του ΙΜΟ δεν έχει αποκατασταθεί πλήρως.

Τα περιστατικά αυτά αναφέρονται προκειμένου να υπογραμμίσουν την έκταση που μπορεί να λάβει κάποιες φορές μια επίθεση στον κυβερνοχώρο. Δεν είναι ύψιστης σημασίας μόνο το προφανές, δηλαδή η παύση των λειτουργιών της εταιρίας τη στιγμή της επίθεσης και η χρηματική ζημία, αλλά και το γεγονός ότι η πλήρης αποκατάσταση και η επαναφορά στην προτεραία κατάσταση μπορεί να διαρκέσει μεγάλο χρονικό διάστημα και να χρειαστεί μεγάλο χρηματικό κεφάλαιο, πχ A.P. Møller-Mærsk. Γίνεται επομένως, αντιληπτό τι μπορεί να σημαίνει αυτό για μία, μέχρι τη στιγμή της επίθεσης, υγιή εταιρία. Επιπλέον, η δημοσιοποίηση περιστατικών κυβερνοεπιθέσεων πολλές φορές προκαλούν έμμεση ζημία σε μία εταιρία βλάπτοντας τη φήμη της και κλονίζοντας την εμπιστοσύνη των πελατών της και εν γένει της ναυτιλιακής αγοράς προς αυτήν. Η δυσφήμηση μιας εταιρίας επιτείνεται λόγω του ανταγωνιστικού περιβάλλοντος της ναυτιλίας. Επιπροσθέτως, εάν με το ανεπιθύμητο περιστατικό στον κυβερνοχώρο διακυβεύονται τα προσωπικά δεδομένα των υπαλλήλων ή των πελατών μιας εταιρίας, ενδέχεται να προκύψουν σημαντικά κόστη γι' αυτήν όσον αφορά την αντιμετώπισή του, όπως πχ αυτά που ορίζονται στο πλαίσιο της ΕΕ από τον κανονισμό GDPR. Τέλος, μετά από ένα περιστατικό στον κυβερνοχώρο, είναι πιθανό να κριθούν από την εταιρία απαραίτητες, οι συμβουλευτικές υπηρεσίες πληροφορικής για τον μετριασμό των επιπτώσεων μιας παραβίασης, την αποκατάσταση συστημάτων πληροφορικής και την αποκατάσταση της εμπιστοσύνης των πελατών και των αντισυμβαλλομένων. Η μετέπειτα, επομένως, επένδυση σε υποδομές πληροφορικής, καθώς οι περισσότερες εταιρίες υστερούν

σε αυτό το κομμάτι, μπορεί να είναι δαπανηρή και χρονοβόρα, όπως και η ενίσχυση της κυβερνοασφάλειας της. Αυτό που πρέπει να πράξει κάθε εταιρία μετά από ένα ανεπιθύμητο περιστατικό στον κυβερνοχώρο, είναι να λάβει όλα τα κατάλληλα μέτρα, ανεξαρτήτως κόστους, προκειμένου να μετριάσει τον αντίκτυπο του συμβάντος.

Το οικονομικό αποτύπωμα των κυβερνοεπιθέσεων είναι τεράστιο σε παγκόσμιο επίπεδο, καθώς τα περιστατικά στον κυβερνοχώρο κατατάσσονται ως ο κορυφαίος κίνδυνος στις εταιρίες σύμφωνα με το Βαρόμετρο Κινδύνου 2020 (Risk Barometer) της Allianz. Για πρώτη φορά βρίσκονται στην υψηλότερη θέση με ποσοστό 39%, αυξημένο κατά 2% από την αντίστοιχη μέτρηση του 2019.

Με βάση τα ανωτέρω, η θαλάσσια ασφάλιση πρέπει να λάβει σοβαρά υπόψη της και το ευρύ φάσμα των απωλειών και ζημιών προκειμένου να προτείνει λύσεις για να ανακουφίσει τους πλοιοκτήτες, τους διαχειριστές ή τον οποιοδήποτε υπεύθυνο, οι οποίοι μέχρι στιγμής, τις περισσότερες φορές σηκώνουν μόνοι τους το βάρος μιας κυβερνοεπίθεσης.

3.5 Οι ευθύνες που απορρέουν από μια κυβερνοεπίθεση

Για να ενεργοποιηθεί μια σύμβαση ασφάλισης και να παράγει τα αποτελέσματά της, μετά από ένα περιστατικό κυβερνοεπίθεσης, είναι πολύ σημαντικό να μπορούν να προσδιοριστούν με ακρίβεια οι ανακύπτουσες ευθύνες. Αυτό είναι αρκετά δύσκολο στην παρούσα χρονική περίοδο λόγω του χαοτικού περιβάλλοντος του κυβερνοχώρου. Ωστόσο, στο πλαίσιο της ασφαλιστικής κάλυψης των κυβερνοκινδύνων, η οποία γίνεται ολοένα και πιο απαραίτητη, οι ασφαλιστικές εταιρίες και τα P&I clubs πρέπει να είναι σε θέση να προσδιορίσουν αυτές τις ευθύνες, γιατί ο προσδιορισμός της είναι το πρώτο βήμα για την μετέπειτα κάλυψη.

Προβλήματα που εμφανίζονται αναφορικά με το ζήτημα της ευθύνης: Ο κίνδυνος στον κυβερνοχώρο μπορεί να προέρχεται από μη εγκληματικές δραστηριότητας, όπως εισαγωγή ενός usb, που περιέχει ιό, από μέλος του πληρώματος σε κάποιο ηλεκτρονικό σύστημα του πλοίου. Οι κυβερνοεπιθέσεις δεν προέρχονται μόνο από χάκερς, αλλά μπορεί να είναι και το τυχαίο αποτέλεσμα μιας δυσλειτουργίας του συστήματος (τεχνικής φύσης θέμα) ή να οφείλεται στο αθώο λάθος ενός μη εξοικειωμένου με τα ηλεκτρονικά συστήματα, πχ ναύτη. Ωστόσο, η δυσλειτουργία ενός συστήματος μπορεί να μην είναι καθόλου τυχαία, αλλά να οφείλεται σε κάποιο κατασκευαστικό λάθος, το οποίο αυτόματα οδηγεί στην ευθύνη του κατασκευαστή ή του προμηθευτή.

Γενικά, το ζήτημα της ευθύνης είναι ένα πολύ σημαντικό θέμα στη θαλάσσια ασφάλιση, πολλώ δε μάλλον όταν αυτή συνδυάζεται με την κυβερνοασφάλεια. Εκεί οι διαχωριστικές

γραμμές της ευθύνης του κάθε εμπλεκόμενου προσώπου είναι πολύ λεπτές και δυσδιάκριτες. Σ' αυτό δε, συνηγορεί και η ρευστότητα του κυβερνοχώρου. Αυτά έχουν ως αποτέλεσμα να δημιουργείται θέμα, όχι μόνο στο είδος της ασφάλειας που θα επιλεχθεί, αλλά και στον αν τελικά και μέχρι ποιο βαθμό καλύπτεται ο ασφαλισμένος.

3.5.1 Η επίδραση της ανεπαρκούς κυβερνοασφάλειας στην αστική ευθύνη

Αξίζει να εξεταστεί, εάν ένα ανεπαρκές σύστημα κυβερνοασφάλειας, είτε στο πλοίο είτε στη ξηρά, μπορεί να επηρεάσει την αστική ευθύνη του πλοίου, του πλοιοκτήτη και του διαχειριστή σε περίπτωση ατυχήματος. Ως ανεπάρκεια νοείται η μη συμμόρφωση ενός πλοιοκτήτη ή διαχειριστή με τον κώδικα ISM, το οποίο έχει ως αποτέλεσμα να βρίσκεται σε αναστολή ή σε απόσυρση το απαραίτητο για την πλεύση έγγραφο συμμόρφωσης. Ομοίως, ένα πλοίο του οποίου το σύστημα ασφαλούς διαχείρισης (SMS) είναι ανεπαρκές, επειδή δε κατάφερε να υιοθετήσει κατάλληλα μέτρα κυβερνοασφάλειας, είναι εμπορικά μη βιώσιμο.

Γενικά, στην περίπτωση ατυχήματος είναι πολύ σημαντικό να βρεθεί η ουσιαστική αιτία που προκάλεσε το ατύχημα για να αποδοθούν στη συνέχεια οι ευθύνες. Χαρακτηριστικό παράδειγμα της εύρεσης της αιτίας και του κατά πόσο παίζει σημαντικό ρόλο η ενσωμάτωση κατάλληλων μέτρων κυβερνοασφάλειας είναι το εξής: Ένα πλοίο του οποίου χακαρίστηκε το σύστημα πλοήγησης, λόγω ανεπαρκούς εκπαίδευσης του πληρώματος και μη εφαρμογής κατάλληλων μέτρων κυβερνοασφάλειας, ενεπλάκη σε μια σύγκρουση. Αν αυτό το πλοίο, λόγω της κυβερνοεπίθεσης βρέθηκε εκτός δρόμου και συγκρούστηκε με έτερο πλοίο, το οποίο βρισκόταν και αυτό εκτός δρόμου, τότε είναι πολύ πιθανό οι απορρέουσες από τη σύγκρουση αστικές ευθύνες να μοιραστούν και στα δύο πλοία, παρά το γεγονός ότι το πρώτο υστερούσε σε θέμα κυβερνοασφάλειας. Ωστόσο, εάν το πρώτο πλοίο είχε λάβει όλα τα απαραίτητα και κατάλληλα μέτρα κυβερνοασφάλειας και παρόλα αυτά το σύστημα πλοήγησής του βρίσκεται στο στόχαστρο κάποιου συμβάντος στον κυβερνοχώρο και μπλέκεται σε σύγκρουση με το πλοίο Β, του οποίου, τα συστήματά του στον κυβερνοχώρο δουλεύουν κανονικά, χωρίς να έχουν εμπλακεί δηλαδή σε κάποια κυβερνοεπίθεση, αλλά ότι γίνεται οφείλεται σε τεχνικό λάθος του συστήματος πλοήγησής του, τότε το πρώτο πλοίο δεν ευθύνεται καθόλου για την εμπλοκή στο εν λόγω ατύχημα. Επίσης, πρέπει να ελέγχεται κάθε φορά, αν το ατύχημα μπορούσε να αποφευχθεί ή όχι στο πλαίσιο των ατυχημάτων που περιλαμβάνουν ή ξεκινούν από κάποιο περιστατικό στον κυβερνοχώρο.

Ένα πλοίο που έχει ενσωματώσει τα κατάλληλα μέτρα, ακολουθεί τις οδηγίες και τις κατευθυντήριες οδούς που δίνονται από τους φορείς της ναυτιλίας και έχει ένα σωστό σχέδιο

διαχείρισης της κυβερνοασφάλειας, δε φέρει καμία ευθύνη σε περίπτωση σύγκρουσης με άλλο πλοίο ή αντικείμενο, εάν το σύστημα του πλοήγησης ή έλεγχου ήταν ανίκανο και δε μπορούσε να αποφευχθεί η πρόσκρουση.

Κεφάλαιο 4. Οι τρέχουσες προσεγγίσεις της θαλάσσιας ασφάλισης

4.1 Η κυβερνοασφάλεια και η σχέση της με την θαλάσσια ασφάλιση

Το δίκαιο που διέπει τις θαλάσσιες ασφαλίσεις είναι στη φύση του ιδιωτικού δικαίου. Τα συμβαλλόμενα μέρη μιας θαλάσσιας ασφάλισης, μετά από πολλές διαπραγματεύσεις, καταλήγουν σε μια δεσμευτική συμφωνία, στη συνέχεια συνάπτουν την επίσημη ασφαλιστική σύμβαση και δεσμεύονται εκατέρωθεν από τις υποχρεώσεις, οι οποίες περιλαμβάνονται σ' αυτή. Υπάρχουν διάφορα είδη θαλάσσιας ασφάλισης ανάλογα με το αντικείμενο που ασφαλίζεται κάθε φορά· η θαλάσσια ασφάλιση που καλύπτει το πλοίο και τον εξοπλισμό του (Hull & Machinery insurance), το φορτίο (Cargo insurance) και την αστική ευθύνη τρίτων (P&I insurance). Οι καλυπτόμενοι κίνδυνοι, αναφορά των οποίων γίνεται στο αρ. 3 της MIA 1906[38], χωρίζονται σε δυο κατηγορίες στους κινδύνους της θάλασσας (perils of the sea), όπως είναι τα καιρικά φαινόμενα και στους κινδύνους στη θάλασσα (perils on the sea), όπως είναι η κλοπή. Όσον αφορά τους κινδύνους στον κυβερνοχώρο, οι οποίοι είναι κάτι καινούργιο, που ακόμα εξετάζεται, τόσο από τις ναυτιλιακές εταιρίες όσο και από τις ασφαλιστικές, δεν υπάρχει συγκεκριμένη και υποχρεωτική θαλάσσια ασφάλιση.

Αυτό που ισχύει σήμερα, σε σχέση με την θαλάσσια ασφάλιση των κυβερνοκινδύνων, είναι ότι κάποια από τα παραδοσιακά ασφαλιστικά προϊόντα καλύπτουν ορισμένες απώλειες που προκύπτουν από κινδύνους στον κυβερνοχώρο, αλλά σε καμία περίπτωση τα παραδοσιακά προϊόντα δε θα καλύψουν όλους τους αναδυόμενους κινδύνους. Επιπλέον, κάποια από αυτά, όπως το Hull & Machinery, αποκλείουν καθολικά την κάλυψη ζημιών που προκύπτουν από τον κυβερνοχώρο. Επομένως, πρέπει να κάνουν την εμφάνισή τους νέα ασφαλιστικά προϊόντα, αποκλειστικά σχετιζόμενα με τους κινδύνους στον κυβερνοχώρο, τα οποία θα καλύψουν τα κενά που αφήνουν τα παραδοσιακά προϊόντα ασφάλισης. Εξάλλου,

[38] "Maritime perils" means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seisures, restraints, and detainments of princes and peoples, jettisons, barratry, and any other perils, either of the like kind or which may be designated by the policy.

είναι προφανές ότι η σωστή διαχείριση των κινδύνων στον κυβερνοχώρο μπορεί να βοηθηθεί από την ύπαρξη και αποτελεσματική εφαρμογή της θαλάσσιας ασφάλισης επί των συγκεκριμένων κινδύνων.

4.2Τα εμπόδια με τα οποία βρίσκεται αντιμέτωπη η βιομηχανία των ναυτασφαλίσεων

Μέχρι και σήμερα δεν υπάρχουν συγκεκριμένες ρήτρες για την ασφάλεια στον κυβερνοχώρο, οι οποίες να έχουν ενσωματωθεί στην πολιτική που ακολουθεί η βιομηχανία των θαλάσσιων ασφαλίσεων και αυτό γιατί, οι κίνδυνοι στον κυβερνοχώρο παρουσιάζουν μια σειρά εμποδίων, τα οποία πρέπει οι ασφαλιστές να ξεπεράσουν. Ειδικότερα:

- Ο κίνδυνος στον κυβερνοχώρο περιλαμβάνει πολλές διαφορετικές πτυχές ανάλογα τον κλάδο που στοχεύει. Οι ασφαλιστές επομένως, πρέπει να τον εξειδικεύσουν, παρά την ευρεία του έννοια, και να τον εντάξουν μέσα στο πλαίσιο της θαλάσσιας ασφάλισης.
- Η ασφάλεια στον κυβερνοχώρο, όσο περίεργο και αν φαίνεται δεδομένης της τεχνολογικής άνθησης, δεν έχει ακόμη εδραιωθεί στη ναυτιλιακή βιομηχανία. Από 1η Ιανουαρίου 2021 που θα καταστεί αυτή υποχρεωτική σε όλα τα πλοία, θα αλλάξουν αλυσιδωτά και τα μέχρι στιγμής δεδομένα που υπάρχουν, όσον αφορά τις ναυτασφαλίσεις.
- Ο σκοπός της ασφαλιστικής κάλυψης. Το πρόβλημα είναι ότι οι ασφαλιστές δε γνωρίζουν ακριβώς το αντικείμενο της ασφαλιστικής κάλυψης.
- Η έκταση μιας επίθεσης και η ζημία που θα προκληθεί από αυτήν είναι δύσκολο να υπολογιστούν. Ωστόσο ενδέχεται να είναι ιδιαίτερα υψηλές, γι' αυτό και οι ασφαλιστές δείχνουν απρόθυμοι να προσφέρουν την ανάλογη κάλυψη.
- Οι κίνδυνοι στον κυβερνοχώρο δεν είναι εύκολα προβλέψιμοι, υπολογίσιμοι και αποτιμητοί σε χρήματα, όπως συμβαίνει με τους παραδοσιακούς θαλάσσιους κινδύνους.
- Ο κυβερνοκίνδυνοι μπορούν ν' αντιμετωπιστούν μόνο από κατηρτισμένους και έμπειρους επαγγελματίες συνεπικουρούμενους από ομάδα εξειδικευμένων συμβούλων σε θέματα πληροφορικής.
- Η έλλειψη νομολογίας από τα αγγλικά δικαστήρια μεγαλώνει το πρόβλημα. Το common law[39], όπως είναι ευρέως γνωστό, θα παίξει σημαντικό ρόλο στη διαμόρφωση του θαλάσσιου ασφαλιστικού νόμου αναφορικά με τις κυβερνοεπιθέσεις.

[39] Το εθιμικό δίκαιο (επίσης γνωστό ως δικαστικό προηγούμενο ή δικαστικό δίκαιο ή νομολογία) είναι το σώμα του νόμου που δημιουργήθηκε από δικαστές και το χαρακτηριστικό είναι ότι προκύπτει ως προηγούμενο. Σε περιπτώσεις δηλαδή, όπου οι διάδικοι διαφωνούν, το δικαστήριο ανατρέχει σε προηγούμενες αποφάσεις, οι οποίες προέρχονται από παρόμοιας φύσης υποθέσεις, μελετά το σκεπτικό τους και το προσαρμόζει στην

Επίσης, δυσκολία έγκειται και από την πλευρά των ασφαλισμένων, όσον αφορά την ασφαλιστική κάλυψη των κυβερνοκινδύνων. Αρχικά, εξαιτίας της πολυπλοκότητας των κυβερνοεπιθέσεων και της συνεχούς μεταβαλλόμενης φύσης τους, ο ασφαλισμένος είναι αυτός που πρέπει σε περίπτωση κάποιου συμβάντος να διαπιστώσει ποια είναι η απώλεια ή η ζημία που έχει υποστεί, διαδικασία εξαιρετικά απαιτητική. Επιπλέον, το βάρος της απόδειξης το φέρνει πάντα ο ασφαλισμένος, ο οποίος πρέπει να αποδείξει ότι η αιτία της απώλεια ή της ζημίας που υπέστη είναι αποτέλεσμα μιας κυβερνοεπίθεσης.

Σα γενικό συμπέρασμα, οι θαλάσσιες ασφαλίσεις, ακόμα και σήμερα, μετά τα τόσα περιστατικά κυβερνοεπιθέσεων που έχουν συμβεί, καθυστερούν στο να ακολουθήσουν τις γρήγορες εξελίξεις που λαμβάνουν χώρα στον κυβερνοχώρο. Είναι επιταγή των καιρών, η συνεργασία ασφαλιστών και πλοιοκτητών προκειμένου να αντιμετωπίσουν τα υφιστάμενα κενά όσον αφορά την ασφαλιστική κάλυψη των κυβερνοκινδύνων. Βέβαια από εδώ και πέρα, θα είναι και ζητούμενο για κάθε πλοιοκτήτη να αποδεικνύει στον ασφαλιστή του ότι διαθέτει ισχυρό σύστημα διαχείρισης κυβερνοκινδύνων, τόσο στη ξηρά όσο και στο πλοίου.

Η δυσκολία στην κατανόηση της πολυπλοκότητας των κυβερνοκινδύνων και η ιδιαίτερη φύση των κυβερνοεπιθέσεων με τις απρόβλεπτες και απροσδιόριστες επιπτώσεις τους, δυσχεραίνουν το έργο των ασφαλιστών και όπως αποδεικνύεται, η βιομηχανία των ναυτασφαλίσεων χρειάζεται περισσότερο χρόνο για να μπορέσει να μελετήσει και να αφομοιώσει τους κινδύνους στον κυβερνοχώρο ώστε να προσφέρει την κατάλληλη κάλυψη. Οι ασφαλιστές, τώρα έχουν αρχίσει ν' αντιλαμβάνονται ότι οι κυβερνοκίνδυνοι είναι ένα ζήτημα που επηρεάζει όλα τα στάδια της δουλειάς τους, από τη διαμόρφωση της πολιτικής που θ' ακολουθήσουν, μέχρι τη διαχείριση και την εκτίμηση των αξιώσεων οι οποίες θα προκύψουν από ένα συναφθέν ασφαλιστήριο συμβόλαιο. Σε αυτό το φλέγον ζήτημα που απασχολεί όλον το ναυτιλιακό κόσμο, οι ασφαλιστικές εταιρίες θα πρέπει να μην εφησυχάσουν και να προσφέρουν στους ασφαλισμένους τους υπηρεσίες ποιότητας μέσω σύγχρονων προϊόντων και διαδικασιών.

Μια έρευνα για την ασφάλεια στον κυβερνοχώρο, που διεξήχθη από την IHS Fairplay και την BIMCO το 2016 αποτύπωσε σε αριθμούς το ζήτημα της κυβερνοεπιθέσεων και της θαλάσσιας ασφάλισης. Μόνο το 11,7% των εξακριβωμένων επιθέσεων αναφέρθηκαν στους ασφαλιστές της εταιρίες ενώ μόνο το 3,3% των ερωτηθέντων δήλωσαν ότι η ζημία

υπόθεση που εκδικάζεται. Εάν μια παρόμοια διαφορά έχει επιλυθεί στο παρελθόν, το δικαστήριο είναι συνήθως υποχρεωμένο να ακολουθήσει το σκεπτικό που χρησιμοποιήθηκε στην προηγούμενη απόφαση. Το αγγλικό δίκαιο εξ ολοκλήρου βασίζεται στο common ή case law.

καλύφθηκε από τους ασφαλιστές. Από το ποσοστό του 3,3%, καμία αξίωση δεν καλύφθηκε από την Hull & Machinery ασφάλιση, λιγότερο του 1% καλύφθηκε από την ασφάλιση P&I, ενώ μόνο το 1,9% είχε ειδική ασφάλιση για τον κυβερνοχώρο, η οποία κάλυπτε τη ζημία. Τα νούμερα είναι απογοητευτικά και δείχνουν πόση προσπάθεια ακόμα πρέπει να καταβάλουν και οι δύο πλευρές για την, ως επί των πλείστων, ουσιαστικότερη αντιμετώπιση του προβλήματος.

4.3 Η αγορά των Lloyd's του Λονδίνου

Η μεγαλύτερη ασφαλιστική αγορά του Λονδίνου, οι Lloyd's, κατέχουν την πρώτη θέση στην ασφαλιστική κάλυψη των κυβερνοκινδύνων έως σήμερα. Αυτό είναι λογικό, γιατί εντός της αγοράς υπάρχουν πολλές ασφαλιστικές εταιρίες, οι οποίες παρέχουν ειδικά ασφαλιστήρια συμβόλαια σχετικά με τους κυβερνοκινδύνους.

Προς το τέλος του 2019, οι Lloyd's εισήγαγαν μία νέα θαλάσσια ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο (Cyber Exclusion Clause LMA 5403) σε αντικατάσταση της προηγούμενης CL. 380[40] και από 1η Ιανουαρίου 2020 την κατέστησαν υποχρεωτική για κάθε καινούργιο War Risks ή Hull & Machinery ασφαλιστήριο συμβόλαιο ή για κάθε ανανέωση αυτών. Δεν επιτρεπόταν πια στους ασφαλιστές να παρέχουν κάλυψη στον κυβερνοχώρο κάτω από την ομπρέλα αυτών των δύο ασφαλίσεων απλώς διαγράφοντας ή τροποποιώντας την CL.380. Οι Lloyd's απαιτούν μια ασφάλεια / κάλυψη στον κυβερνοχώρο ξεχωριστή και όχι ν' αποτελεί μέρος κάποιας άλλης ασφαλιστικής κάλυψης. Προκειμένου να καλυφθεί μάλιστα, το σχετικό κενό δημιουργήθηκαν αρκετά προϊόντα, τα οποία είναι πλέον, διαθέσιμα στην αγορά καθένα εκ των οποίων, καλύπτει διαφορετικές απώλειες ή ζημίες.

4.4 Δύο νέα μοντέλα εξαιρέσεων για κινδύνους στον κυβερνοχώρο από τον IUA

Οι κυβερνοκίνδυνοι και η αντίστοιχη ασφαλιστική τους κάλυψή έχουν δημιουργήσει κατά καιρούς πολλά προβλήματα και σύγχυση στους ασφαλιστές λόγω της έλλειψης σαφούς ασφαλιστικής κάλυψης που υπάρχει για κινδύνους στον κυβερνοχώρο. Κάποιες φορές οι ασφαλιστές με τις παραδοσιακές πολιτικές που ακολουθούν, οι οποίες σχεδιάστηκαν όταν ακόμα ο κυβερνοχώρος δεν αποτελούσε σημαντική πηγή κινδύνων, καλύπτουν ακούσια και

[40] βλ. ανάλυση στο κεφάλαιο 4.5 «*Η τρέχουσα αντιμετώπιση των κυβερνοεπιθέσεων από τα P&I Clubs*»

απώλειες στον κυβερνοχώρο[41]. Εξάλλου και η ρήτρα Cl. 380 που χρησιμοποιείται κατά κόρον δεν είχε σχεδιαστεί με αυτόν τον σκοπό· την ευρεία χρήση της σε κάθε ασφαλιστήριο συμβόλαιο. Ζητούμενο επομένως για τους ασφαλιστές, είναι να υπάρξει μεγαλύτερη σαφήνεια στη διατύπωση και συγκεκριμένα στα όρια της παρεχόμενης κάλυψης. Για την αντιμετώπιση αυτών των ζητημάτων, η Διεθνής Ένωση Ασφαλιστών (International Underwriting Association - IUA)[42] δημοσίευσε δύο νέες ρήτρες αποκλεισμού στον κυβερνοχώρο την IUA 09-081 και την IUA 09-082.

Η πρώτη ρήτρα είναι η ρήτρα του απόλυτου αποκλεισμού από απώλεια στον κυβερνοχώρο. Αυτή αποκλείει σ' ένα πιο διευρυμένο πλαίσιο κάθε απώλεια προερχόμενη από τη χρήση υπολογιστών, διαδικτύων ή δεδομένων. Η δεύτερη ρήτρα είναι ρήτρα περιορισμένου αποκλεισμού από απώλεια στον κυβερνοχώρο. Αυτή είναι πιο περιορισμένη και ισχύει μόνο για απώλειες που προκαλούνται άμεσα από περιστατικά στον κυβερνοχώρο. Οι νέες ρήτρες, οι οποίες δημοσιεύθηκαν από την IUA τον Ιούνιο του 2019, αδιαμφισβήτητα προσφέρουν πιο συγκεκριμένο ορισμό και σαφέστερη διατύπωση σε σχέση με την μέχρι εκείνη τη στιγμή μοναδική ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο, τη CL.380, η οποία ήταν ασαφής στη διατύπωση, προκαλούσε σύγχυση, τόσο στους ασφαλιστές όσο και στους ασφαλισμένους, σχετικά με την έκταση της κάλυψης των κυβερνοκινδύνων και είχε δημιουργηθεί το 2003, όταν η ανάγκη για ασφάλιση από τους κυβερνοκινδύνους ήταν σχεδόν ανύπαρκτη, αφού τα ηλεκτρονικά συστήματα στη ναυτιλιακή βιομηχανία δεν είχαν ακόμα

[41] Η διατύπωση για την κάλυψη στον κυβερνοχώρο είναι « non – affirmative» ή «silent». Το «silent cyber» είναι ένας όρος που χρησιμοποιείται όλο και συχνότερα προκειμένου να περιγράψει τις απώλειες που σχετίζονται με τον κυβερνοχώρο και οι οποίες προέρχονται από ασφαλιστήρια συμβόλαια, τα οποία δεν είχαν σχεδιαστεί με σκοπό την κάλυψη τέτοιων κινδύνων. Δηλαδή ένας ασφαλιστής μπορεί να κληθεί να πληρώσει αξιώσεις για απώλειες στον κυβερνοχώρο βάσει μιας σύμβασης που δεν είχε εξαρχής σχεδιαστεί γι' αυτόν το σκοπό. Ένας τέτοιος κίνδυνος (silent ή non–affirmative) μπορεί να προκαλέσει ένα σημαντικό και απροσδόκητο κίνδυνο για τα χαρτοφυλάκια των ασφαλιστών. Γενικά, ένας ασφαλιστής όταν ακολουθεί μία μη καταφατική διατύπωση πολιτικής, δεν έχει εξετάσει τον πιθανό κίνδυνο στον κυβερνοχώρο που καλύπτεται από αυτήν κατά λάθος και κατ' επέκταση, δεν έχει υπολογίσει την αυξημένη έκθεση του αντισυμβαλλόμενου στον κίνδυνο, δεν έχει προσαρμόσει το ασφάλιστρο, αλλά ούτε και έχει αξιολογήσει τη συγκέντρωση πιθανών κινδύνων στο δικό του χαρτοφυλάκιο.

[42] Η IUA εκπροσωπεί τα μέλη της ασφαλιστικής αγοράς (διεθνείς ασφαλιστικές & αντασφαλιστικές εταιρίες), τα οποία λειτουργούν ανεξάρτητα από τους Lloyd's, και δρα προκειμένου να προωθήσει και να ενισχύσει το επιχειρηματικό περιβάλλον στο οποίο κινούνται τα μέλη της. Στατιστικά δεδομένα της IUA έδειξαν ότι τα έσοδά της από ασφάλιστρα το 2017 άγγιξαν τις 26,314 δισεκατομμύρια λίρες Αγγλίας.

αναπτυχθεί πλήρως. Επομένως, οι συγκεκριμένες νέες ρήτρες παρέχοντας ευρείες πολιτικές εξαίρεσης μπορούν ευκολότερα να χρησιμοποιηθούν από ασφαλιστές.

4.5 Η αντιμετώπιση των κυβερνοεπιθέσεων από τα P&I Clubs

Έχοντας ως δεδομένα την πολυπλοκότητα των κυβερνοκινδύνων και το ασαφές εύρος των επιπτώσεων μιας κυβερνοεπίθεσης γίνεται αντιληπτό ότι μία απλή ασφάλιση δεν είναι αρκετή για να παράσχει την απαιτούμενη κάλυψη για τέτοιου είδους κινδύνους. Γι' αυτό το λόγο, θα πρέπει να εξεταστεί η ασφάλιση των κυβερνοκινδύνων και στο πλαίσιο των P&I clubs.

Οι Αλληλασφαλιστικοί Οργανισμοί Προστασίας και Αποζημίωσης - P&I (protection & indemnity) clubs θεωρούνται οι μεγαλύτεροι παίκτες στην αγορά των ναυτασφαλίσεων και είναι μη κερδοσκοπικές εταιρείες με κεφάλαιο, μέλη των οποίων είναι οι ίδιοι οι πλοιοκτήτες. Στην περίπτωση των P&I Club, ασφαλιστής είναι ο ίδιος ο αλληλασφαλιστικός οργανισμός και κατά αυτού στρέφονται οι απαιτήσεις περί αποζημίωσης, ενώ η ναυτασφάλιση σε P&I Clubs προσφέρεται σε χαμηλό κόστος για τους πλοιοκτήτες σε σχέση με άλλους τρόπους ασφάλισης.

Η κάλυψη που προσφέρουν τα Clubs είναι κάλυψη Αστικής Ευθύνης έναντι Τρίτων (Third Party Liability Insurance) για πλοιοκτήτες (Ship-owners), διαχειριστές πλοίων (Ship-operators) και ναυλωτές (Charterers) και γι' αυτό το λόγο δεν περιορίζεται μόνο σε απώλεια ή βλάβη στο πλοίο, αλλά καλύπτει και την ευθύνη του προς τρίτους, όπως οι ιδιοκτήτες φορτίου ή οι ασφαλιστές τους, το πλήρωμα, οι επιβάτες και άλλοι.

Τα P&I Clubs δημιούργησαν το 1889 το International Group of P&I Clubs (IGPANDI) ή άλλως το Διεθνή Όμιλο Ενώσεων Προστασίας & Αποζημίωσης, που αριθμεί 13 διαφορετικά clubs από όλον τον κόσμο. Μέσω του IGPANDI ασφαλίζεται για P&I risks το 90% του παγκόσμιου στόλου, καθώς αυτό έχει τη δυνατότητα να αγοράζει υψηλά επίπεδα αντασφάλισης σε συλλογική βάση επιτρέποντας έτσι σε κάθε Club να παρέχει υψηλότερα επίπεδα κάλυψης από αυτά που είναι κανονικά διαθέσιμα στην αγορά. Το IGPANDI για να γίνει κατανοητό λειτουργεί ως αντασφαλιστής των αλληλασφαλιστικών συνεταιρισμών. Κάθε σύλλογος (club) μέσα στον όμιλο (group) είναι μια ξεχωριστή μη κερδοσκοπική ένωση αμοιβαίας ασφάλισης παρέχοντας κάλυψη στα μέλη του, πλοιοκτήτες και ναυλωτές, έναντι τρίτων σε σχέση με τη διαχείριση των πλοίων. Επιπλέων, τα clubs έχουν τους δικούς τους τυπικούς και προκαθορισμένους κανόνες και συγχρόνως ενσωματώνουν ειδικά διαμορφωμένες ρήτρες στις κατά περίσταση ασφαλιστικές συμβάσεις που συνάπτουν.

Ωστόσο παρά το γεγονός ότι πολλά από τα παραγόμενα αποτελέσματα μιας κυβερνοεπίθεσης προσομοιάζουν αρκετά με το αντικείμενο ασφάλισης των P&I Clubs, στην πραγματικότητα τέτοιοι κίνδυνοι δεν ασφαλίζονται, καθώς τα P&I clubs ασφαλίζουν μόνο συγκεκριμένους κινδύνους και δεν παρέχουν γενική και πλήρη κάλυψη. Στη μη κάλυψη από τα P&I clubs, όπως είναι φυσικό, περιλαμβάνονται και απώλειες, που ενώ προκύπτουν από ένα περιστατικό που λαμβάνει χώρα στον κυβερνοχώρο κατά τη λειτουργία του πλοίου, δεν επιφέρουν αποτελέσματα που να απαιτούν την κάλυψη υποχρεώσεων έναντι τρίτων (το κατεξοχήν αντικείμενο κάλυψης από τα P&I clubs). Σχετικά παραδείγματα είναι η προκληθείσα οικονομική ζημία λόγω εισβολής κάποιου ιού στα συστήματα της εταιρίας ή το κόστος για την ανάκτηση χαμένων δεδομένων.

Όσον αφορά τους κυβερνοκινδύνους και την κάλυψη τους ή μη από τα P&I Clubs, δέον να αναφερθεί ότι οι περισσότεροι οργανισμοί έχουν ενσωματώσει τη Ρήτρα Εξαίρεσης από Επίθεση στον Κυβερνοχώρο (cyber – exclusion clause) CL380 / 10.11.2003, η οποία είναι αποδεκτή από όλους και θεωρείται ως η επικρατούσα στην αγορά ρήτρα για το συγκεκριμένο ζήτημα. Μάλιστα, η δεδομένη ρήτρα θεωρείται "paramount clause" είναι δηλαδή, πρωταρχικής σημασίας ρήτρα και υπερισχύει έναντι οτιδήποτε άλλου περιλαμβάνει η ασφάλιση.

Σε γενικές γραμμές, η CL380 εξαιρεί από την ασφαλιστική κάλυψη κάθε ζημία η απώλεια, η οποία προήλθε είτε άμεσα είτε έμμεσα από τη χρήση ή λειτουργία ενός υπολογιστή και των λογισμικών προγραμμάτων του[43]. Ωστόσο, για να εξαιρεθούν από την κάλυψη τέτοιου είδους ζημίες ή απώλειες, οι οποίες είναι απότοκες της χρήσης υπολογιστή, σύμφωνα με την CL380, είναι απαραίτητο η χρήση του υπολογιστή να γίνεται επί τούτου γι' αυτόν τον σκοπό, δηλαδή να χρησιμοποιείται ως μέσο για την πρόκληση της ζημίας. Υπάρχει μία αδυναμία στη συγκεκριμένη ρήτρα όσον αφορά τη διατύπωση " *ως μέσο για την πρόκληση βλάβης*". Όπως συμβαίνει με τις περισσότερες εξαιρέσεις, έτσι και σε αυτήν, οι ασφαλιστές είναι αυτοί που πρέπει ν' αποδείξουν πιθανολογικά στην κάθε περίπτωση που εξετάζουν, ότι ο υπολογιστής κ.α. χρησιμοποιήθηκε ως μέσο με σκοπό την πρόκληση βλάβης. Επίσης, ασαφές παραμένει, αν ο ασφαλισμένος πρέπει να είναι ο επιδιωκόμενος στόχος του δράστη ή αν ο αποκλεισμός που ορίζει η ρήτρα εφαρμόζεται και όταν ο ασφαλισμένος δεν είναι ο αρχικός στόχος, αλλά είναι το θύμα κάποιας παράπλευρης επίθεσης έναντι τρίτου. Η Ρήτρα Εξαίρεσης από Επίθεση

[43] Παρατίθεται και η αγγλική διατύπωση"….in no case shall this agreement cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system." (Institute Cyber Attack Exclusion Clause – CL380)

στον Κυβερνοχώρο, όπως είναι φυσικό, γεννά πλήθος ερωτημάτων, αφού η εφαρμογή της επαφίεται αποκλειστικά στην ερμηνεία που δίνουν κατά περίσταση οι ασφαλιστές, κυρίως λόγω της έλλειψης νομολογίας από τα αγγλικά δικαστήρια.

Ο υπολογιστής ή το κάθε ηλεκτρονικό σύστημα, σε τι πλαίσιο θεωρείται το υπαίτιο μέσο για την πρόκληση της ζημίας ή της απώλειας; Για να γίνει κατανοητή το ερώτημα, ας εξεταστεί το εξής απλοϊκό και συνάμα ακραίο παράδειγμα· ένας κλέφτης αποσπάει ένα φορτίο από τον τερματικό λιμένα χτυπώντας τον αρμόδιο υπάλληλο στο κεφάλι μ' έναν λοστό. Στην προκειμένη περίπτωση, η ανάμειξη των ασφαλιστών θεωρείται δεδομένη, καθώς αυτοί εμπλέκονται τόσο για την απώλεια του φορτίου όσο και για τον τραυματισμό του υπαλλήλου. Αν τώρα, ο κλέφτης της προηγούμενης υπόθεσης αποσπάσει το φορτίο, χτυπώντας όμως τον υπάλληλο στο κεφάλι μ' έναν υπολογιστή (το μέσο για την πρόκληση της ζημίας), τι γίνεται όσον αφορά την ασφαλιστική κάλυψη; Οι ασφαλιστές σε αυτήν την περίπτωση θα εφαρμόσουν την ρήτρα εξαίρεσης CL380 με βάση τα όσα ορίζονται σε αυτήν, αφού "*εξαιρεί από την ασφαλιστική κάλυψη κάθε ζημία η απώλεια, η οποία προήλθε είτε άμεσα είτε έμμεσα από τη χρήση ή λειτουργία ενός υπολογιστή*" και δε θα εμπλακούν στην απαίτηση των εγειρόμενων αξιώσεων. Επιπροσθέτως, όταν η σχετική ζημία που εκ πρώτης όψεως συγκεντρώνει τα χαρακτηριστικά τα οποία απαιτούνται από την CL380, αλλά προκαλείται από κάποιον ακούσια, θα εξαιρεθεί τελικά από την κάλυψη ή όχι; Τέλος, τι θα γίνει, αν αυτή οφείλεται σε κάποιο τεχνικό λάθος κατά τη διάρκεια αναβάθμισης ή συντήρησης των ηλεκτρονικών συστημάτων;

Σε συνέχεια των ανωτέρω, χρήσιμο θα ήταν να εξεταστεί, ποια είναι η γενική προσέγγιση των 13 clubs, που ανήκουν στο IGPANDI, σχετικά με τους κυβερνοκινδύνους και την αντίστοιχη ή μη, κάλυψή τους και ποια από αυτά έχουν ενσωματώσει τη Ρήτρα Εξαίρεσης από Επίθεση στον Κυβερνοχώρο (CL380), καθώς η τελική ασφαλιστική κάλυψη που ακολουθείται από κάθε club υπόκειται αποκλειστικά στους δικούς του κανόνες. Οι κάτωθι αναφορές γίνονται με βάση την πιο πρόσφατη έκδοση των κανόνων του εκάστοτε συλλόγου. Τα P&I clubs παρατίθενται με την ίδια σειρά, όπως αυτά παρουσιάζονται, στην επίσημη ιστοσελίδα του Διεθνή Ομίλου Ενώσεων Προστασίας & Αποζημίωσης[44].

4.5.1 American P&I club

[44] https://www.igpandi.org/group-clubs

Το συγκεκριμένο club δεν ενσωματώνει την τη Ρήτρα Εξαίρεσης από Επίθεση στον Κυβερνοχώρο (cyber – exclusion clause) CL380, το οποίο σαν πρακτική είναι αρκετά σπάνιο και δε συναντάται εύκολα στα υπόλοιπα P&I clubs, που ανήκουν στο IGPANDI.

Ωστόσο, το club αποκλείει όλες τις υποχρεώσεις που απορρέουν από τα ηλεκτρονικά συστήματα συναλλαγών[45], όπως τις ηλεκτρονικές φορτωτικές.

4.5.2 The Britannia P&I club

Σύμφωνα με το βιβλίο κανόνων του club η ρήτρα εξαίρεσης Cl. 380 δεν ενσωματώνεται στην πολιτική του, ούτε περιλαμβάνει οποιαδήποτε εξαίρεση που να σχετίζεται με τη χρήση υπολογιστή.

4.5.3 Gard P&I club

Το Gard ενσωματώνει τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο Cl.380. Στους κανόνες που διατρέχουν την πολιτική του club για το τρέχον έτος και συγκεκριμένα στο παράρτημα 1 " πρόσθετες ασφάλειες" αναφέρεται στον αποκλεισμό των καλύψεων για βλάβη που προκαλείται από υπολογιστή, από πρόγραμμα λογισμικού, από κακόβουλο ιό ή από κάθε άλλο ηλεκτρονικό σύστημα.

4.5.4 The Japan P&I club

Το συγκεκριμένο club διαχωρίζει τους κίνδυνος στον κυβερνοχώρο σε εσωτερικούς και σε εξωτερικούς. Όπως αναφέρεται στο "βιβλίο κανόνων" του, δεν παρέχει κάλυψη για τους εσωτερικούς κυβερνοκινδύνους.

4.5.5 The London P&I club

[45] Electronic Trading System: είναι ένα ηλεκτρονικό σύστημα συναλλαγών είναι οποιοδήποτε σύστημα το οποίο αντικαθιστά ή θα αντικαταστήσει τα έντυπα έγγραφα (paperless trading) που χρησιμοποιούνται για την πώληση εμπορευμάτων ή και για τη θαλάσσια μεταφορά τους ή εν μέρει δια θαλάσσης.

Το London P&I club ενσωματώνει στην πολιτική του τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο Cl. 380. Επίσης αποκλείει υποχρεώσεις, ζημίες και έξοδα που προκύπτουν από τη χρήση οποιουδήποτε ηλεκτρονικού συστήματος συναλλαγών, ομοίως με την τακτική που ακολουθούν και τα υπόλοιπα clubs στη συγκεκριμένη εξαίρεση.

4.5.6 The North of England P&I club

Το club αποκλείει τις ευθύνες που εγείρονται από οποιοδήποτε ηλεκτρονικό σύστημα συναλλαγής. Όσον αφορά τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο, το συγκεκριμένο club δεν την ενσωματώνει ακριβώς στην πολιτική του, αλλά εξαιρεί μόνο ότι προκύπτει από τη χρήση υπολογιστή.

4.5.7 The Shipowners' P&I club

Το club, κατανοώντας την πραγματική έκταση των ευπαθειών του κυβερνοχώρου, προσπαθεί να ενημερώνει σε τακτά χρονικά διαστήματα τα μέλη του σχετικά με ανάλογα ζητήματα που ανακύπτουν. Μάλιστα, το 2017 φιλοξένησε ένα διαδικτυακό σεμινάριο με τον τίτλο "Maritime Cyber Security Webinar" προκειμένου να βοηθήσει τα μέλη του να κατανοήσουν πόσο σημαντικό είναι να βρίσκονται σε ετοιμότητα απέναντι σε κυβερνοαπειλές, αλλά και να παρουσιάσει σε αυτά την πολιτική που ακολουθεί όσον αφορά την αντιμετώπιση αξιώσεων που εγείρονται από παρόμοιους κινδύνους.

Το Shipowners' club ακολουθεί την συνήθη πρακτική των περισσότερων clubs και ενσωματώνει τη Ρήτρα Εξαίρεσης Cl. 380. Ωστόσο, στη μη κάλυψη ζημιών που προέρχονται από τη χρήση υπολογιστή προσθέτει και την όποια ζημία προκαλείται από οποιοδήποτε " Χημικό, Βιοχημικό ή ηλεκτρομαγνητικό όπλο". Αξίζει στο σημείο αυτό να παρατεθεί η άποψη του κ. Nicholas Gooding[46], όπως διατυπώθηκε από τον ίδιο στο Συνέδριο "*Insurance Sweden Conference*", που πραγματοποιήθηκε στην Στοκχόλμη τον Μάιο του 2015. Η ρήτρα 380 κυκλοφόρησε την ίδια ημερομηνία με τη ρήτρα εξαίρεσης 370, δηλαδή τη ρήτρα εξαίρεσης από Χημικό, Βιολογικό, Βιοχημικό ή ηλεκτρομαγνητικό όπλο. Πλέον, ο κ. Gooding, ο οποίος είναι αυτός μάλιστα, που σχεδίασε τη Cl.380, θεωρεί ότι η ήταν

[46] Ο κ. Nicholas Gooding, υπήρξε κορυφαίος ασφαλιστής στην αγορά του Λονδίνου και πλέον εκπροσωπεί, ως αναπληρωτής αξιωματούχος, τη Διεθνή ένωση Θαλάσσιων Ασφαλίσεων (IUMI) στον Διεθνή Ναυτιλιακό Οργανισμό (IMO).

λανθασμένη επιλογή η ταυτόχρονη κυκλοφορία των δύο ρητρών, καθώς αυτό το γεγονός οδήγησε στην κατάχρηση της Ρήτρας Εξαίρεσης από Επίθεση στον Κυβερνοχώρο, ήτοι της Cl.380.

Τέλος, το Shipowners' P&I club αποκλείει από την κάλυψη που προσφέρει κάθε ευθύνη, απώλεια ή ζημία απορρέουσα από το ηλεκτρονικό σύστημα συναλλαγής.

4.5.8 Skuld P&I club

Σύμφωνα με τους πιο ενημερωμένους κανόνες του club, οι οποίοι αφορούν την πολιτική που ακολουθεί το Skuld και έχουν τεθεί σε ισχύ από τις 20 Φεβρουαρίου του 2020 (*2020 P&I Rules*), αυτό δεν προσφέρει καμία κάλυψη σχετική με την κυβερνοασφάλεια. Επίσης, όπως ορίζει στην ενότητα των εξαιρέσεων και συγκεκριμένα στην υπ' αριθ. 30.4.4 περίπτωση, εξαιρεί από την κάλυψή του ευθύνες και έξοδα που προκύπτουν από τη χρήση ενός ηλεκτρονικού συστήματος συναλλαγών, εκτός και αν αυτό το σύστημα έχει εγκριθεί από το IGPANDI.

4.5.9 The Standard Club

Το club αποκλείει τις ευθύνες που εγείρονται από οποιοδήποτε ηλεκτρονικό σύστημα συναλλαγής και ενσωματώνει τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο,Cl.380.

4.5.10 The Steamship P&I club

Το Steamship P&I club ενσωματώνει τη ρήτρα εξαίρεσης Cl. 380. Επίσης, εξαιρεί από την κάλυψή του ο, οτιδήποτε ανακύπτει (απώλειες, ζημίες, κόστη, ευθύνες) από το σύστημα ηλεκτρονικών συναλλαγών.

4.5.11 The Swedish Club

Το club εξαιρεί κάθε ευθύνη, κόστη και έξοδα, τα οποία προκλήθηκαν από τη χρήση υπολογιστή ή συστήματος υπολογιστή. Ενσωματώνει τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο και αποκλείει οτιδήποτε προκύπτει από ηλεκτρονικό σύστημα συναλλαγής.

4.5.12 UK P&I club

Το UK P&I club ακολουθεί τη συνήθη πολιτική των υπολοίπων clubs και ενσωματώνει τη ρήτρα εξαίρεσης από επίθεση στον κυβερνοχώρο Cl. 380. Επίσης αποκλείει υποχρεώσεις, ζημίες και έξοδα που προκύπτουν από τη χρήση οποιουδήποτε ηλεκτρονικού συστήματος συναλλαγών (paperless trading). Τα ηλεκτρονικά συστήματα συναλλαγών θα μπορούσαν να είναι ευάλωτα σε κυβερνοεπιθέσεις. Εξαιρεί επομένως, από την κάλυψη και κάθε ευθύνη, απώλεια, ή κόστη που γεννούνται από μια κυβερνοεπίθεση, η οποία επηρεάζει ένα εγκεκριμένο ηλεκτρονικό σύστημα, παρά το γεγονός ότι ο συγκεκριμένος αποκλεισμός δεν κάνει ρητή και συγκεκριμένη αναφορά σε κυβερνοκινδύνους.

4.5.13 The West of England P&I club

Το West of England P&I club ενσωματώνει τη ρήτρα εξαίρεσης Cl. 380. Επίσης, εξαιρεί από την κάλυψή του ο, οτιδήποτε ανακύπτει από τις ηλεκτρονικές συναλλαγές.

Όλα τα μέλη του συλλόγου επωφελούνται από το ίδιο επίπεδο ασφάλισης σε περίπτωση που προκύψει αξίωση από κάποιο περιστατικό στον κυβερνοχώρο, όπως θα συνέβαινε και με κάθε άλλο θαλάσσιο κίνδυνο. Κανένα P&I club δεν προσφέρει ξεχωριστή ασφάλεια για κυβερνοκινδύνους, εκτός αν εμπίπτουν σε κάποιον συνηθισμένο κίνδυνο που καλύπτεται από το club.

Ωστόσο, λόγω της μεταβατικής περιόδου επί του παρόντος ζητήματος και της έλλειψης μιας συγκεκριμένης ασφαλιστικής πολιτικής, είναι λογικό ότι, εάν προκύψει μία αξίωση σχετιζόμενη με κίνδυνο στον κυβερνοχώρο, ο πλοιοκτήτης, ο διαχειριστής ή ο ναυλωτής θα πρέπει να αποδείξει στον ασφαλιστή του ότι είχε λάβει τα κατάλληλα μέτρα προκειμένου να αποτρέψει το συμβάν. Δε μπορούν τα σχετιζόμενα πρόσωπα να αγνοήσουν την ανάγκη λήψης απαιτούμενων μέτρων έχοντας την πεποίθηση ότι το P&I club στο οποίο ανήκουν θα καλύψει την ζημία, την απώλεια ή την οποιαδήποτε ευθύνη έναντι τρίτου που θα προκύψει. Όσο ο καιρός περνά και κυρίως τώρα που βρισκόμαστε προ των πυλών του 2021 και της καθολικής εφαρμογής του ψηφίσματος MSC.428(98) του IMO σχετικά με την ενίσχυση της κυβερνοασφάλειας, οι ασφαλιστές περισσότερο από ποτέ περιμένουν να δουν σωστή και αποτελεσματική διαχείριση του κυβερνοκινδύνου τόσο στη ξηρά όσο και στα πλοία.

Συμπεράσματα

Η κυβερνοασφάλεια αποτελέι πλέον μια πραγματικότητα στη ναυτιλική βιομηχανία. Όλες οι εταιρίες είναι απαραίτητο να λάβουν τα κατάλληλα μέτρα προκειμένου να διαχειριστούν αποτελεσματικά κάθε κυβερνοκίνδυνο, αλλά και κάθε περιστατικό που μπορεί να λάβει χώρα. Ο σημαίνων ρόλος της στην υγειή λειτουργία μιας εταιρίας έχει πολλάκις αναφερθεί, αλλά αξίζει να αντιπαραβάλλουμε σαν παράδειγμα την οικία μας, ώστε να κατανοήσουν οι ειθύνοντες ότι η κυβερνοασφάλεια πρέπει να αποτελεί την προτεραιότητά τους. Κανείς δε φεύγει από το σπίτι του αφήνοντας ξεκλείδωτή ή ανοιχτή την πόρτα, γιατί επομένως να αφήσει κάποιος μια εταιρία, ένα πλοίο, ένα φορτίο, ένα πλήρωμα, απροσταύτετο απέναντι σε κάποιον κυβερνοκίνδυνο;

Η θαλάσσια ασφάλιση, αναφορικά με την κάλυψη των κυβερνοκινδύνων, πρέπει να δρα παράλληλα και επικουρικά με τα μέτρα προστασίας, που λαμβάνει κάθε εταιρία προς αυτόν τον σκοπό. Η σημασία της είναι μεγάλη, αφού θα ανακουφίσει τις εταιρίες, παρέχοντας προστασία από τις οικονομικές επιπτώσεις μιας κυβερνοεπίθεσης και βοηθώντας, όσους καθημερινά αγωνίζονται για την ασφάλεια και την προστασία των δεδομένων. Ωστόσο, οι ασφαλιστές παραμένουν επιφυλαχτικοί απέναντι στους κυβερνοκινδύνους, κυρίως λόγω πολύπλοκης φύσης τους και των αμέτρητων και απρόβλπετων συνεπειών τους.

Οι συνεχόμενες κυβερνοεπιθέσεις που συμβαίνουν στη ναυτιλιακή βιομηχανία και η επικείμενη καθολική εφαρμογή του ψηφίσματος MSC.428(98) του IMO, σίγουρα θα αποτελέσουν το ερέθισμα για τη δημιουργία αντίστοιχων ασφαλιστικών προϊόντων. Η βιομηχανία των θαλάσσιων ασφαλίσεων, αργά ή γρήορα, θα αναγκαστεί λόγω των συνθηκών να συμμορφωθεί με την νέα πραγματικότητα.

Εν κατακλειδει, τα υπάρχοντα ασφαλιστικά προγράμματα που σχετίζονται με την κυβερνοασφάλεια δεν έχουν λάβει την τελική τους μορφή, γιατί συνεχώς προκύπτουν νέες απαιτήσεις, οι οποίες πρέπει να καλυφθούν. Στο πλαίσιο αυτό, θα πρέπει τόσο οι ναυτιλιακές εταιρίες να επιδεικνύουν τη δέουσα επιμέλεια αναφορικά με την ασφάλεια στον κυβερνοχώρο όσο και οι ασφαλιστές να είναι ενήμεροι για τον τρόπο που λειτουργεί η κάθε εταιρία, τα μέτρα προστσίας που εφαρμόζει έναντι στους κυβερνοκινδύνους και ποιες είναι οι ακριβείς διαδικασίες και οι μηχανισμοί που ακολουθεί προκειμένου ν' αντιμετωπίσει μια κυβερνοεπίθεση[47].

[47] Απόσπασμα από το webinar «Cyber Security in the maritime Environment» που πραγματοποιήθηκε στις 04.02.2021 υπό την αιγίδα της Alpha Marine Consulting P.C & την Diaplous Cyber.

Μόνο με βάση αυτές τις αρχές θα προκύψουν ασφαλιστήρια συμβόλαια που θα καλύπτουν τους κυβερνοκινδύνους και συγχρόνως θα προστατεύουν τις ναυτιλιακές εταιρίες και τους ασφαλιστές.

ΠΗΓΕΣ

Βιβλιογραφία:

A. Karitzis & Associates L.L.C. Advokatfirmaet Selmer AS. Ana Cristina Pimentel & Associados, Sociedade de Advogados, SP RL, Arias, Fábrega & Fábrega, Banwo & Ighodalo, et.al (2019). The International Comparative Legal Guide to: Shipping Law 2019 (7th edition). Rory Smith.

Bennett Howard (2006). The Law of Marine Insurance (2nd edition). Oxford University Press.

Hodges Susan (1996). Law of Marine Insurance. Cavendish Publishing Limited.

Merkin Robert (2010). Marine Insurance Legislation (4th edition). MPG Books.

Soyer Baris (2006).Warranties in Marine Insurance (2nd edition). Cavendish Publishing Limited.

Institute of Chartered Shipbrokers (2015). Marine Insurance

Γκατζόλη Α.(2017). Λειτουργική Διαχείριση Πλοίου

Αρθρογραφία & Papers:

Ξενόγλωσση

Adrian Durkin & Colin Gillespie (2018). Cyber Risk and Marine Insurance: Mind the Gap: https://safety4sea.com/cyber-risk-marine-insurance-mind-gap/

Allianz Global Corporate & Specialty. Q&A: Cyber risk on the rise in shipping: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-risk-on-the-rise-in-shipping.html

Allianz Global Corporate & Specialty (2015). Shipping losses lowest for 10 years, but mega-ships and cyber-attacks pose new threats for maritime sector: https://www.agcs.allianz.com/news-and-insights/news/safety-shipping-review-2015.html

A.P. Moller – Maersk (2017). Cyber-attack update: https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Batini Alberto for IUMI (2017). Cyber Marine Insurance: are we ready? https://iumi.com/news/iumi-eye-newsletter-september-2017/cyber-marine-insurance-are-we-ready

Clarkson PLC (2017). Notice of cyber security incident https://www.clarksons.com/media/1129201/notice_of_cyber_security_incident.pdf

Cyprus Shipping Chamber (2017). Cyber Security Case Study: https://csc-cy.org/wp-content/uploads/2018/06/Cyprus-Shipping-Chamber-Cyber-Security-Case-Study.pdf

DNV – GL. Cyber security awareness: https://www.dnvgl.com/maritime/webinars-and-videos/videos/cyber-security-awareness.html

ENISA (2011). Analysis of cyber security aspects in the maritime sector file:///C:/Users/petra%20chita/Downloads/2011_ENISA_Analysis_of_cyber_security_aspects_in_the_maritime_sector_1%200.pdf

Gard P&I Club – Rules 2020. https://www.gard.no/Content/29167884/Rules%202020_web.pdf

Goud Naveen. Cyber Attack on COSCO: https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/

Hadwin Steven (2016). Cyber risks and the maritime industries: risk identification, mitigation and response https://www.nortonrosefulbright.com/en/knowledge/publications/e57a8885/cyber-risks-and-the-maritime-industries-risk-identification-mitigation-and-response

Handy Shipping Guide (2018). Cyber Security Boss Says Marine Insurance Industry is Outdated and Needs an Update: https://www.handyshippingguide.com/shipping-news/cyber-security-boss-says-marine-insurance-industry-is-outdated-and-needs-an-update_9392

IHS Fairplay – John Guy (2016). Cyber security threat worries marine insurers: http://edgegroup.com/cyber-security-threat-worries-marine-insurers/

IUA of London in Association with Norton Rose Fulbright LLP (2016). Cyber Risks and Insurance:https://www.maritimelondon.com/wpcontent/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf

IUA publishes Cyber Exclusion Clauses (2019). https://www.iua.co.uk/IUA_Member/Press/Press_Releases_2019/IUA_publishes_cyber_exclusion_clauses.aspx

Japan P&I club (May 2018). P&I Loss Prevention Bulletin https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf

Japan P&I club – Rules 2020. https://www.piclub.or.jp/attachment/insurance_guidebooks/Rules%202020.pdf

Kapalidis Chronis (2018). 4 Cases of Cyber Security Failures in Shipping History. https://www.linkedin.com/pulse/4-cases-cyber-security-failures-shipping-history-chronis-kapalidis/

Lange Lars for IUMI (2017). IUMI cooperates with shipowners and classification societies on cyber security https://iumi.com/news/iumi-eye-newsletter-june-2017/iumi-cooperates-with-shipowners-and-classification-societies-on-cyber-security

Maersk: Ransomware Incident Business Impact (2017): https://www.maritimecyberadvisors.com/

Offshore Energy (2018). COSCO Shipping Lines Falls Victim to Cyber Attack https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/

Osborne Charlie (2018). Clarksons says single user account to blame for data breach. https://www.zdnet.com/article/clarkson-says-single-user-account-to-blame-for-data-breach/

Safety4sea (2018). Maersk Line: Surviving from a cyber-attack. https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

Schuler Mike (2018). Clarkson Plc Reveals Details of 2017 Cyber Security Incident. https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/

Skuld P&I club – Rules 2020. https://www.skuld.com/products/Conditions/pi-rules/2020-pi-rules/

The North of England P&I Association (July 2017). Cyber Risks in Shipping file:///C:/Users/petra%20chita/Downloads/Cyber-Risks-in-Shipping-LP-Briefing.pdf%20(4).pdf

The North of England P&I Association – Rules 2020. file:///C:/Users/petra%20chita/Downloads/PI-Rules-2019-20.pdf

The West P&I club – Rules 2020. file:///C:/Users/petra%20chita/Downloads/Rules-of-Classes-2020-web%20(1).pdf

Threats at Sea: A Security Evaluation of AIS (2014). https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais

UK P&I club Q&A document (March 2018). Cyber Risks and P&I insurance https://safety4sea.com/wp-content/uploads/2018/03/UK-PI-Club-Cyber-Risks-and-PI-insurance-2018_03.pdf

Ελληνική

e Nautilia (2017). Συνέρχεται από την κυβερνοεπίθεση που την "γονάτισε" η Maersk https://e-nautilia.gr/synerhetai-apo-thn-kyvernoepithesi-pou-thn-gonatise-h-maersk/

The SeaNation (2018). Κυβερνοεπίθεση δέχθηκε η Cosco στις ΗΠΑ https://bit.ly/3peBlbC

Γιαννοπούλου Κατερίνα (2019). Ναυτιλία και Κυβερνοασφάλεια. https://www.huffingtonpost.gr/entry/naetilia-kai-kevernoasfaleia_gr_5cadae14e4b0a15bb479654f

Κακαμούκας Β. (2019). Cyber Risk στη ναυτιλία: Πραγματικός κίνδυνος ή ένας ακόμα μύθος; https://www.isalos.net/2019/11/cyber-risk-sti-naftilia-pragmatikos-kindynos-i-enas-akoma-mythos/

Καπτ. Γεωργούλης Γ. (2018). Κυβερνοεπιθέσεις στη ναυτιλία: η σύγχρονη απειλή μπορεί να περιοριστεί: https://www.isalos.net/2018/08/kyvernoepitheseis-sti-naftilia-i-synchroni-apeili-borei-na-perioristei/

Ναυτικά Χρονικά (2018). Θύμα κυβερνοεπίθεσης η COSCO Shipping Lines. https://www.naftikachronika.gr/2018/07/25/thyma-kyvernoepithesis-i-cosco-shipping-lines/

Τσαμόπουλος Μηνάς (2018). Θύμα κυβερνοεπίθεσης η Cosco μετά την Maersk. https://www.newmoney.gr/roh/palmos-oikonomias/nautilia/thima-kibernoepithesis-i-cosco-meta-tin-maersk/

Χρυσανθοπούλου Λαλέλα (2017). Πώς η κυβερνο-επίθεση στη Maersk χτύπησε την παγκόσμια ναυτιλία. https://insuranceworld.gr/40985/eidiseis/diethni-eidiseis/pos-i-kyverno-epithesi-sti-maersk-chtypise-tin-pagkosmia-naftilia/

Κανονισμοί, Οδηγίες, Νομοθεσία:

Glencore International vs MSC Mediterranean Shipping Company (case study) https://www.onlinedmc.co.uk/index.php/Glencore_International_v_MSC_Mediterranean_Shipping_Company

IMO, Guidelines on Maritime Cyber Risk Management: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO, Interim Guidelines on Maritime Cyber Risk Management: https://www.standard-club.com/media/2207683/imo-interim-guidelines.pdf

International Safety Management (ISM) Code: https://www.classnk.or.jp/hp/pdf/activities/statutory/ism/ism_cd/ism-code-e.pdf

ISO/IEC 27001 standard on Information technology: https://www.iso.org/isoiec-27001-information-security.html

Marine Insurance Act 1906: https://www.legislation.gov.uk/ukpga/Edw7/6/41/contents

Marine Insurance Act 2015: https://www.legislation.gov.uk/ukpga/2015/4/pdfs/ukpga_20150004_en.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation 19 of SOLAS: Carriage Requirements for Shipborne Navigational Systems and Equipment https://www.liscr.com/sites/default/files/SOLAS%20V_Reg19.pdf

The Guidelines on cyber security on board ships (2017): https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

Webinars:

“Cyber security στη Ναυτιλία: Μια νέα πραγματικότητα ή business as usual?” από την Isalos.net και τα Ναυτικά Χρονικά.

“Cyber Security” από το 2020 SAFETY4SEA Virtual Forum

“Maritime security webinar” από το Shipowners’ P&I Club (2017).

“Cyber Security in the Maritime Environment” υπό την αιγίδα των Alpha Marine Consulting P.C & Diaplous Cyber (2021).