ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Maritime Cyber Security

Κοντοστέργιος Ιωάννης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Φιλιππόπουλος Ιωάννης

Λαμία, Ιούνιος 2018

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Maritime Cyber Security

Kontostergios John

Master thesis

Filippopoulos John

Lamia, June 2018

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Περίληψη

Η ναυτιλία είναι ένας τομέας ζωτικής σημασίας για την ευρωπαϊκή αλλά και την παγκόσμια κοινωνία και οικονομία γενικότερα. Η σημασία αυτή εκφράζεται μέσα από την συνεχή αύξηση της εξάρτησης κοινωνίας και οικονομίας από τις θαλάσσιες μεταφορές. Η βελτιστοποίηση των σύγχρονων ναυτιλιακών δραστηριοτήτων όμως, βασίζεται ολοένα και περισσότερο στις τεχνολογίες των πληροφοριών και των επικοινωνιών. Έτσι, σήμερα, βασικές ναυτιλιακές δραστηριότητες, από τη ναυσιπλοΐα έως την πρόωση, από τη διαχείριση των εμπορευματικών μεταφορών έως τις επικοινωνίες παντός τύπου, κ.λπ., δείχνουν να εξαρτώνται από συστήματα πληροφοριών και επικοινωνιών.

Η αυξανόμενη εξάρτηση των τελευταίων ετών, όμως, όλων των τομέων της βιομηχανίας, από τα συστήματα πληροφοριών και επικοινωνιών, συνοδεύεται και από μια παράλληλα αυξανόμενη εμφάνιση απειλών και επιθέσεων στον κυβερνοχώρο που μπορούν να οδηγήσουν σε σκόπιμη διακοπή κρίσιμων συστημάτων αυτοματοποίησης και να έχουν σημαντικό αντίκτυπο σε υποδομές ζωτικής σημασίας. Η διακοπή ή η μη διαθεσιμότητα των συστημάτων πληροφοριών και επικοινωνιών μπορεί να έχει καταστροφικές συνέπειες για τις κυβερνήσεις των ευρωπαϊκών κρατών αλλά και την κοινωνική ευημερία γενικότερα. Η ανάγκη διασφάλισης της αξιοπιστίας και της ευρωστίας των συστημάτων αυτών κατά των επιθέσεων στον κυβερνοχώρο αποτελεί βασική πρόκληση σε εθνικό, πανευρωπαϊκό και διεθνές επίπεδο.

Κάτι ανάλογο ισχύει και για τον τομέα της ναυτιλίας, όπου η ανάλυση της ασφάλειας στον κυβερνοχώρο αποτελεί σημαντική πτυχή της συνεχόμενης ανάπτυξης του τομέα αυτού. Οι παντός φύσεως ναυτιλιακές δραστηριότητες, από τη στιγμή που εξαρτώνται σε μεγάλο βαθμό από την ορθή λειτουργία των σύγχρονων ψηφιακών επικοινωνιακών και πληροφοριακών συστημάτων, δεν θα μπορούσαν να αποτελέσουν εξαίρεση παρουσιάζοντας ανοσία στην αποδιοργάνωση των συστημάτων αυτών. Η ανάδειξη επομένως των πλεονεκτημάτων των σύγχρονων τεχνολογιών στον τομέα της ναυτιλίας απαιτεί τη γνώση και ανάπτυξη στρατηγικών αντιμετώπισης των αναπόφευκτων ζητημάτων ασφάλειας που συνοδεύουν τα σύγχρονα συστήματα πληροφοριών και επικοινωνιών.

Στα πλαίσια της παρούσας πτυχιακής εργασίας παρουσιάζονται τα βασικά σημεία στα οποία μπορούν να δημιουργηθούν ζητήματα ασφάλειας στον κυβερνοχώρο και αφορούν τον τομέα της ναυτιλίας. Η ανάδειξη των τρωτών αυτών σημείων θα μπορούσε να χρησιμεύσει ως βάση για την ανάπτυξη στρατηγικών ασφάλειας στον κυβερνοχώρο στον τομέα της ναυτιλίας. Η υπόδειξη τέτοιων στρατηγικών αποτελεί έναν ακόμα σκοπό της παρούσας εργασίας.

Λέξεις κλειδιά: Ανθρώπινος παράγοντας, ασφάλεια στον κυβερνοχώρο, κυβερνο-επιθέσεις, κυβερνοχώρος, λιμάνια, ναυτιλία, ναυτιλιακές υποδομές, πλοία, συστήματα πληροφοριών και επικοινωνιών.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Abstract

Maritime is a field of vital importance to European but also to global society and economy in general. This importance is reflected in the continuous increase in the dependence of society and economy on maritime transport. However, the optimization of modern maritime activities is increasingly based on information and communication technologies. Thus, today, basic maritime activities, from navigation to propulsion, from freight management to all types of communications, etc., seem to be dependent on information and communication systems.

However, recent years have proved that the growing dependence of all sectors of industry in information and communication systems is also accompanied by a growing number of cyber threats and attacks that can lead to deliberate disruption of critical automation systems and have a significant impact on critical infrastructure importance. Disruption or unavailability of information and communication systems can have devastating consequences for European governments, as well as social welfare in general. The need to ensure reliability and robustness of these systems against cyber-attacks is a key challenge at national, pan-European and international level.

Maritime industry could not be immune to such issues and thus cyber security analysis is an important aspect. Since all maritime activities depend to a large extent on the proper functioning of modern digital communication and information systems, could not be an exception by showing immunity to the disruption of these systems. The emergence of the benefits of modern maritime technologies therefore requires the knowledge and development of strategies to tackle the inevitable security issues that accompany modern information and communication systems.

This thesis presents the basic cyber security issues in the maritime field. The emergence of these vulnerabilities could serve as a basis for the development of cyber security strategies in the maritime sector. The suggestion of such strategies is another purpose of this paper.

Keywords: Cyber-attacks, cyber security, cyberspace, information and communication systems, human factor, maritime, maritime infrastructure, ports, ships.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Περιεχόμενα

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

1 Εισαγωγή

1.1 Θεωρητικό υπόβαθρο

Ο κυβερνοχώρος (cyber space) στη σύγχρονη ψηφιακή εποχή αποτελεί μια έννοια η οποία δημιουργεί νέα παγκόσμια σύνορα, όπως ακριβώς η εποχή της παγκοσμιοποίησης έφερε τον φυσικό κόσμο κοντά όπως ποτέ άλλοτε. Αυτή η εικονική σύνδεση δικτύων έχει αυξήσει εκθετικά την δυνατότητα για άμεση επικοινωνία, ενώ η αποτελεσματικότητά της δίνει την ευκαιρία δημιουργίας μιας πληθώρας άλλων χρηστικών δυνατοτήτων. Εκτός από τους κοινούς χρήστες, τις επιχειρήσεις και τους κυβερνητικούς φορείς, όλοι οι βιομηχανικοί κλάδοι και τομείς, ανάμεσα στους οποίους και η ναυτιλία (maritime), υιοθέτησαν και εφάρμοσαν με ενθουσιασμό τον κόσμο της τεχνολογίας της πληροφορίας στην καθημερινές δραστηριότητές τους. Οι σύγχρονες τεχνολογικές εξελίξεις έχουν ανοίξει δρόμους για εφαρμογές που παλαιότερα θεωρούνταν αδιανόητες. Ωστόσο, αυτή η εξάρτηση των βιομηχανικών κλάδων από την τεχνολογία, τους έχει εκθέσει σε όλους τους πιθανούς κινδύνους που μπορεί να προέρθουν από την κακόβουλη χρήση των τεχνολογιών αυτών.

Φυσικά, από τη στιγμή που η ίδια η τεχνολογία δεν αποτελεί κάποιο ζωντανό οργανισμό αλλά ούτε έχει γνώση της ίδιας της της ύπαρξης, η ορθή ή η κακόβουλη χρήση της εξαρτάται εξ ολοκλήρου από τον ανθρώπινο παράγοντα. Η εξέλιξη των τεχνολογιών αποσκοπεί στην παροχή μιας καλύτερης ποιότητας ζωής στους χρήστες. Τα πλεονεκτήματα χρήσης τους πολλές φορές θεωρούνται δεδομένα, όμως η σταδιακή υιοθέτησή τους από έναν εκθετικά αυξανόμενο αριθμό ατόμων, μπορεί τελικά να οδηγήσει σε αντίθετα αποτελέσματα. Με τον τρόπο αυτό, οι τεχνολογίες της σύγχρονης ψηφιακής εποχής έχουν εξελιχθεί σε εργαλεία διφορούμενης ηθικής, η οποία σε τελική ανάλυση καθορίζεται από τα άτομα που επηρεάζονται από την ορθή ή κακόβουλη χρήση των τεχνολογιών αυτών.

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) ορίζεται ως [1]: *«Η διασύνδεση μέσω του Διαδικτύου των υπολογιστικών συσκευών που ενσωματώνονται σε καθημερινά αντικείμενα, επιτρέποντάς τους να στέλνουν και να λαμβάνουν δεδομένα».* Αυτή ακριβώς η αόριστη έννοια του IoT έχει δημιουργήσει πλήθος συζητήσεων που αφορούν την ασφάλεια των ψηφιακών διασυνδέσεων. Η ψηφιακή τεχνολογία είναι αναμφισβήτητα το ταχύτερα αναπτυσσόμενο τεχνικό κατόρθωμα της σύγχρονης εποχής. Οι τηλεοράσεις έχουν γίνει λεπτότερες, πιο επίπεδες και μεγαλύτερες, τα οχήματά μπορούν να αντιλαμβάνονται αντικείμενα που βρίσκονται στον περιβάλλοντα χώρο τους και τα τηλέφωνα έχουν καταστεί ισχυροί υπολογιστές που μπορούν να μπουν στις τσέπες των χρηστών.

Η ασφάλεια στον κυβερνοχώρο (cyber security), γενικότερα, αφορά τη διατήρηση της ακεραιότητας και της διαθεσιμότητας πληροφοριών και συστημάτων, την επιβεβαίωση της συνέχισης της δραστηριότητας και τη συνεχή χρησιμότητα των ηλεκτρονικών στοιχείων που βρίσκονται στον κυβερνοχώρο [2]. Η σημασία της ασφάλειας στον κυβερνοχώρο έχει αυξηθεί στον ναυτιλιακό τομέα, καθώς ο αυξανόμενος αριθμός συσκευών και υπηρεσιών IoT που χρησιμοποιούνται και εφαρμόζονται στον τομέα της ναυτιλίας, έχει επηρεάσει θετικά και αρνητικά τον τομέα αυτό, όπως ακριβώς έχει παρατηρηθεί και σε όλους σχεδόν τους άλλους

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

βιομηχανικούς τομείς. Βέβαια, η χρήση υπολογιστών και ψηφιακών επικοινωνιών δεν αποτελεί καινοτομία στον χώρο της ναυτιλίας, καθώς οι τεχνολογίες ραδιοσυχνοτήτων χρησιμοποιούνται στον τομέα αυτό εδώ και δεκαετίες. Όμως, η χρήση των διασυνδεδεμένων στο Διαδίκτυο τεχνολογιών στον τομέα των θαλάσσιων μεταφορών και το μέγεθος της εμπιστοσύνης των ανθρώπων που χρησιμοποιούν τις τεχνολογίες αυτές, αποτελούν τη μεγαλύτερη απειλή που αντιμετωπίζει σήμερα ο ναυτιλιακός τομέας. Καθώς η χρήση των εφαρμογών IoT εξακολουθεί να παραμένει αόριστη, η ασφάλεια των ναυτιλιακών συστημάτων θα συνεχίσει να αποτελεί το πιο σημαντικό ζήτημα που αντιμετωπίζει ο τομέας της ναυτιλίας στο σύνολό της.

Τα δίκτυα υπολογιστών και επικοινωνιών αποτελούν, επίσης, τον πυρήνα των ευφυών συστημάτων μεταφορών (Intelligent Transport Systems - ITS). Τα συστήματα ITS είναι τεχνολογίες, εφαρμογές ή πλατφόρμες που βελτιώνουν την ποιότητα των μεταφορών, βασισμένα σε εφαρμογές που παρακολουθούν, διαχειρίζονται ή ενισχύουν τα συστήματα μεταφορών. Τα συστήματα αυτά έχουν βελτιώσει την αποτελεσματικότητα, τη συνοχή και την αποδοτικότητα του δικτύου μεταφορών. Σε σχέση με την ασφάλεια στον κυβερνοχώρο, οι βασικοί στόχοι ενός συστήματος μεταφορών είναι [3]:

- η ασφαλή λειτουργία όλων των τρόπων μεταφοράς
- η εκμετάλλευση και η αποτελεσματική μετακίνηση ανθρώπων, αγαθών και υπηρεσιών, και
- η ασφαλής επικοινωνία

Το ζήτημα της ασφάλειας στον τομέα της ναυτιλίας αποτελεί σημαντική πρόκληση στις μέρες μας. Η κατανόηση της ύπαρξης ασφάλειας στον κυβερνοχώρο στον τομέα της ναυτιλίας είναι σημαντική καθώς ο αριθμός των απειλών στον κυβερνοχώρο αυξάνεται ραγδαία ενώ παράλληλα ο συνεχώς αναπτυσσόμενος παγκόσμιος στόλος εξακολουθεί να εξαρτάται ολοένα και περισσότερο από την τεχνολογική εξέλιξη των συστημάτων πληροφοριών και επικοινωνίας [4].

1.2 Σκοπός της πτυχιακής εργασίας

Στη σύγχρονη έννοια του ναυτιλιακού τομέα, πλοία, λιμάνια και κάθε είδους ναυτιλιακής υποδομής είναι εξοπλισμένα με συστήματα που απαιτούν σύνδεση στο Διαδίκτυο. Μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει η ναυτιλιακή βιομηχανία είναι η παροχή ασφάλειας στη συνεχώς αυξανόμενη διασύνδεση στον κυβερνοχώρο.

Σκοπός της παρούσας πτυχιακής εργασίας είναι να παρουσιαστεί το πλήθος των σύγχρονων κυβερνο-απειλών που αντιμετωπίζει ο ναυτιλιακός τομέας στο σύνολό του. Για το σκοπό αυτό, στα πλαίσια της παρούσας πτυχιακής εργασίας θα γίνει μια παρουσίαση και μια ανάλυση των απειλών και των τρωτών σημείων που υπάρχουν στα συστήματα πληροφοριών και επικοινωνίας στον τομέα της ναυτιλίας, θα διερευνηθεί η ύπαρξη ή έλλειψη τεχνικών ασφάλειας στον κυβερνοχώρο, θα παρουσιαστούν οι τρέχουσες τεχνικές αντιμετώπισης των όποιων τρωτών σημείων και θα προταθούν κάποιοι τρόποι αντιμετώπισης των κυβερνο-απειλών.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

1.3 Δομή της πτυχιακής εργασίας

Στα πλαίσια της παρούσας πτυχιακής εργασίας, για την μελέτη της ασφάλειας στον κυβερνοχώρο στον τομέα της ναυτιλίας επιλέχθηκε η ακόλουθη δομή.

Στο κεφάλαιο 2 αναλύονται οι έννοιες του κυβερνοχώρου και της ασφάλειας του σε τέτοιο βαθμό ώστε να γίνει κατανοητή η αντίληψη της πλήρους διαδικασίας διαχείρισης του κυβερνοχώρου. Για το σκοπό αυτό θα γίνει μια συνοπτική περιγραφή των απειλών, των κινδύνων, των τρωτών σημείων και γενικά των γνωστών πτυχών που αφορούν τις κυβερνο-απειλές.

Στο κεφάλαιο 3 γίνεται μια ανάλυση της έννοιας της ασφάλειας στον κυβερνοχώρο που σχετίζεται με τον τομέα της ναυτιλίας. Αρχικά περιγράφονται οι στόχοι της κυβερνο-ασφάλειας αλλά και τα κίνητρα και οι δράστες των κυβερνο-επιθέσεων στο χώρο της ναυτιλίας. Στη συνέχεια δίνεται μια αναλυτική περιγραφή της σχέσης της ασφάλειας στον κυβερνοχώρο με τα λιμάνια και τα πλοία. Στα πλαίσια αυτής της σχέσης γίνεται μια αναφορά στα στοιχεία και τα συστήματα λιμανιών και πλοίων που μπορούν να θεωρηθούν ως τρωτά σημεία ασφάλειας στο κυβερνοχώρο, ενώ αναλύεται και η σημασία της κυβερνο-ασφάλειας για δύο αυτά βασικά στοιχεία της ναυτιλίας.

Το κεφάλαιο 4 περιλαμβάνει μια λεπτομερή ταξινόμηση και ανάλυση των κυβερνο-απειλών που αφορούν τον τομέα της ναυτιλίας.

Στο κεφάλαιο 5 γίνεται μια διερεύνηση των τεχνικών αντιμετώπισης των κυβερνο-επιθέσεων που αφορούν το χώρο της ναυτιλίας, καθώς και μια πρόταση σχετικά με την συνεχή επικαιροποίησή τους, ώστε να επιτευχθεί μια σταθερή θωράκιση ασφαλείας όλων των πιθανών τρωτών σημείων. Στο κεφάλαιο παρουσιάζεται μια σύνοψη των σημαντικότερων βιβλιογραφικών προσεγγίσεων που έχουν εκδοθεί κατά καιρούς και αφορούν τους τρόπους υλοποίησης της ασφάλειας στον κυβερνοχώρο.

Τέλος, η εργασία ολοκληρώνεται με κάποια συμπεράσματα που προκύπτουν από την ανάλυση της ασφάλειας στον κυβερνοχώρο στον τομέα της ναυτιλίας.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

2 Κυβερνοχώρος και Ασφάλεια

2.1 Κυβερνοχώρος

Ο όρος κυβερνοχώρος πρωτοεμφανίστηκε το 1984 όταν ο William Gibson δημοσίευσε το μυθιστόρημα «Neuromancer», στο οποίο ο κυβερνοχώρος περιγράφεται ως ένας τρισδιάστατος χώρος όπου οι καθαρές πληροφορίες μετακινούνται μεταξύ υπολογιστών και ομάδων υπολογιστών. Στο μυθιστόρημα, ο συγγραφέας προσδιορίζει τους ανθρώπους ως παραγωγούς και χρήστες πληροφοριών [5]. Σήμερα, ο κυβερνοχώρος μπορεί να γίνει κατανοητός ως ένας ηλεκτρονικός κόσμος, όπου πληροφορίες, λογισμικό και άνθρωποι συνυπάρχουν και ο οποίος επεκτείνεται στον φυσικό κόσμο. Σε ότι αφορά τη σύνδεσή του με υποδομές ζωτικής σημασίας, ο κυβερνοχώρος γίνεται ολοένα και περισσότερο θέμα συζητήσεων παγκόσμιας κλίμακας και βρίσκεται στο ίδιο επίπεδο αντιμετώπισης με άλλα σοβαρά ζητήματα που απασχολούν την ανθρωπότητα όπως η παγκόσμια έλλειψη νερού και οι κλιματικές αλλαγές. Ο κυβερνοχώρος έχει εξελιχθεί σε τέτοιο βαθμό που μπορεί να θεωρηθεί ως το νευρικό σύστημα των σύγχρονων κοινωνιών, καθώς είναι σε θέση να συνδέει άτομα και οργανισμούς σε παγκόσμιο επίπεδο. Στη περίπτωση που προκύψουν προβλήματα στον κυβερνοχώρο, όπως για παράδειγμα μια κυβερνο-επίθεση στον τομέα ενέργειας ενός κράτους, οι πολίτες του συγκεκριμένου κράτους γίνονται πολύ ευάλωτοι [6].

Ο κυβερνοχώρος αποτελείται από συνδυασμένα δίκτυα συστημάτων πληροφοριών και κυβερνο-φυσικών συστημάτων (Cyber-Physical Systems - CPS). Ένα σύστημα CPS έχει σχεδιαστεί ως οντότητα ή σύνολο οντοτήτων με συγκεκριμένο σκοπό ή για την επίτευξη ενός συγκεκριμένου στόχου και πρέπει να περιλαμβάνει ένα υπολογιστικό (cyber) και ένα φυσικό μέρος που συνεργάζονται για να ολοκληρώσουν μια εργασία ή λειτουργία [2]. Τα συστήματα πληροφοριών και τα συστήματα CPS χρησιμοποιούν ηλεκτρονικές, υπολογιστικές και ασύρματες συνδέσεις, όπως πληροφορίες, υπηρεσίες και κοινωνικές και εμπορικές λειτουργίες που υπάρχουν μόνο στον κυβερνοχώρο. Ο κυβερνοχώρος βασίζεται στην επικοινωνία και η επιχειρησιακή του επιτυχία εξαρτάται από τη διατήρηση των γραμμών επικοινωνίας [7].

Η λειτουργία του κυβερνοχώρου εξαρτάται από πέντε (5) βασικές συνιστώσες [8]:

- τον Χρόνο (Time),
- τον Χώρο (Space),
- την Ανωνυμία (Anonymity),
- την Ασυμμετρία (Asymmetry) και
- την Αποτελεσματικότητα (Efficiency)

Οι παράγοντες αυτοί δημιουργούν το ακρώνυμο «TSAAE», που αποτελεί μια από τις πιο θεμελιώδεις έννοιες στην κατανόηση της ασφάλειας στον κυβερνοχώρο. Λόγω της ευελιξίας που παρουσιάζει ο κυβερνοχώρος ως περιβάλλον, αυτές οι βασικές συνιστώσες του εμφανίζονται διαφορετικά στον φυσικό κόσμο [8].

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Ο χρόνος είναι ένα ζωτικό και αναντικατάστατο κομμάτι της ανθρώπινης ζωής. Η προετοιμασία και η υλοποίηση οποιασδήποτε δραστηριότητας χρειάζονται χρόνο. Στον φυσικό κόσμο, σε γενικές γραμμές, οι φυσικές απειλές δεν συμβαίνουν ακαριαία. Στον κυβερνοχώρο, όμως, μια απειλή μπορεί να εμφανιστεί σε κλάσματα δευτερολέπτου και χωρίς προειδοποίηση. Από χρονικής άποψης, το σημείο που ξεκινάει μια κυβερνο-επίθεση δεν παίζει κανένα ρόλο [8].

Ο χώρος είναι απόλυτα συνυφασμένος με το χρόνο. Στον κυβερνοχώρο, κανείς δεν μπορεί να θεωρηθεί ασφαλής από μια κυβερνο-επίθεση αλλά την ίδια στιγμή ο οποιοσδήποτε μπορεί δυνητικά να είναι ο δράστης μιας. Μια κυβερνο-επίθεση μπορεί να ξεκινήσει ακόμα και από ένα μόνο άτομο με το πάτημα ενός και μόνο πλήκτρου. Στον κυβερνοχώρο, οποιοσδήποτε προορισμός μπορεί να δεχθεί επίθεση. Ο κυβερνοχώρος, επίσης, δεν είναι οριοθετημένος και αλλάζει συνεχώς μέσω των τεχνολογικών εξελίξεων και των αλλαγών των δικτύων. Μακροπρόθεσμα, ο κυβερνοχώρος μπορεί να αλλάξει προς την επιθυμητή κατεύθυνση με διεθνείς συμβάσεις και οδηγίες. Πρόκληση στον κυβερνοχώρο αποτελεί η δυσκολία καθορισμού των επιπτώσεων μιας κυβερνο-επίθεσης και το σημείο από όπου ξεκίνησε [8].

Βασική πρόκληση όσον αφορά την ανωνυμία αποτελεί η ταυτοποίηση του κυβερνοχώρου και των λειτουργιών του. Ως ταυτοποίηση θεωρείται η αναγνώριση της ταυτότητας των φορέων και η ένδειξη της θέσης τους, στοιχεία τα οποία είναι δύσκολο να προσδιοριστούν στον κυβερνοχώρο. Το επίπεδο βεβαιότητας της ταυτοποίησης εξαρτάται από τρεις παράγοντες: το επίπεδο στόχευσής της, τη φύση των ενεργειών και τον επιδιωκόμενο στόχο της. Μερικές φορές μια κυβερνο-επίθεση έχει πολιτικά κίνητρα. Για παράδειγμα, η κυβέρνηση των Ηνωμένων Πολιτειών συμμετείχε, ανεπίσημα, στη δημιουργία και εφαρμογή του κακόβουλου λογισμικού Stuxnet που διέλυσε το πυρηνικό πρόγραμμα του Ιράν το 2011. Με την αποδοχή της συμμετοχής τους σε αυτή την κυβερνο-επίθεση, οι ΗΠΑ έδειξαν στον κόσμο ότι είχαν τόσο την δύναμη όσο και τους πόρους για χρήση προηγμένων κυβερνο-όπλων [8].

Ο όρος ασυμμετρία είναι αρκετά παλαιός, αλλά έγινε ευρύτερα γνωστός μετά τις επιθέσεις της 11ης Σεπτεμβρίου [8]. Οι ασύμμετρες επιθέσεις εκμεταλλεύονται τα αδύναμα σημεία του αντιπάλου, προσπαθώντας να τα χρησιμοποιήσουν με τον βέλτιστο τρόπο. Ο κυβερνοχώρος δημιουργεί νέες ευκαιρίες για ασύμμετρο πόλεμο. Κάθε λειτουργία που πραγματοποιείται στον κυβερνοχώρο, συμπεριλαμβανομένου του πολέμου πληροφοριών, είναι ασύμμετρη από τη φύση της, παρόλο που η κατανομή και η υλοποίηση των ίδιων των λειτουργιών είναι συμμετρικές [8]. Ασυμμετρία, επίσης, χαρακτηρίζει τις κυβερνο-απειλές, παρέχοντας περιορισμένες δυνατότητες εντοπισμού των ατόμων που πραγματοποίησαν μια κυβερνο-επίθεση και προσφέροντας τη δυνατότητα χρήσης τους από μη κρατικούς φορείς, οι οποίοι μπορεί να είναι άτομα ή οργανώσεις που έχουν σημαντική πολιτική επιρροή αλλά δεν είναι σύμμαχοι με κάποια συγκεκριμένη χώρα ή κράτος [9]. Τέλος, η ασυμμετρία επιτρέπει στους κυβερνο-επιτιθέμενους να επωφελούνται από τις αλλαγές στον κυβερνοχώρο ταχύτερα και πιο εύκολα [10].

Η αποτελεσματικότητα μιας κυβερνο-επίθεσης δεν αφορά τη διακοπή λειτουργίας του Διαδικτύου. Σκοπός μιας κυβερνο-επίθεσης είναι συνήθως η αποδυνάμωση της αξιοπιστίας της λειτουργίας των εταιριών, των οργανισμών ή των κυβερνητικών φορέων. Βασικό στοιχείο

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

της αποτελεσματικότητας στον κυβερνοχώρο αποτελεί η ικανότητα ταυτόχρονης εκτέλεσης πολλαπλών λειτουργιών και σε διαφορετικές διαστάσεις. Όσο μεγαλύτερο είναι το δίκτυο λειτουργίας που χρησιμοποιούν οι εταιρίες, οι οργανισμοί και οι κυβερνητικοί φορείς, τόσο περισσότερα δίκτυα και συστήματα πληροφοριών πρέπει να προστατεύονται [8]. Όσον αφορά την αποτελεσματικότητα, οι μη κυβερνητικοί φορείς έχουν δύο τρόπους να ασκήσουν στρατηγικές επιρροές. Πρώτον, μπορούν να εμπορευματοποιήσουν τις δικές τους λειτουργίες στον κυβερνοχώρο και να συνεργαστούν με κυβερνητικούς ή μη φορείς. Δεύτερον, μπορούν να σχηματίσουν διαφορετικές συμμαχίες, για παράδειγμα με κρατικούς φορείς που μπορούν να τους προσφέρουν λειτουργίες στον κυβερνοχώρο. Παρόλο που ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί για κακόβουλες ενέργειες, η ύπαρξή του έχει δημιουργήσει μια πλατφόρμα για νέες καινοτομίες, όπως ψηφιοποίηση, εικονικοποίηση και αυτοματοποίηση. Χάρη σε αυτές τις καινοτομίες, πλήθος εταιριών μπόρεσαν να παρέχουν στους τελικούς χρήστες μεγάλο εύρος προϊόντων και υπηρεσιών [8].

2.2 Ασφάλεια στον κυβερνοχώρο

Η ασφάλεια στον κυβερνοχώρο είναι ένας ευρέως χρησιμοποιούμενος όρος, οι ορισμοί του οποίου διαφέρουν πολύ και είναι συχνά υποκειμενικοί.

Σύμφωνα με τον J.A. Lewis, η ασφάλεια στον κυβερνοχώρο *«συνεπάγεται τη διασφάλιση των δικτύων υπολογιστών και των πληροφοριών που περιλαμβάνουν από μη εξουσιοδοτημένη πρόσβαση και από κακόβουλες ζημιές ή αλλοιώσεις»* [11].

Οι Craigen και συν. ορίζουν την ασφάλεια στον κυβερνοχώρο ως *«οργάνωση και συλλογή πόρων, διαδικασιών και δομών, με σκοπό την προστασία του κυβερνοχώρου και των συστημάτων που σχετίζονται με αυτόν, τα οποία αποπροσανατολίζουν τις νόμιμες ιδιοκτησίες από τα πραγματικά δικαιώματα ιδιοκτησίας»* [5].

Σύμφωνα με τους Boyes και συν. η ασφάλεια στον κυβερνοχώρο μπορεί να θεωρηθεί επίσης ως *«μια συλλογή εργαλείων, μεθόδων, εννοιών ασφάλειας, διασφαλίσεων ασφάλειας, κατευθυντήριων γραμμών, μεθόδων διαχείρισης κινδύνου, διεργασιών, εκπαίδευσης, ασφαλίσεων και τεχνολογιών. Αυτή η συλλογή μπορεί να χρησιμοποιηθεί για την προστασία των στοιχείων του κυβερνοχώρου, των οργανισμών και των χρηστών»* [2].

Ο D. Colesniuc έχει ορίσει την ασφάλεια στον κυβερνοχώρο ως *«μέθοδο που βοηθά να διασφαλιστεί η ασφάλεια του κυβερνοχώρου από απειλές που μπορούν να λάβουν διάφορες μορφές, όπως η κατασκοπεία ή η απόκρυψη μυστικών πληροφοριών από εταιρείες, πολυεθνικές και κρατικούς φορείς»* [9].

Ο M. Chertoff υπογράμμισε ότι υπεύθυνες για θέματα ασφάλειας στον κυβερνοχώρο δεν είναι μόνο οι κυβερνήσεις αλλά και άτομα, οργανισμοί και ιδρύματα, με βάση τον τρόπο που χρησιμοποιούν το Διαδίκτυο και τα λειτουργικά συστήματα που βασίζονται στην τεχνολογία πληροφοριών και επικοινωνιών [12].

Η ασφάλεια στον κυβερνοχώρο μπορεί να υποστηριχθεί μέσω διαφόρων μέτρων και διαδικασιών. Οι πιο συνηθισμένοι τρόποι αφορούν τον έλεγχο της διαχείρισης ασφαλείας σε σχέση με την πληρότητα των απαραίτητων κανόνων, διαδικασιών και μεθόδων και την

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

ικανότητα εντοπισμού των πιθανών τρωτών σημείων ενός συστήματος. Επιπλέον, σημαντικό στοιχείο αποτελεί η συνεχής αναζήτηση νέων τάσεων ασφαλείας βάσει των οποίων μπορεί να πραγματοποιείται μια διαρκής ανανέωση του τρόπου αντιμετώπισης των όποιων πιθανών επιθέσεων [2]. Ο γρήγορος ρυθμός των τεχνολογικών εξελίξεων δημιουργεί μια σταθερή ροή εμφάνισης νέων σοβαρών τρωτών σημείων σε λειτουργικά συστήματα, βιβλιοθήκες λογισμικού και εφαρμογές, γεγονός που συνεπάγεται την τακτική επανεξέταση κάθε στρατηγικής.

Η μεγάλη γκάμα απειλών κατά της ασφάλειας στον κυβερνοχώρο συνεπάγεται την αδυναμία ύπαρξης μιας ενιαίας προσέγγισης που να είναι σε θέση να αντιμετωπίσει όλους τους κινδύνους που προκύπτουν. Οι επιχειρηματικές αλλαγές έχουν επίσης σημαντικό αντίκτυπο στην ασφάλεια στον κυβερνοχώρο, όπως για παράδειγμα, η εισαγωγή της έννοιας «Φέρε τη Συσκευή σου» (Bring Your Own Device - BYOD) και η τάση παραχώρησης κρίσιμων στοιχείων, όπως η παροχή εφεδρικών τροφοδοσιών, για διαχείριση και έλεγχο σε τρίτα μέρη [2].

2.3 Βασικοί σκοποί της ασφάλειας στον κυβερνοχώρο

Ο εντοπισμός των επιπέδων των απειλών κατά της ασφάλειας του κυβερνοχώρου, προϋποθέτει την πλήρη κατανόηση όλων παραμέτρων που περιλαμβάνονται στην διαδικασία. Άτομα, επιχειρήσεις αλλά και κράτη αντιμετωπίζουν τις ίδιες προκλήσεις από τις απειλές στον κυβερνοχώρο και πρέπει να είναι σε θέση να αναγνωρίσουν ότι οι απειλές αυτές αυξάνονται σε συχνότητα, πολυπλοκότητα και πεδίο εφαρμογής [12]. Οι επιτιθέμενοι στον κυβερνοχώρο δεν έχουν κανένα ενδοιασμό στο να χρησιμοποιήσουν όλα τα απαραίτητα μέσα που θα τους επιτρέψουν την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα [13]. Πρόσφατο παράδειγμα αποτελεί η μαζική επίθεση με ransomware της WannaCry, η οποία ήταν παγκόσμιας κλίμακας και είχε ως στόχο τους υπολογιστές που λειτουργούν με το λειτουργικό σύστημα Windows. Η επίθεση άρχισε στις 12 Μαΐου 2017 και μόλυνε περισσότερους από 300.000 υπολογιστές σε 150 χώρες. Μεταξύ αυτών ήταν η Εθνική Υπηρεσία Υγείας της Βρετανίας, ο διεθνής αποστολέας FedEx, η τηλεπικοινωνιακή εταιρεία Telefonica στην Ισπανία και ο σιδηροδρομικός φορέας Deutsche Bahn στη Γερμανία [14].

Οι απειλές κατά της ασφάλειας στον κυβερνοχώρο εκμεταλλεύονται την αυξανόμενη πολυπλοκότητα και τη συνδεσιμότητα των υποδομών ζωτικής σημασίας, θέτοντας σε κίνδυνο την ασφάλεια, την οικονομία, τη δημόσια ασφάλεια και την υγεία ολόκληρων χωρών. Οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο μπορούν να επηρεάσουν, για παράδειγμα, έναν οργανισμό, αυξάνοντας το κόστος λειτουργίας και επηρεάζοντας τα έσοδα. Μπορούν επίσης να βλάψουν την ικανότητα ανάπτυξης ενός οργανισμού, δημιουργώντας προβλήματα στη συντήρηση και την παροχή υπηρεσιών στους χρήστες [15].

Κατά την αξιολόγηση της ασφάλειας των λειτουργιών μιας εταιρείας, μιας επιχείρησης, ενός οργανισμού ή ενός κυβερνητικού φορέα και την εύρεση της πιθανότητας ύπαρξης απειλών, κινδύνων και τρωτών σημείων, θα πρέπει να απαντηθούν τρία σημαντικά ερωτήματα που αφορούν το «τι», το «πώς» και το «από ποιόν/ ποιους ή τι» προστατεύεται. Οι απαντήσεις στα ερωτήματα αυτά, αποτελούν και τους βασικούς σκοπούς της ασφάλειας στον κυβερνοχώρο, οι οποίοι είναι [8]:

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

- Η διευκρίνηση του τι ή ποιος προστατεύεται πρωτίστως και πόσο αποτελεσματικά μπορεί να λειτουργήσει η εταιρεία, επιχείρηση, κλπ. σε περίπτωση αποτυχίας των λαμβανόμενων μέτρων ασφαλείας
- Ο εντοπισμός όλων των πιθανών απειλών μέσω της ανάλυσής τους
- Η εφαρμογή των μέτρων και των διαδικασιών για την εξασφάλιση της ασφάλειας της εταιρείας, επιχείρησης, κλπ. από τον παράγοντα που την απειλεί

Σε μια μελέτη του ομίλου CyberEdge, διαπιστώθηκε ότι οι εταιρίες, επιχειρήσεις, κλπ. θεωρούν ως μεγαλύτερες κυβερνο-απειλές τις επιθέσεις αλίευσης (phishing), κακόβουλου λογισμικού (malware), ιών (virus), σκουληκιών (worm), καθώς και τις zero-day-attacks [16]. Μια ακόμα διαπίστωση της μελέτης αφορά το γεγονός ότι οι εταιρίες, επιχειρήσεις, κλπ. δίνουν λιγότερη προσοχή στις κυβερνο-επιθέσεις ενάντια στο λογισμικό του Διαδικτύου, στις εστιασμένες επιθέσεις, στους ιούς ενάντια στις φορητές συσκευές και στα κακόβουλα προγράμματα που έχουν εγκατασταθεί στο σύστημα μετά από κάποιο download και έχουν ως στόχο την αδρανοποίηση των παρεχόμενων υπηρεσιών.

Ο Ευρωπαϊκός Οργανισμός Δικτύων και Πληροφοριών (ENISA) χαρακτήρισε ως κυβερνο-επιθέσεις τις επιθέσεις που επικεντρώνονται σε ιστοσελίδες ή εφαρμογές ιστού, κλοπές ταυτότητας, επιθέσεις που εκμεταλλεύονται διαρροές πληροφοριών και προγράμματα που καταστρέφουν ή αναστέλλουν τη λειτουργική ικανότητα των επιχειρήσεων [17]. Για παράδειγμα, η επίθεση drive-by-malware εκτελείται με την έγχυση ενός κακόβουλου κώδικα στον κώδικα HTML μιας ιστοσελίδας. Η εν λόγω επίθεση εστιάζεται στον χρήστη του ηλεκτρονικού υπολογιστή και μολύνει τον υπολογιστή, ακόμα και αν η μόνη ενέργεια του χρήστη είναι η απλή επίσκεψη σε μια ιστοσελίδα.

2.4 Επίπεδα απειλών

Ως απειλή (threat) μπορεί να θεωρηθεί μια οποιαδήποτε ενέργεια που μπορεί να δημιουργήσει κίνδυνο, βλάβη ή αβεβαιότητα στον κυβερνοχώρο. Ο καθορισμός των απειλών καθιστά ευκολότερο τον προσδιορισμό του απαιτούμενου επιπέδου ασφάλειας, την αξιολόγηση διαφορετικών απειλητικών παραγόντων και την αύξηση της κατανόησης του είδους της μεθόδου που απαιτείται για την παροχή ασφάλειας. Μια απειλή μπορεί να είναι ακόμα μια ενέργεια που δημιουργεί ζημιά, λειτουργική δυσχέρεια ή και αναστολή μιας λειτουργίας [8]. Οι απειλές προκαλούνται από κακόβουλες ενέργειες ή από τα ακούσια αποτελέσματα καλοπροαίρετων ενεργειών. Στις κακόβουλες ενέργειες μπορούν, για παράδειγμα, να περιλαμβάνονται το χακάρισμα ή η εισαγωγή κακόβουλου λογισμικού. Στις καλοπροαίρετες ενέργειες και τα ακούσια αποτελέσματα τους μπορούν να περιλαμβάνονται η συντήρηση λογισμικού ή τα δικαιώματα των χρηστών [18].

Οι κυβερνο-επιθέσεις θεωρούνται επικίνδυνες επειδή υπάρχουν τόσες πολλές παράμετροι που επηρεάζουν τα αποτελέσματα, τις συνέπειες και τη φύση τους. Για παράδειγμα, μια κυβερνο-επίθεση μπορεί να τραυματίσει ακόμα και θανάσιμα τους υπαλλήλους, να βλάψει τον εξοπλισμό ή να οδηγήσει σε εκτεταμένη οικονομική αναστάτωση [9].

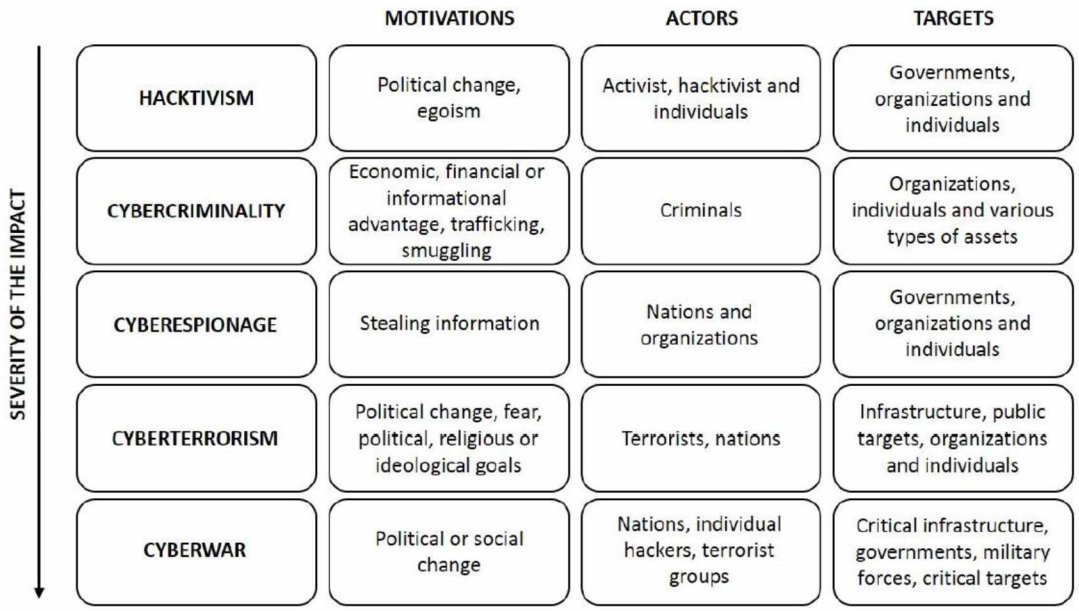
Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Η πραγματοποίηση κυβερνο-επιθέσεων δεν απαιτεί εξειδικευμένες γνώσεις ή εμπειρία. Ακόμα και ένας ελάχιστος εξοπλισμός μπορεί να δώσει τη δυνατότητα στους επιτιθέμενους να προκαλέσουν σοβαρές βλάβες τόσο στον κυβερνοχώρο αλλά και στον φυσικό κόσμο. Τα αποτελέσματα ή οι συνέπειες των κυβερνο-επιθέσεων μπορεί να είναι δύσκολο να καθοριστούν, ακριβώς επειδή η ζημιά μπορεί να είναι μεγαλύτερη από την αναμενόμενη. Ο παράγοντας της ανωνυμίας αποτελεί μια πολύ δύσκολα διαχειρίσιμη έννοια στον κυβερνοχώρο, επειδή δημιουργεί κενά και πολυπλοκότητα στη σχέση μεταξύ ατόμων και κυβερνητικών νομοθεσιών [9].

Ο J.A. Lewis εντόπισε τέσσερα στοιχεία τα οποία μπορούν να επανεκτιμήσουν μια κυβερνο-επίθεση [19]:

- Ο προσδιορισμός ενός ιστορικού πλαισίου των κυβερνο-επιθέσεων ενάντια σε υποδομές ζωτικής σημασίας
- Οι κυβερνο-επιθέσεις θα πρέπει να εξετάζονται με βάση τον αριθμό και τη σοβαρότητα των βλαβών, όπως οι διακοπές στην ηλεκτροδότηση, οι καθυστερήσεις στις μεταφορές και οι διακοπές επικοινωνίας
- Η εξέταση του βαθμού εξάρτησης των υποδομών ζωτικής σημασίας από τα δίκτυα υπολογιστών και των πλεονασμάτων που υπάρχουν σε αυτά τα συστήματα
- Σε περιπτώσεις κυβερνο-τρομοκρατίας η εξέταση της χρήσης κυβερνο-όπλων σε πολιτικούς στόχους καθώς και η πιθανότητα επίτευξης των στόχων αυτών, είναι επιτακτική

Στην εικόνα 1 παρουσιάζονται τα διαφορετικά επίπεδα απειλών κατά της ασφάλειας στον κυβερνοχώρο. Ο όρος επίπεδο, χρησιμοποιείται επειδή κάθε ένα από αυτά περιέχει διαφορετικά πολιτικά και κοινωνικά χαρακτηριστικά [2].



ΕΙΚΟΝΑ 1: Κίνητρα, δράστες και στόχοι των κυβερνο-απειλών [2]

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Στην εικόνα 1 επίσης παρουσιάζονται παραδείγματα κινήτρων, δραστών (actors) και στόχων των κυβερνο-απειλών. Μια κυβερνο-επίθεση μπορεί να αποτελεί χακτιβισμό (hacktivism), εγκληματικότητα (criminality), κατασκοπεία (espionage), τρομοκρατία (terrorism), εχθροπραξία ή πολεμική διαμάχη (warfare). Οι επιτιθέμενοι μπορούν να επιδιώξουν να αποκτήσουν πολιτικό ή κοινωνικό έλεγχο και εξουσία, να προκαλέσουν πολιτικές αλλαγές, να κλέψουν πληροφορίες ή να κερδίσουν οικονομικό πλεονέκτημα. Οι επιτιθέμενοι μπορεί να είναι μεμονωμένα άτομα, ομάδες ακτιβιστών, ανταγωνιστές, κυβερνο-εγκληματίες, τρομοκράτες, καθώς και κράτη. Οι στόχοι είναι συνήθως υποδομές ζωτικής σημασίας, διάφοροι τύποι περιουσιακών στοιχείων, έθνη, κυβερνήσεις, οργανισμοί ή άτομα [2].

Τα κίνητρα των κυβερνο-απειλών είναι πολλά και μπορούν να χωριστούν σε διάφορα επίπεδα, όπως απειλές για λόγους στρατηγικής, πολιτικοί λόγοι, οικονομικοί λόγοι, κ.α. Η λήψη αποφάσεων σχετικά με την ασφάλεια στον κυβερνοχώρο συμβάλλει στη δημιουργία καταλόγου απειλών, στον οποίο περιλαμβάνονται οι απειλές που θεωρούνται από μια εταιρεία, επιχείρηση, κτλ. ως επιβλαβείς για τις δραστηριότητές της και πρέπει να προστατεύεται από αυτές [8].

2.5 Κίνδυνοι

Ο κίνδυνος (risk) μπορεί να γίνει αντιληπτός ως ενέργεια ή πιθανότητα κάποιας απειλής ή άλλου γεγονότος που θα προκαλούσε επικίνδυνα αποτελέσματα. Άλλοι ορισμοί θεωρούν τον κίνδυνο ως μέτρο της πιθανότητας και της αυστηρότητας των δυσμενών συνεπειών. Στη δεκαετία του 1990 ο κίνδυνος ορίστηκε ως τριάδα σεναρίου, πιθανότητας και αποτελεσμάτων. Αργότερα, στον ορισμό προστέθηκε η πτυχή της ευπάθειας [21]. Ο κίνδυνος χαρακτηρίζεται από δύο βασικά στοιχεία. Το πρώτο θεωρεί τον κίνδυνο ως μελλοντικό αποτέλεσμα και μπορεί να λάβει διάφορες μορφές. Το δεύτερο είναι η πιθανότητα να προκύψει κάποιο αποτέλεσμα [22].

Οι κίνδυνοι αποτελούν μέρος κάθε λειτουργίας και συνεπώς δεν μπορούν να παρεμποδιστούν. Θεωρούνται συνήθως ως ύπαρξη των συνθηκών μιας λειτουργίας. Μπορούν επίσης να θεωρηθούν ως αρνητικές περιπτώσεις του μέλλοντος και αλλάζουν συνεχώς. Μπορούν να αποφευχθούν, να υιοθετηθούν, να οριστούν, να μετρηθούν και να μεταφερθούν. Ο εντοπισμός και έλεγχος τους απαιτεί υπεύθυνη διαχείριση. Η διαχείριση των κινδύνων συνεπάγεται ότι τα άτομα, οι οργανισμοί και οι κοινωνίες έχουν ως στόχο να προβλέψουν τις συνεχείς αλλαγές. Ο στόχος της πρόβλεψης είναι ο σαφής καθορισμός και η αξιολόγηση των κινδύνων και η ανάπτυξη διαφορετικών μεθόδων αντιμετώπισής τους. Η διαχείριση των κινδύνων συνίσταται στον προγραμματισμό, τον εντοπισμό και την ανάλυση τους, την ανάπτυξη της παρακολούθησης τους και την επανεκτίμησή τους [8].

Οι κίνδυνοι είναι αναπόφευκτοι ανεξαρτήτως διαδικασίας και λειτουργίας. Η διαχείρισή τους παρέχει ένα αποτελεσματικό πλαίσιο για τον μετριασμό τους. Επίσης, προσδιορίζει, αξιολογεί και δίνει προτεραιότητα στους κινδύνους, χρησιμοποιώντας οικονομικούς πόρους για να ελαχιστοποιήσει, να παρατηρήσει και να ελέγξει τη δυνατότητα των γεγονότων που προκαλούν ανεπανόρθωτες συνέπειες [22].

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

2.6 Τρωτά σημεία

Τα τρωτά σημεία ή ευπάθειες (vulnerabilities) θεωρούνται αδυναμίες του κυβερνοχώρου και μπορούν να χρησιμοποιηθούν από τους δράστες για την αποδυνάμωση της αξιοπιστίας μιας μεμονωμένης λειτουργίας ή ενός ολόκληρου συστήματος. Η ύπαρξη ενός τρωτού σημείου αφορά την ύπαρξη σφάλματος ή αδυναμίας στο σύστημα που επιτρέπει στον εκάστοτε εισβολέα ανεπιθύμητη πρόσβαση. Η διαχείριση των τρωτών σημείων συνίσταται από την συστηματική ταυτοποίηση, ταξινόμηση, διόρθωση και έλεγχο. Εκτός του κυβερνοχώρου, τα τρωτά σημεία αποτελούν αδυναμίες που συνδέονται με θέματα τεχνολογίας, υλικού ή τεχνογνωσίας [8].

Πάνω από το 90% των επιτιθέμενων στον κυβερνοχώρο είναι εξοικειωμένοι με τα τρωτά σημεία των στόχων τους και έχουν εύκολη πρόσβαση στις τεχνολογίες που υποτίθεται ότι υπάρχουν με σκοπό την πρόληψη των επιθέσεων [23]. Οι ευπάθειες προκύπτουν συχνά από την ανεπάρκεια σχεδιασμού, ολοκλήρωσης και συντήρησης ενός συστήματος, καθώς και από τα λάθη στον έλεγχο του κυβερνοχώρου [18]. Τέτοιες ευπάθειες αφορούν ατέλειες του λειτουργικού συστήματος των ηλεκτρονικών υπολογιστών ή σφάλματα στο λογισμικό των εκτελέσιμων προγραμμάτων ή εφαρμογών και μπορεί να είναι είτε άμεσες, όπως αδύναμοι κωδικοί πρόσβασης που οδηγούν σε μη εξουσιοδοτημένη πρόσβαση, είτε έμμεσες, όπως η απουσία διαχωρισμού δικτύου. Η ύπαρξη τρωτών σημείων έχει επιπτώσεις για την ασφάλεια και την εμπιστευτικότητα αλλά και τη διαθεσιμότητα πληροφοριών [18].

Ο J.A. Lewis διαπίστωσε ότι το μεγάλο ζήτημα των υφιστάμενων ευπαθειών των δικτύων υπολογιστών και των υποδομών ζωτικής σημασίας, προκύπτει από την ταχεία ανάπτυξη της τεχνολογίας. Επίσης, τόνισε την διαφορετικότητα που παρουσιάζουν τα τρωτά σημεία των δικτύων υπολογιστών από αυτά των υποδομών ζωτικής σημασίας, υποστηρίζοντας ότι τα δίκτυα υπολογιστών ενδέχεται να είναι πιο ευάλωτα σε επιθέσεις [19].

Ο Διεθνής Οργανισμός Ναυσιπλοΐας (International Maritime Organization – IMO) έχει επισημάνει τις ευπάθειες που μπορούν να οδηγήσουν σε κινδύνους στον κυβερνοχώρο σε ορισμένα συστήματα των πλοίων, όπως συστήματα γεφυρών, συστήματα διαχείρισης φορτίων, συστήματα ελέγχου πρόσβασης και επικοινωνίας κ.α. [18]. Για τα λιμάνια, οι πιθανές ευπάθειες περιλαμβάνουν, για παράδειγμα, περιορισμένη εκπαίδευση και ετοιμότητα του προσωπικού σχετικά με την ασφάλεια στον κυβερνοχώρο, σφάλματα λογισμικού, σύνδεση και αλληλεξάρτηση δικτύων, κ.α. [24].

Με δεδομένο ότι η ιδιωτική βιομηχανία διαθέτει και εκμεταλλεύεται πολλά κρίσιμα οικονομικά περιουσιακά στοιχεία, όπως οικονομικές υποδομές, οι εκάστοτε κυβερνήσεις τίθενται αντιμέτωπες με το πρόβλημα έλλειψης ελέγχου και μηχανισμών που να μπορούν να αντιμετωπίσουν επιθέσεις στον κυβερνοχώρο. Ένα παράδειγμα κυβερνο-επίθεσης κατά υποδομών ζωτικής σημασίας πραγματοποιήθηκε στην Εσθονία στις 26 Απριλίου 2007. Η ιδέα πίσω από την επίθεση ήταν να ασκηθεί πίεση στην κυβέρνηση της Εσθονίας να μεταφέρει ένα σοβιετικό άγαλμα του Δεύτερου Παγκόσμιου Πολέμου από το στρατιωτικό νεκροταφείο στο αρχικό του σημείο, το κέντρο του Ταλίν. Η κυβέρνηση της Εσθονίας, η αστυνομία, το τραπεζικό σύστημα, τα μέσα ενημέρωσης και η υποδομή του Διαδικτύου αποτέλεσαν φορείς που έπρεπε να αντιμετωπίσουν τις κυβερνο-επιθέσεις επί τρεις εβδομάδες. Ένας χάκερ

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

παραβίασε τον ιστότοπο του Πρωθυπουργού της Εσθονίας, εισάγοντας μια επιστολή συγγνώμης για την μετακίνηση του αγάλματος μαζί με μια υπόσχεση για την μεταφορά του στην αρχική του θέση [25].

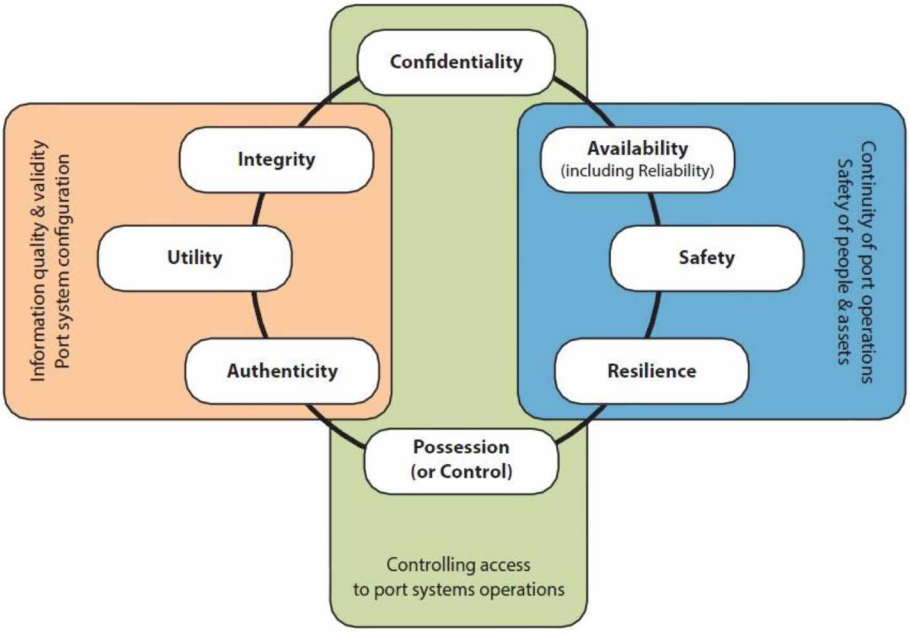
Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

3 Κυβερνο-ασφάλεια στη Ναυτιλία

3.1 Στόχοι της κυβερνο-ασφάλειας στη ναυτιλία

Το ναυτιλιακό περιβάλλον (λιμάνια και πλοία) περιλαμβάνει μια ποικιλία τεχνολογιών, υφιστάμενων και αναδυόμενων [2]. Το στοιχείο αυτό καθιστά την εκάστοτε προσέγγιση της ασφάλειας στον κυβερνοχώρο που υιοθετείται να ποικίλλει από εγκατάσταση σε εγκατάσταση ή από σύστημα σε σύστημα, ανάλογα με την πολυπλοκότητα, το ιδιοκτησιακό καθεστώς, τη χρήση και την αλυσίδα εφοδιασμού που υποστηρίζουν το σχεδιασμό και τη λειτουργία οποιασδήποτε ναυτιλιακής δραστηριότητας. Επομένως, σε ένα τόσο ποικιλόμορφο και πολυδιάστατο περιβάλλον, η ασφάλεια στον κυβερνοχώρο αντιμετωπίζεται καλύτερα λαμβάνοντας υπόψη ένα σύνολο χαρακτηριστικών ασφαλείας που να δίνουν τη δυνατότητα υιοθέτησης των κατάλληλων λύσεων με βάση τη φύση της εκάστοτε εγκατάστασης ή του εκάστοτε συστήματος και των πιθανών απειλών που καλούνται να αντιμετωπίσουν.

Με βάση τους βασικούς σκοπούς της ασφάλειας στον κυβερνοχώρο, που αναφέρθηκαν στο προηγούμενο κεφάλαιο και με βάση την πολυπλοκότητα που παρουσιάζει το ναυτιλιακό περιβάλλον, καθίσταται μάλλον εύκολος ο προσδιορισμός των στόχων που θα πρέπει να έχει η κυβερνο-ασφάλεια στον τομέα της ναυτιλίας (Εικ. 2). Για την εξέταση της επίτευξης των στόχων αυτών, πρέπει να υιοθετείται μια προσέγγιση διαχείρισης κινδύνου, η οποία θα αναδεικνύει το βαθμό υλοποίησης των εκάστοτε λαμβανόμενων μέτρων προστασίας ή πρόληψης καθώς και το βαθμό στον οποίο οι τυχόν υπολειπόμενοι κίνδυνοι είναι αποδεκτοί [27].



ΕΙΚΟΝΑ 2: Στόχοι της κυβερνο-ασφάλειας στον τομέα της ναυτιλίας [2]

Οι στόχοι της κυβερνο-αφάλειας στον τομέα της ναυτιλίας είναι οι εξής [2]:

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

- ***Εμπιστευτικότητα (Confidentiality):*** Αφορά τον έλεγχο πρόσβασης και την πρόληψη μη εξουσιοδοτημένης πρόσβασης στα ευαίσθητα δεδομένα των πλοίων ή των λιμανιών. Τα συστήματα των πλοίων ή των λιμανιών καθώς και οι σχετικές διεργασίες τους, θα πρέπει να σχεδιάζονται, να εφαρμόζονται, να λειτουργούν και να διατηρούνται, έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα (οικονομικά, εμπορικά ή προσωπικά). Για παράδειγμα, όλα τα προσωπικά δεδομένα θα πρέπει να διαχειρίζονται σύμφωνα με τον νόμο περί προστασίας δεδομένων, ενώ μπορεί να απαιτείται η λήψη πρόσθετων μέτρων για την προστασία της ιδιωτικότητας του προσωπικού λόγω της συγκέντρωσης δεδομένων, πληροφοριών ή μεταδεδομένων

- ***Κατοχή ή/και έλεγχος (Possession and/or control):*** Αφορούν το σχεδιασμό, την υλοποίηση, τη λειτουργία και τη συντήρηση των συστημάτων των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους, ώστε να αποφευχθεί μη εξουσιοδοτημένος έλεγχος, χειρισμός ή παρεμβολή. Τα συστήματα των πλοίων ή των λιμανιών καθώς και οι σχετικές διεργασίες τους, θα πρέπει να σχεδιάζονται, να εφαρμόζονται, να λειτουργούν και να συντηρούνται έτσι ώστε να αποφεύγεται ο μη εξουσιοδοτημένος έλεγχος, ο χειρισμός ή η παρεμβολή. Παράδειγμα θα μπορούσε να αποτελέσει η απώλεια μιας κρυπτοσυσκευής αποθήκευσης. Ένα τέτοιο γεγονός δεν δημιουργεί καμία απώλεια εμπιστευτικότητας, καθώς οι πληροφορίες είναι απρόσιτες χωρίς το κλειδί κρυπτογράφησης

- ***Ακεραιότητα (Integrity):*** Αφορά τη διατήρηση της συνέπειας, της συνοχής και της διαμόρφωσης πληροφοριών και συστημάτων και την πρόληψη μη εξουσιοδοτημένων αλλαγών σε αυτά. Τα συστήματα των πλοίων ή των λιμανιών καθώς και οι σχετικές διεργασίες τους, θα πρέπει να σχεδιάζονται, να εφαρμόζονται, να λειτουργούν και να συντηρούνται έτσι ώστε να αποφεύγεται η μη εξουσιοδοτημένη αλλαγή των στοιχείων, των διαδικασιών και της κατάστασης του συστήματος ή ακόμα και η διαμόρφωση του ίδιου του συστήματος. Απώλεια της ακεραιότητας του συστήματος θα μπορούσε να συμβεί μέσω φυσικών αλλαγών σε ένα σύστημα, όπως η μη εξουσιοδοτημένη σύνδεση ενός σημείου πρόσβασης Wi-Fi σε ασφαλές δίκτυο ή μέσω ενός σφάλματος, όπως η αλλοίωση μιας βάσης δεδομένων ή ενός αρχείου, που δημιουργείται από ιό στα μέσα αποθήκευσης

- ***Αυθεντικότητα (Authenticity):*** Αφορά τη διασφάλιση γνησιότητας, μη αλλοίωσης και τροποποίησης των δεδομένων εισόδου και εξόδου των συστημάτων των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους. Θα πρέπει επίσης να είναι δυνατή η επαλήθευση της αυθεντικότητας των στοιχείων, του λογισμικού και των δεδομένων εντός των συστημάτων αυτών αλλά και οποιωνδήποτε άλλων σχετικών διαδικασιών. Τα ζητήματα αυθεντικότητας θα μπορούσαν να αφορούν δεδομένα, όπως πλαστά πιστοποιητικά ασφάλειας, ή hardware υλικά, όπως κλωνοποιημένες συσκευές

- ***Διαθεσιμότητα – Αξιοπιστία (Availability - reliability):*** Αφορά τη διασφάλιση ότι οι πληροφορίες των συστημάτων των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους είναι σταθερά προσβάσιμες και χρησιμοποιήσιμες ανά πάσα στιγμή. Για να επιτευχθεί η απαιτούμενη διαθεσιμότητα των πληροφοριών αυτών πολλές

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

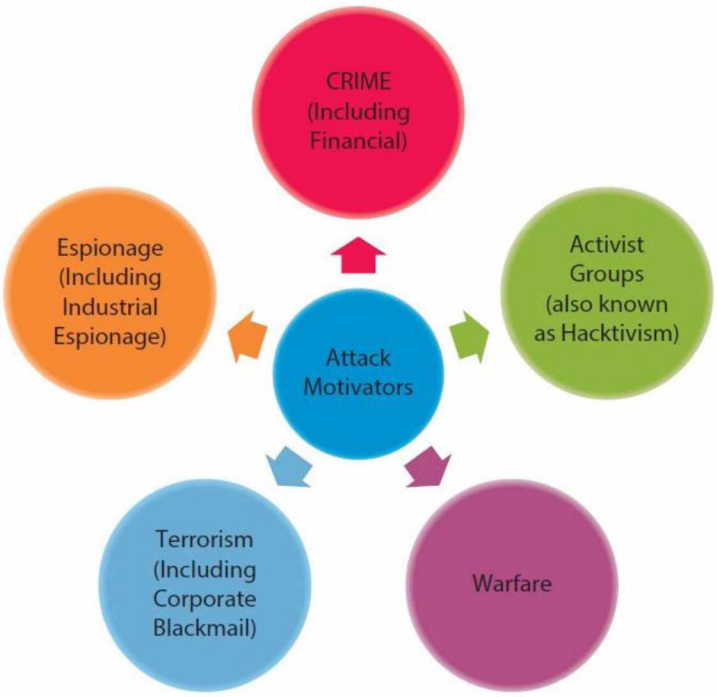
φορές απαιτείται η ύπαρξη ενός κατάλληλου και ανάλογου επιπέδου ανθεκτικότητας (resilience). Απώλεια της διαθεσιμότητας μπορεί να συμβεί μέσω της βλάβης ενός στοιχείου του συστήματος, όπως το κρασάρισμα ενός σκληρού δίσκου ή μέσω μιας κακόβουλης πράξης όπως μια επίθεση άρνησης υπηρεσίας (Denial of Service attack – DoS) που αποτρέπει τη χρήση ενός συστήματος διασυνδεδεμένου στο Διαδίκτυο

- ***Χρησιμότητα (Utility):*** Αφορά τη διασφάλιση ότι οι πληροφορίες και τα συστήματα παραμένουν χρηστικά και χρήσιμα καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα συστήματα των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους πρέπει να σχεδιάζονται, να εφαρμόζονται, να λειτουργούν και να διατηρούνται έτσι ώστε η χρήση τους να διατηρείται σε επιθυμητά επίπεδα καθ' όλη τη διάρκεια του κύκλου ζωής τους. Ένα παράδειγμα απώλειας χρησιμότητας θα ήταν μια κατάσταση όπου ένα σύστημα έχει αλλάξει ή αναβαθμιστεί και το αρχείο δεδομένων του ιστορικού δεν είναι πλέον κατανοητό από το νέο σύστημα. Στην περίπτωση αυτή δεν υπάρχει απώλεια διαθεσιμότητας αλλά τα δεδομένα είναι άχρηστα
- ***Ασφάλεια (Safety):*** Ο σχεδιασμός, η υλοποίηση, η λειτουργία και η συντήρηση των συστημάτων των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους θα πρέπει να πραγματοποιούνται με τέτοιο τρόπο ώστε να αποφευχθεί η δημιουργία επιβλαβών καταστάσεων που μπορεί να οδηγήσει σε τραυματισμό ή απώλεια ζωής ή ακούσια σωματική ή περιβαλλοντική βλάβη. Ένα ζήτημα ασφάλειας μπορεί να προκύψει από κακόβουλο λογισμικό που προκαλεί την αποτυχία προβολής των καταστάσεων συναγερμού των συστημάτων. Για παράδειγμα, η αποτυχία ορθής λειτουργίας ενός ανιχνευτή εγγύτητας ή άλλων αισθητήρων θα μπορούσε να προκαλέσει ζημιά σε μέρος της εγκατάστασης ή ακόμα και απώλεια ζωής
- ***Ανθεκτικότητα (Resilience):*** Αφορά την ικανότητα των πληροφοριών και των συστημάτων να μετασχηματίζονται, να ανανεώνονται και να ανακτώνται έγκαιρα ως απάντηση σε ανεπιθύμητες ενέργειες. Ο σχεδιασμός, η υλοποίηση, η λειτουργία και η συντήρηση των συστημάτων των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους θα πρέπει να είναι τέτοια ώστε να αποφεύγονται οι διαδοχικές αποτυχίες (cascading failures). Σε περίπτωση που σε ένα σύστημα ή μια σχετική διαδικασία υφίσταται διακοπή ή αναστολή λειτουργίας, η αποκατάσταση της λειτουργίας θα πρέπει να πραγματοποιείται σε εύλογο χρονικό διάστημα

3.2 Κίνητρα κυβερνο-επιθέσεων

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, τα κίνητρα εξαπόλυσης κάποιας επίθεσης στον κυβερνοχώρο είναι αρκετά.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29



ΕΙΚΟΝΑ 3: Κίνητρα πραγματοποίησης κυβερνο-επιθέσεων στον τομέα της ναυτιλίας [2]

Όσον αφορά τον τομέα της ναυτιλίας, μια επίθεση στον κυβερνοχώρο μπορεί να πραγματοποιηθεί για έναν από τους ακόλουθους πέντε σκοπούς (Εικ.3) [2], [26]:

- ***Κατασκοπεία (Espionage):*** επιδιώκοντας μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες (πνευματική ιδιοκτησία, εμπορικές πληροφορίες, εταιρικές στρατηγικές, προσωπικά δεδομένα) και διαταραχές για κρατικούς ή εμπορικούς σκοπούς
- ***Χακτιβισμός (Hactivism):*** αναζητώντας τη δημοσιότητα ή τη δημιουργία πιέσεων για λογαριασμό συγκεκριμένου στόχου ή αιτίας, για παράδειγμα, για την αποτροπή χειρισμού συγκεκριμένων φορτίων ή τη διακοπή της κατασκευής μιας νέας λιμενικής εγκατάστασης. Ο στόχος μπορεί να είναι ο ίδιος ο λιμένας, ο χειριστής μιας λιμενικής εγκατάστασης ή ένας τρίτος όπως ο προμηθευτής ή ο αποδέκτης κάποιου φορτίου
- ***Εγκληματικότητα (Criminality):*** οδηγείται κυρίως από οικονομικό όφελος και μπορεί να περιλαμβάνει ζημιές, κλοπή του φορτίου, λαθρεμπόριο αγαθών και ανθρώπων, αποφυγή φόρων ή ειδικών φόρων κατανάλωσης
- ***Τρομοκρατία (Terrorism):*** χρήση του λιμένα ή των πλοίων για την ενθάρρυνση του φόβου και την πρόκληση σωματικών βλαβών ή οικονομικών επιπτώσεων
- ***Εχθροπραξία ή πολεμική διαμάχη (Warfare):*** σύγκρουση μεταξύ κρατών, όπου ο στόχος είναι η διακοπή των συστημάτων μεταφορών ή της λειτουργίας των υποδομών με σκοπό την αδυναμία επιχειρησιακής χρήσης ή την απενεργοποίηση συγκεκριμένων λιμενικών εγκαταστάσεων

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

3.3 Δράστες κυβερνο-επιθέσεων

Οι δράστες των κυβερνο-απειλών, όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, μπορούν να ταξινομηθούν σε μία από τις εξής επτά κατηγορίες [2]: μεμονωμένα άτομα, ομάδες ακτιβιστών, ανταγωνιστές, κυβερνο-εγκληματίες, τρομοκράτες καθώς και κράτη.

Οποιαδήποτε από αυτές τις κατηγορίες δραστών είναι εξίσου σημαντική και η δράση της σχετίζεται με τα στοιχεία των συστημάτων που είναι εγκατεστημένα στα λιμάνια ή εντός των πλοίων, με πληροφορίες και δεδομένα των συστημάτων αυτών που είναι αποθηκευμένα σε εξωτερικούς διακομιστές, με υπηρεσίες που παρέχονται από τρίτα μέρη και με την ναυτιλιακή εφοδιαστική αλυσίδα.

Κατά τη διερεύνηση όλων των πιθανών κυβερνο-απειλών σε ένα σύστημα του ναυτιλιακού τομέα θα πρέπει να λαμβάνεται υπόψη ότι μπορεί να υπάρξει κάποια σύγκλιση μεταξύ των σκοπών και των στόχων όλων των παραπάνω μεμονωμένων κατηγοριών. Για παράδειγμα, μερικά από τα κακόβουλα προγράμματα που αναπτύχθηκαν από ομάδες εγκληματιών στον κυβερνοχώρο περιλαμβάνουν εξελιγμένες λειτουργίες εντολών και ελέγχου, επιτρέποντας την απενεργοποίηση των μηχανισμών ασφαλείας του συστήματος και την εγκατάσταση νέων ενημερώσεων σε διαφορετικά μέρη του, με σκοπό τη διαρκή έκθεση του συστήματος σε νέες επιθέσεις. Με τον τρόπο αυτό, ένα σύστημα ή μια συσκευή που κάποια στιγμή στο παρελθόν είχε παραβιαστεί για την πραγματοποίηση κυβερνο-επίθεσης οικονομικής φύσης, θα μπορούσε κάλλιστα να χρησιμοποιηθεί στο μέλλον για πρόσβαση σε ευαίσθητα δεδομένα ή ως κερκόπορτα (backdoor), μέσω της οποίας θα μπορούν να εξαπολύονται επιθέσεις σε λιμενικές εγκαταστάσεις και συστήματα [2].

3.3.1 Μεμονωμένα άτομα

Η σοβαρότητα και η πολυπλοκότητα της απειλής καθορίζεται από τις ικανότητες και τις δυνατότητες του ατόμου. Πιο συγκεκριμένα [2]:

- η αμέλεια ή η άγνοια ενός υπαλλήλου που δεν τηρεί τις πολιτικές ασφάλειας ή από παράληψη, μπορεί να εκθέσει τα συστήματα των πλοίων ή των λιμανιών καθώς και των συναφών διεργασιών τους σε κίνδυνο
- «φιλικά» άτομα που δεν επιδιώκουν να βλάψουν συστήματα ή δεδομένα, αλλά μπορούν να αποκτήσουν πρόσβαση στα συστήματα χωρίς άδεια, μπορούν να προκαλέσουν τυχαίες βλάβες. Τα κίνητρα αυτών των ατόμων γενικά προέρχονται από την επιθυμία τους να διερευνήσουν τις αδυναμίες και τα τρωτά σημεία των συστημάτων
- υπάλληλοι με περιορισμένες γνώσεις σε θέματα πληροφορικής μπορούν να μπουν στη διαδικασία απόκρυψης ή διαρροής ευαίσθητων πληροφοριών, υπονόμευσης ή η διατάραξης των λειτουργιών του λιμανιού, κλπ. Το ποσό της βλάβης που μπορεί να προκληθεί σε αυτήν την περίπτωση εξαρτάται από τα δικαιώματα πρόσβασης που έχουν τα άτομα αυτά στο σύστημα και την αποτελεσματικότητα των μέτρων που έχουν ληφθεί για την ασφάλεια στον κυβερνοχώρο σχετικά με τα ναυτιλιακά συστήματα και δεδομένα

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

- υπάλληλοι με σημαντικές γνώσεις σε θέματα πληροφορικής ή διαχειριστές του συστήματος μπορούν να προκαλέσουν σοβαρές βλάβες, ιδιαίτερα αν έχουν πρόσβαση στα συστήματα με δικαιώματα διαχειριστή. Η επάρκεια των γνώσεών τους ή οι ικανότητές τους, μπορεί να τους δώσουν τη δυνατότητα παράκαμψης των ελέγχων και των μέτρων προστασίας, ενώ παράλληλα μπορεί να έχουν τη γνώση αφαίρεσης των αποδεικτικών στοιχείων σχετικά με τις δραστηριότητές τους, για παράδειγμα, διαγράφοντας ή τροποποιώντας τις καταχωρήσεις στα αρχεία καταγραφής του συστήματος
- μεμονωμένοι χάκερ με περιορισμένες γνώσεις που χρησιμοποιούν τεχνικές και εργαλεία που σχεδιάζονται και αναπτύσσονται από άλλους. Η ευκολία με την οποία εργαλεία χακαρίσματος ή άρνησης εξυπηρέτησης μπορούν να βρεθούν στο Διαδίκτυο σημαίνει ότι το απαιτούμενο επίπεδο τεχνικής κατάρτισης για την εξαπόλυση μιας επίθεσης έχει μειωθεί σημαντικά
- χάκερ με πολλές γνώσεις και ικανότητα να αναπτύσσουν ή να αναβαθμίζουν δικά τους εργαλεία μπορεί να μην έχουν οικονομικά ή ιδεολογικά κίνητρα για να εξαπολύσουν μια επίθεση, όμως χακάρουν το σύστημα ή αναπτύσσουν κακόβουλο λογισμικό επειδή μπορούν και θέλουν να δείξουν τι μπορούν να κάνουν. Μπορούν, για παράδειγμα, να παραβιάζουν έναν ιστότοπο ή να εισέλθουν σε ένα διακομιστή με σκοπό την υποκλοπή των διαπιστευτηρίων χρήστη, τα οποία στη συνέχεια δημοσιεύουν σε έναν δημόσιο ιστότοπο απλά και μόνο για να αποδείξουν τις ικανότητές τους
- άτομα με πολύ προχωρημένες τεχνικές γνώσεις μπορούν να είναι ικανά να αποκρύψουν στοιχεία που να αποδεικνύουν τις δραστηριότητές τους, για παράδειγμα, διαγράφοντας ή τροποποιώντας τις καταχωρήσεις στα αρχεία καταγραφής του συστήματος. Μπορούν επίσης να έχουν επαρκείς γνώσεις και ικανότητες παράκαμψης των μέτρων ελέγχου και προστασίας

3.3.2 Ομάδες ακτιβιστών

Οι ομάδες αυτές περιλαμβάνουν άτομα με ιδεολογικά κίνητρα και μπορεί να αποτελούν δυναμικές ομάδες ή υποομάδες. Οι ενέργειές τους αφορούν διαδικτυακές διαμαρτυρίες, οι οποίες ενδέχεται να έχουν ως στόχο τη διακοπή συστημάτων ή την απόκτηση εμπιστευτικών ή ευαίσθητων πληροφοριών για δημοσίευση ή διάδοση, ώστε να αμβλύνουν τους στόχους τους. Η δράση τους μπορεί να πάρει διαστάσεις χιονοστιβάδας όταν, όπως έχει αποδειχθεί, προσλαμβάνουν ή πείθουν αφελείς τρίτους να συμμετάσχουν σε αυτή επιτρέποντας την εγκατάσταση κακόβουλου λογισμικού στους υπολογιστές τους, δημιουργώντας έτσι botnets και μεγιστοποιώντας την επίδραση οποιασδήποτε επίθεσης κατανεμημένης άρνησης εξυπηρέτησης (DDoS) [2].

3.3.3 Ανταγωνιστές

Αυτή η ομάδα αποτελείται συνήθως από μεγάλες εταιρείες που επιδιώκουν να δημιουργήσουν πλεονεκτήματα έναντι των αντιπάλων τους [2]. Μπορούν να ενεργούν άμεσα ή μέσω τρίτων με σκοπό να βλάψουν έναν αντίπαλο συλλέγοντας επιχειρηματικές πληροφορίες, κλέβοντας πνευματική ιδιοκτησία, συγκεντρώνοντας πληροφορίες που αφορούν

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

τις επιχειρηματικές δραστηριότητες των ανταγωνιστών τους (π.χ. προσφορές) ή ακόμα και δημιουργώντας βλάβες στα λειτουργικά συστήματα των αντίπαλων επιχειρήσεων με σκοπό τη διακοπή των εργασιών, την πρόκληση οικονομικών απωλειών ή δημιουργώντας κακή φήμη στους ανταγωνιστές τους. Ανάλογα με το μέγεθος, τον τομέα, τη γεωγραφική θέση και την πολυπλοκότητα των διεργασιών κυβερνοχώρου που μπορεί να έχει μια ναυτιλιακή εταιρεία, οι ανταγωνιστές μπορεί να είναι σε θέση να εκτελούν εξελιγμένα κακόβουλα λογισμικά που να τους επιτρέπουν τη στόχευση αλλά και τη διείσδυση στα συστήματα των ανταγωνιστών τους.

3.3.4 Κυβερνο-εγκληματίες

Πρόκειται για εξελιγμένες εγκληματικές ομάδες που διαπράττουν ένα ευρύ φάσμα παράνομων εγκληματικών πράξεων στον κυβερνοχώρο. Κίνητρό τους αποτελεί το όφελος από παράνομες δραστηριότητες και επομένως εστιάζονται σε απάτες, σε κλοπές από λογαριασμούς και σε κλοπές πνευματικής ιδιοκτησίας. Ωστόσο, οι δραστηριότητες αυτής της ομάδας μπορούν να περιλαμβάνουν επίσης εκβιασμούς μέσω της χρήσης κακόβουλου λογισμικού για την κρυπτογράφηση δεδομένων ή απειλές για επιθέσεις DDoS σε εταιρικούς ιστότοπους. Όσον αφορά τα λιμάνια, οι εγκληματίες στον κυβερνοχώρο μπορεί να επιδιώξουν την παρακολούθηση ή την απόκτηση πρόσβασης σε πληροφορίες σχετικά με αποστολές φορτίου ή σε ρυθμίσεις ασφαλείας ως πρόδρομος εγκληματικών δραστηριοτήτων ή φυσικών επιθέσεων σε λιμενικές εγκαταστάσεις.

Η πολυπλοκότητα του κακόβουλου λογισμικού που χρησιμοποιείται από αυτές τις ομάδες αυξάνεται καθώς η αγορά της εγκληματικότητας στον κυβερνοχώρο ανθίζει, μια αγορά όπου οι υπεύθυνοι ανάπτυξης, οι πάροχοι και οι φορείς εκμετάλλευσης δημιουργούν, προμηθεύουν και λειτουργούν εξελιγμένα εργαλεία κακόβουλης λειτουργίας και εγκλήματος στον κυβερνοχώρο σε εμπορική βάση, καθιστώντας τα εργαλεία τους διαθέσιμα σε τρίτους.

3.3.5 Τρομοκράτες

Οι τρομοκράτες γίνονται όλο και περισσότερο γνώστες της τεχνολογίας της πληροφορικής και ήδη χρησιμοποιούν ευρέως το Διαδίκτυο για προπαγανδιστικούς και επικοινωνιακούς σκοπούς. Καλά χρηματοδοτούμενες ομάδες θα μπορούσαν να επωφεληθούν από την υπηρεσία που προσφέρουν οι εγκληματίες στον κυβερνοχώρο, να επιδιώξουν την υποστήριξη από κάποιο κράτος ή να ενθαρρύνουν υπάλληλους εταιριών να υιοθετήσουν τρομοκρατικές μεθόδους επίθεσης. Με την ευρεία χρήση ηλεκτρονικών συστημάτων και εφαρμογών στον κυβερνοχώρο στον τομέα της ναυτιλίας, οι τρομοκρατικές ομάδες μπορούν να βασιστούν στα διάφορα εργαλεία που υπάρχουν στο Διαδίκτυο και να τα χρησιμοποιήσουν για να διαταράξουν τη λειτουργία ή να καταστρέψουν τις λιμενικές εγκαταστάσεις θύρες ή να επιτεθούν στα συστήματα πλοίων και λιμανιών. Οι τρομοκράτες είναι επίσης σε θέση να εκμεταλλευτούν τρωτά σημεία που διαπιστώνουν στα συστήματα αυτά, τα οποία τους δίνουν τη δυνατότητα απομακρυσμένης αναγνώρισης των στόχων τους, μειώνοντας έτσι τον χρόνο που θα χρειάζονταν για να τους παρακολουθήσουν από μέσα ή από κοντά.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

3.3.6 Κράτη

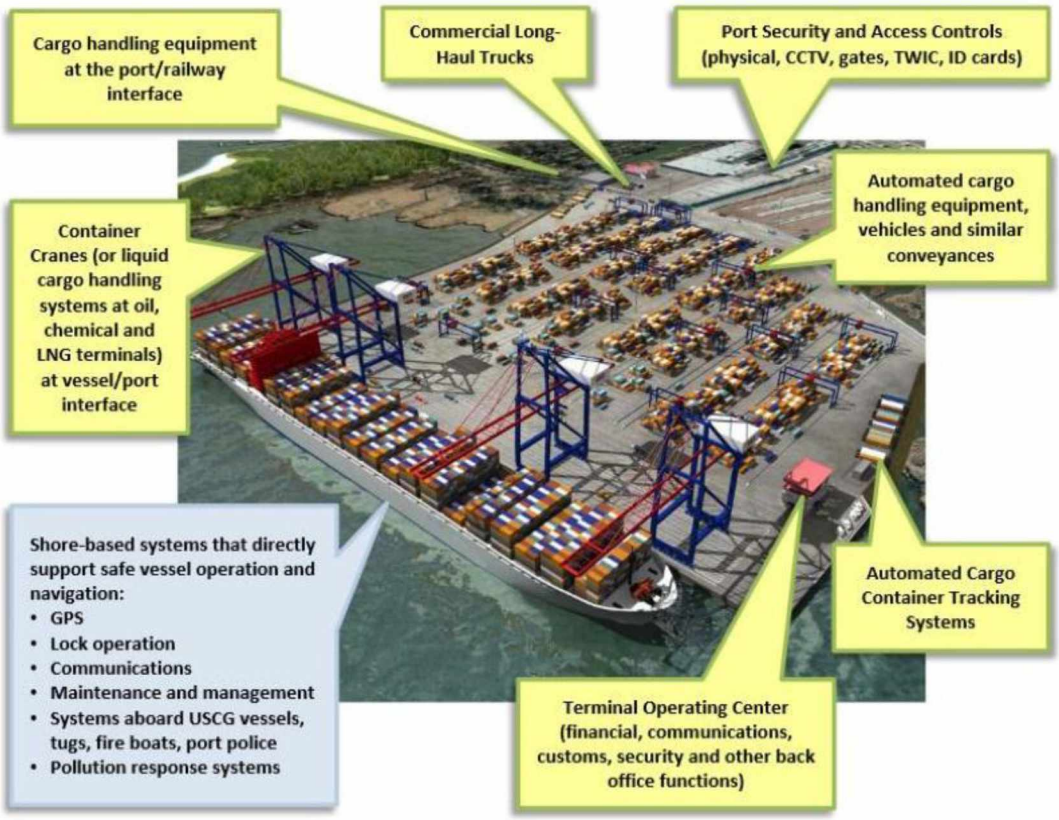
Ορισμένα κράτη συμμετέχουν ενεργά σε επιθέσεις στον κυβερνοχώρο για να αποκτήσουν κρατικά μυστικά ή ευαίσθητες πληροφορίες άλλων κρατών. Μπορούν επίσης να εξαπολύσουν κυβερνο-επιθέσεις που θα τους επιτρέψουν την δημιουργία βλαβών ή ακόμα και διακοπή της λειτουργίας υποδομών ζωτικής σημασίας, όπως είναι οι λιμενικές υποδομές. Κατά τη διάρκεια περιόδων αυξημένης διεθνούς έντασης και συγκρούσεων, αυτές οι δραστηριότητες μπορεί να περιλαμβάνουν πιο εκτεταμένες επιθέσεις, με τη χρήση κακόβουλων λογισμικών, όπως τα Stuxnet, Duqu και Flame [2].

3.4 Λιμάνια και ασφάλεια στον κυβερνοχώρο

Με την πάροδο των ετών, τα λιμάνια έχουν γίνει όλο και περισσότερο αντικείμενο ερευνών σε εθνικό αλλά και παγκόσμιο επίπεδο, με σκοπό τον καλύτερο έλεγχο και την πρόληψη πιθανών απειλών. Το κυριότερο κοινό συμφέρον ασφάλειας των λιμανιών σε παγκόσμιο επίπεδο είναι η παροχή ασφαλούς διέλευσης και αγκυροβόλησης. Την τελευταία δεκαετία, η προσοχή επικεντρώθηκε σε ανασφάλειες που σχετίζονται με μηχανισμούς μεταφορών, όπως τα εμπορευματοκιβώτια. Είναι γνωστό ότι τα εμπορευματοκιβώτια είναι εξαιρετικός τρόπος μεταφοράς παράνομων ναρκωτικών και μεταναστών και ότι συχνά δεν ελέγχονται για παρατυπίες [26]. Για το λόγο αυτό, η ανάγκη ανάπτυξης κατάλληλων μέτρων για την ασφάλεια του κυβερνοχώρου στο χώρο των λιμανιών είναι επιτακτική. Τα μέτρα αυτά θα πρέπει να είναι ανάλογα των τρωτών σημείων που υπάρχουν στα λιμάνια και σχετίζονται άμεσα ή έμμεσα με (Εικ. 4) [24]:

- κτιριακές και άλλες υποδομές
- εγκαταστάσεις και μηχανήματα
- συστήματα πληροφοριών και επικοινωνιών

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29



ΕΙΚΟΝΑ 4: Τυπικά συστήματα λιμανιών [24]

3.4.1 Κτιριακές και άλλες υποδομές

Οι λιμενικές εγκαταστάσεις περιλαμβάνουν μια ποικιλία κτιρίων, που απαιτούν ασφάλεια, έλεγχο πρόσβασης και διαφορετικά επίπεδα τεχνικής υποδομής. Τα κτίρια που μπορεί να βρεθούν σε ένα λιμάνι περιλαμβάνουν [2]:

- ναυτιλιακά κέντρα ελέγχου που φιλοξενούν τα συστήματα, τους τερματικούς σταθμούς και τις οθόνες που απαιτούνται για τη διαχείριση της θαλάσσιας κυκλοφορίας των πλοίων τόσο εντός των λιμανιών όσο και των θαλάσσιων τομέων πλησίον αυτών
- κέντρα δεδομένων
- υπόστεγα συντήρησης και συνεργεία
- αποθήκες και άλλα σημεία αποθήκευσης, ορισμένα από τα οποία ενδέχεται να απαιτούν συγκεκριμένο περιβαλλοντικό έλεγχο, για παράδειγμα ψυγεία
- διοικητικά κτίρια για το προσωπικό και για όλες τις υπηρεσίες που λειτουργούν εντός του λιμανιού

Στις λιμενικές εγκαταστάσεις απαντώνται και άλλα είδη υποδομών για τις οποίες απαιτούνται συστήματα ελέγχου και παρακολούθησης καθώς και έλεγχο πρόσβασης. Αυτού του είδους οι υποδομές περιλαμβάνουν: οδικές αρτηρίες, σιδηροδρομικά συστήματα, συστήματα διακίνησης φορτίου, όπως αγωγοί και συστήματα μεταφορέων, κ.α.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Σε όλες σχεδόν αυτές τις κτιριακές και άλλου είδους υποδομές υπάρχουν συστήματα διαχείρισης που βασίζονται σε τεχνολογίες πληροφορικής και τηλεπικοινωνιών, ενσύρματης ή ασύρματης δικτύωσης, τα οποία συνδέονται άμεσα ή έμμεσα με το Διαδίκτυο.

3.4.2 Εγκαταστάσεις και μηχανήματα

Στους χώρους των λιμανιών χρησιμοποιείται ένα ευρύ φάσμα εγκαταστάσεων και μηχανημάτων για τη διαχείριση του λιμένα και των συστημάτων μεταφορών (εμπορευμάτων και επιβατών), όπως [2]:

- πύλες για τον έλεγχο της πρόσβασης των οχημάτων και των πεζών σε περιοχές εντός του λιμανιού
- γερανοί και μεταφορικά συστήματα που χρησιμοποιούνται για τη διακίνηση φορτίων
- οχήματα ή μη σταθεροί γερανοί που μεταφέρουν εμπορευματοκιβώτια και άλλα είδη φορτίου

Κοινό χαρακτηριστικό όλων αυτών των μονάδων και μηχανημάτων είναι η χρήση βιομηχανικών συστημάτων ελέγχου και συστημάτων εποπτικού ελέγχου και συλλογής πληροφοριών (Supervisory Control And Data Acquisition - SCADA). Μερικά από αυτά τα συστήματα μπορεί να λειτουργούν ως μονάδες standalone, αλλά με την πάροδο των ετών όλο και περισσότερο συνδέονται με το επιχειρηματικό δίκτυο του λιμένα [24].

3.4.3 Συστήματα πληροφοριών και επικοινωνιών

Τα συστήματα πληροφοριών και επικοινωνιών που χρησιμοποιούνται στους χώρους των λιμανιών διαχειρίζονται ένα ευρύ φάσμα δεδομένων, όπως πληροφορίες που χρησιμοποιούνται για την υποστήριξη των λήψεων αποφάσεων και δεδομένα που χρησιμοποιούνται για τον έλεγχο των φορτίων και των εμπορευματοκιβωτίων. Η ευαισθησία των μεμονωμένων συστημάτων εξαρτάται από το αν δημιουργούν, επεξεργάζονται, αποθηκεύουν ή παρέχουν πρόσβαση σε ευαίσθητα στοιχεία ασφαλείας ή άλλες ευαίσθητες πληροφορίες [2].

Όσον αφορά τα συστήματα διαχείρισης φορτίου, η τεχνολογία της πληροφορίας αποτελεί ουσιαστικό μέρος της ταχείας και ακριβούς μεταφοράς και επεξεργασίας σημαντικών όγκων δεδομένων που σχετίζονται με τις αποστολές, τον εκτελωνισμό, τα δρομολόγια των πλοίων και τις πληροφορίες που διαχειρίζονται από το πλήρωμα. Όλα αυτά τα δεδομένα επεξεργάζονται από διεθνείς επιχειρήσεις μεταφορών και λιμενικούς οργανισμούς. Η επεξεργασία αυτή ισχύει τόσο για τη διαχείριση της μεταφοράς εμπορευματοκιβωτίων ή άλλων ειδών φορτίων όπως, οχήματα, φορτία σε παλέτες κλπ., αλλά και τη διαχείριση της θαλάσσιας κυκλοφορίας των πλοίων, οχηματαγωγών πλοίων, ταχύπλοων σκαφών, κλπ.

Οι ναυτιλιακές δραστηριότητες απαιτούν σημαντικά επίπεδα σχεδιασμού και συντονισμού, όπως [28]:

- τον προγραμματισμό της άφιξης από ξηρά και συλλογής των εμπορευματοκιβωτίων στο λιμάνι, δραστηριότητες που απαιτούν πληροφορίες για τα φορτία, όπως δεδομένα σχετικά με το όχημα παράδοσης, τον οδηγό, τον αριθμό του εκάστοτε

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

εμπορευματοκιβωτίου, το μέγεθος του εμπορευματοκιβωτίου και τον εκτιμώμενο χρόνο άφιξης

- τον σχεδιασμό και οργάνωση των θέσεων των εμπορευματοκιβωτίων στην περιοχή στοίβαξης και την επιτήρησή τους
- τον προγραμματισμό της φόρτωσης των εμπορευματοκιβωτίων στα πλοία με σκοπό την τοποθέτησή τους σε αυτά με τρόπο που θα ελαχιστοποιεί τον χρόνο εκφόρτωσης στο λιμάνι προορισμού
- την παροχή πληροφοριών στις τελωνειακές αρχές ώστε να καταστεί δυνατή η πληρωμή οποιωνδήποτε δασμών και η παροχή εκτελωνισμού

Η διαχείριση των δραστηριοτήτων αυτών γίνεται μέσω χρήσης ενός συστήματος το οποίο αρκετές φορές συνδυάζεται με ένα σύστημα διαχείρισης λιμένος ή ένα σύστημα διαχείρισης της κυκλοφορίας των εμπορευματοκιβωτίων. Μαζί μπορούν να περιλαμβάνουν [24]:

- τερματικά πληροφοριών σε πραγματικό χρόνο στις πύλες εισόδου του λιμανιού και στους σταθμούς φόρτωσης και εκφόρτωσης των εμπορευματοκιβωτίων
- αυτόματη αναγνώριση πινακίδας κυκλοφορίας (Automatic Number Plate Recognition - ANPR) για φορτηγά που εισέρχονται και εξέρχονται από τους σταθμούς φόρτωσης και εκφόρτωσης των εμπορευματοκιβωτίων που περιλαμβάνει κάμερες CCTV και σύστημα ανάλυσης βίντεο
- αυτόματη ανάγνωση του αριθμού των εμπορευματοκιβωτίων και οπτική επιθεώρηση για τυχόν ζημιές τόσο κατά την άφιξη όσο και κατά την αναχώρηση από τον λιμένα
- λεπτομερή παρακολούθηση της θέσης των εμπορευματοκιβωτίων όταν τοποθετούνται ή μετακινούνται στις αποβάθρες στους χώρους αποθήκευσης
- παροχή οδηγιών μετακίνησης και φόρτωσης στα συστήματα χειρισμού (για παράδειγμα, φορητοί γερανοί, γερανογέφυρες, μεταφορείς περιτυλίγματος, κ.λπ.)
- αρχεία σχετικά με την παραλαβή του εκτελωνισμού προκειμένου να εγκριθεί η απελευθέρωση της αποβάθρας από εισαγόμενα εμπορευματοκιβώτια

Τα μέσα επικοινωνίας που χρησιμοποιούνται για την ανταλλαγή των απαραίτητων δεδομένων περιλαμβάνουν τη χρήση πομποδεκτών VHF/FM, ηλεκτρονικού ταχυδρομείου, ηλεκτρονική ανταλλαγή δεδομένων και δικτυακές πύλες. Το επίπεδο της πολυπλοκότητας αυτών των ανταλλαγών ποικίλλει σημαντικά ανάλογα με το βαθμό αυτοματοποίησης διαχείρισης των φορτίων και των ικανοτήτων των συστημάτων πληροφορικής που χρησιμοποιεί η εκάστοτε ναυτιλιακή κοινότητα. Τα συστήματα επικοινωνιών που σχετίζονται με τα συστήματα ελέγχου μπορούν να χρησιμοποιούν μια ποικιλία τεχνολογιών επικοινωνιών, όπως δίκτυα IP, ασύρματων και ενσύρματων μέσων με τα αντίστοιχα και πρωτόκολλα. Ανεξάρτητα των μέσων επικοινωνίας, η ακεραιότητα της βάσης δεδομένων και των σχετικών συναλλαγών είναι κρίσιμη για την ομαλή λειτουργία του τερματικού σταθμού εμπορευματοκιβωτίων.

Παρόμοιες λειτουργίες και συστήματα απαιτούνται για τον χειρισμό φορτίων που δεν βρίσκονται εντός εμπορευματοκιβωτίων, όπως για παράδειγμα, οχήματα, φορτία σε παλέτες

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

κλπ. Τα φορτία αυτών των ειδών διαχειρίζονται εντός συγκεκριμένων λιμενικών εγκαταστάσεων, με συστήματα προσαρμοσμένα στη διαχείριση, την κυκλοφορία, το χειρισμό και αποθήκευση ή ταξινόμηση του φορτίου και περιλαμβάνουν:

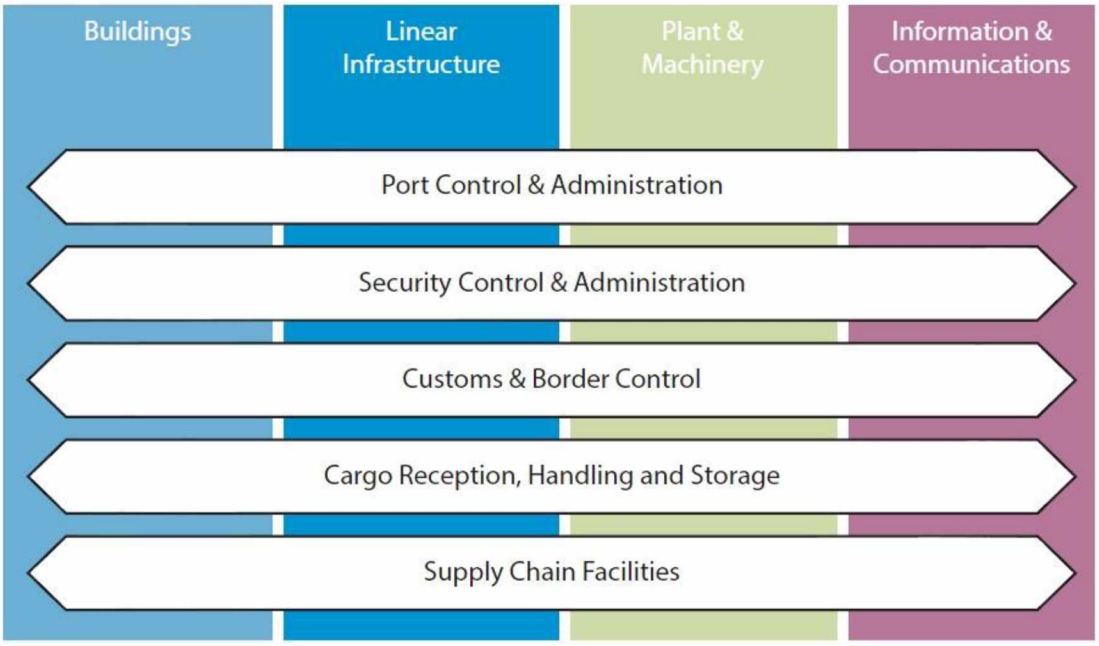
- έλεγχο ασφάλειας στον κυβερνοχώρο των συστημάτων του λιμένα τα οποία μπορούν να χρησιμοποιηθούν για παροχή ελέγχου πρόσβασης του προσωπικού ή των επισκεπτών, για έλεγχο ασφάλειας του λιμένα ή / και την περίμετρο των λιμενικών εγκαταστάσεων, για τον έλεγχο πρόσβασης οχημάτων και πεζών και για την αποτροπή κλοπής αγαθών ή / και ζημιών στις λιμενικές εγκαταστάσεις
- έλεγχο και διοίκηση των λιμενικών εγκαταστάσεων, δηλαδή την καθημερινή διαχείριση των λειτουργιών του λιμένα, όπως ο προγραμματισμός φόρτωσης και εκφόρτωσης φορτίων, μετακίνηση και αποθήκευση φορτίων, κινήσεις οχημάτων και επιβατών εντός του χώρου του λιμένα και ενδεχομένως διαχείριση της κίνησης των πλοίων κατά την προσέγγισή τους προς το λιμάνι
- τελωνειακό ή / και συνοριακό έλεγχο
- έλεγχο εγκαταστάσεων εφοδιαστικής αλυσίδας, ο οποίος, σε ορισμένες περιπτώσεις, μπορεί να λειτουργεί ανεξάρτητα από τις υποδομές πληροφοριών και επικοινωνιών του λιμένα, με πολύ περιορισμένη πρόσβαση στις πληροφορίες που αφορούν τις κινήσεις των πλοίων, ενώ σε άλλες περιπτώσεις μπορεί να είναι ενσωματωμένος στα συστήματα λειτουργίας του λιμένα ή των λιμενικών εγκαταστάσεων
- παραλαβή, αποθήκευση και διακίνηση φορτίου, αν και η ακριβής φύση αυτών των συστημάτων ποικίλλει ανάλογα με τη φύση του φορτίου που διαχειρίζονται

3.4.4 Σημασία της κυβερνο-ασφάλειας για τα λιμάνια

Η αδυναμία λειτουργίας ή η παραβίαση ενός ή περισσοτέρων από τα στοιχεία λειτουργίας ενός λιμανιού, που αναφέρθηκαν στις προηγούμενες υποενότητες, είναι σε θέση να έχει αρνητικές συνέπειες [2]:

- στην ταχύτητα και στην αποτελεσματικότητα λειτουργίας του λιμανιού
- στην πραγματοποίηση με ασφάλεια όλων των ναυτιλιακών διαδικασιών που αφορούν ένα λιμάνι
- στην ασφάλεια του προσωπικού του λιμανιού αλλά και ατόμων που επηρεάζονται άμεσα από τις εργασιακές δραστηριότητες στους χώρους του

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29



ΕΙΚΟΝΑ 5: Στοιχεία του λιμανιού που επηρεάζονται από την ασφάλεια στον κυβερνοχώρο [2]

Επιπλέον, η αποτυχία των λιμενικών φορέων να εκτιμήσουν ορθά τη δομή και τη λειτουργία των στοιχείων του λιμανιού, των συστημάτων που περιλαμβάνει και των παντός φύσης συναφών δραστηριοτήτων μπορεί να οδηγήσει σε έναν αριθμό ανεπιθύμητων καταστάσεων, όπως [2]:

- ακούσια έκθεση των ευαίσθητων συστημάτων, εφαρμογών ή δεδομένων σε μη εξουσιοδοτημένους χρήστες
- απώλεια ανθεκτικότητας ή αδυναμία λειτουργίας των συστημάτων
- ανεπανόρθωτες βλάβες που μπορούν να οδηγήσουν σε αλλεπάλληλη ή καταστροφική αστοχία κρίσιμων συστημάτων ή διαδικασιών

Οποιαδήποτε από τις ανεπιθύμητες αυτές καταστάσεις μπορεί επίσης να έχει σημαντικές οικονομικές απώλειες, διαταραχές στη λειτουργία του λιμένα, δυσφήμιση της λειτουργικότητας του λιμένα, περιβαλλοντικές συνέπειες, αλλά και τη δημιουργία νομικών ζητημάτων [4].

3.5 Πλοία και ασφάλεια στον κυβερνοχώρο

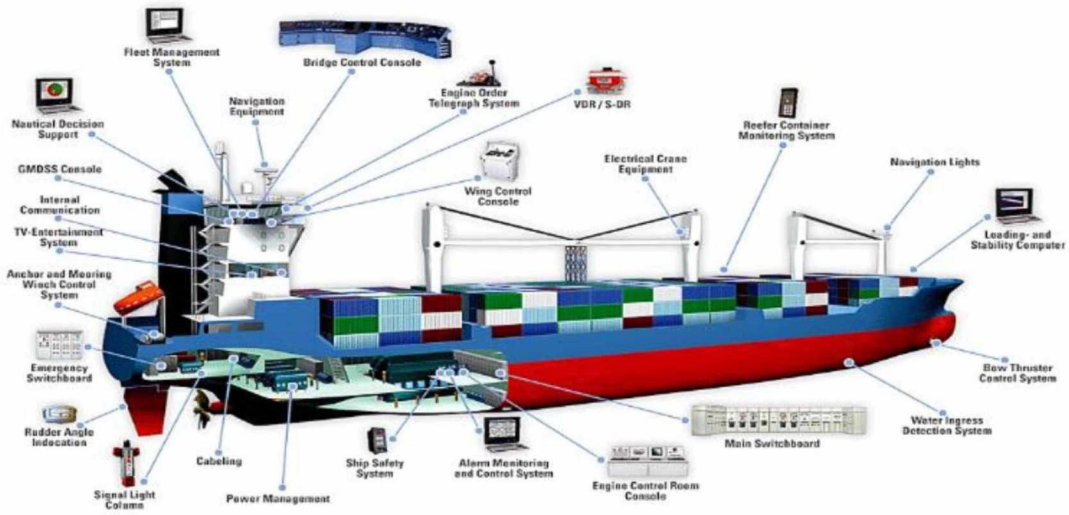
Η πολυπλοκότητα των συστημάτων των πλοίων αφορά γενικά το μέγεθος και τη λειτουργία. Ένα πλοίο απαιτεί συστήματα παροχής και ελέγχου πρόωσης, πλοήγησης, έρματος, κ.λπ. Η προσθήκη του πληρώματος και των επιβατών αυξάνει τον αριθμό των συστημάτων επί των πλοίων αλλά δημιουργεί και επιπλέον πολυπλοκότητα σε αυτά, καθώς στο σύστημα διαχείρισης του πλοίου προστίθεται και το σύστημα διαχείρισης του ανθρώπινου δυναμικού.

Το πλοίο, από την ίδια του τη φύση, στην περίοδο ταξιδίου πρέπει να λειτουργεί ανεξάρτητα από την ξηρά και η μόνη σύνδεση με αυτή γίνεται μέσω ενός από τα πολλά εν δυνάμει κανάλια επικοινωνίας φωνής και δεδομένων. Ως εκ τούτου, το πλοία, όσον αφορά τον

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

κυβερνοχώρο, μπορεί να θεωρηθεί ως «σύστημα συστημάτων» που λειτουργεί σε ένα περιορισμένο περιβάλλον.

Η μεγάλη γκάμα ειδών και η διαφορετικότητα σχεδιασμού των πλοίων αλλά και ο μεγάλος αριθμός των κατασκευαστών συστημάτων για πλοία, δημιουργεί ακόμα μεγαλύτερη πολυπλοκότητα κατά την ανάπτυξη ενός μοντέλου κυβερνοχώρου που να είναι αντιπροσωπευτικό και ικανό να χρησιμοποιηθεί για όλες τις κατηγορίες πλοίων.



ΕΙΚΟΝΑ 6: Τυπικά συστήματα επί του πλοίου [24]

Για την ανάπτυξη κατάλληλων μέτρων για την ασφάλεια στον κυβερνοχώρο που αφορά τα πλοία, θα πρέπει να ληφθούν υπόψη κάθε ένα από τα υπάρχοντα τεχνικά συστήματα που βρίσκονται σε αυτά. Για την καλύτερη διαχείριση των μέτρων αυτών, τα συστήματα των πλοίων μπορούν να ταξινομηθούν στις εξής κατηγορίες [24]:

- Συστήματα επικοινωνιών που εξυπηρετούν τις εσωτερικές επικοινωνίες του πλοίου, τις επικοινωνίες μεταξύ πλοίων και τις επικοινωνίες πλοίου - ξηράς. Τα συστήματα αυτά μπορεί να περιλαμβάνουν συστήματα απομακρυσμένης παρακολούθησης όπως καταγραφείς δεδομένων ταξιδίου και συστήματα που παρακολουθούν την απόδοση συστημάτων επί του πλοίου
- Συστήματα πλοήγησης που υποστηρίζουν την πλοήγηση των πλοίων
- Συστήματα εγκαταστάσεων που χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο οποιουδήποτε μηχανήματος και εγκατάστασης που συνδέονται με τη γενική λειτουργία του σκάφους και δεν καλύπτονται από άλλες κατηγορίες
- Συστήματα ασφαλείας που χρησιμοποιούνται για τη διατήρηση της ακεραιότητας και της ασφάλειας του πλοίου και του φορτίου του
- Συστήματα φορτίου που χρησιμοποιούνται για την άμεση παρακολούθηση και διαχείριση του φορτίου
- Συστήματα διαχείρισης επιβατών που χρησιμοποιούνται για την παροχή υπηρεσιών στους επιβάτες αλλά και τη διατήρηση της υγείας επιβατών και πληρώματος

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

- Συστήματα πρόσβασης επιβατών και πληρώματος που αφορούν την παροχή αλληλεπίδρασης επιβατών – πληρώματος και δεν σχετίζονται με τη λειτουργία του πλοίου ή τη διαχείριση επιβατών και πληρώματος

Η ομαδοποίηση των κατηγοριών αυτών βασίζεται σε μια σειρά από υποθέσεις, όπως η λειτουργικότητα του συστήματος, η σχέση του με άλλα συστήματα της ίδιας κατηγορίας, η αλληλεπίδραση του χειριστή/διαχειριστή και η χρησιμοποιούμενη τεχνολογία.

Ο σχεδιασμός και κατασκευή των πλοίων βασίζεται στο αρθρωτό μοτίβο, γεγονός που έχει ως αποτέλεσμα μια κοινή υποδομή καλωδίων μεταφοράς που απαιτείται για τη διασύνδεση των αισθητήρων και του εξοπλισμού με τις λειτουργίες και την ικανότητα παρακολούθησης και ελέγχου, καθώς και την παροχή και διανομή ενέργειας. Αυτή η υποδομή περιλαμβάνει επίσης πίνακες διακλαδώσεων που βρίσκονται σε πολλά σημεία του πλοίου και χρησιμοποιούνται για την επιδιόρθωση και τη διαχείριση της καλωδιακής υποδομής και επομένως την υποστήριξη πολλών από τα συστήματα των πλοίων. Μια τέτοια υποδομή δημιουργεί ένα περιβάλλον στο οποίο το οποιοδήποτε σφάλμα ή βλάβη ενός συστήματος μπορεί να συμβεί είτε από αμέλεια είτε από κακόβουλη πράξη. Η ελαχιστοποίηση οποιασδήποτε μορφής κινδύνου μπορεί να πραγματοποιηθεί μόνο μέσα από την καλή επίγνωση, τον έλεγχο πρόσβασης και τη σωστή διαχείριση των συστημάτων.

Η επιθυμία για μείωση του πληρώματος των πλοίων είχε ως αποτέλεσμα την ανάπτυξη συστημάτων που να περιέχουν κάποια μορφή ανίχνευσης για την παρακολούθηση των λειτουργικών παραμέτρων τους και κεντρικούς πίνακες εντολών και ελέγχου που να παρέχουν όχι μόνο μια συγκεντρωτική επίγνωση της κατάστασης, αλλά και κεντρικές θέσεις από όπου τα συστήματα μπορούν να λειτουργούν. Αυτές οι κεντρικές θέσεις εντολών και ελέγχου μπορεί να έχουν κεντρικές μονάδες (master) και τηλεχειρισμούς (slave) για τον έλεγχο και τη λειτουργία των συστημάτων από τη γέφυρα ή από άλλα σημεία ελέγχου που βρίσκονται στο πλοίο.

Όλα τα συστήματα που βρίσκονται στα πλοία παρουσιάζουν μια αλληλεξάρτηση είτε για λειτουργικούς λόγους, είτε για πρόσβαση σε επικοινωνίες είτε επειδή χρησιμοποιούν μια κοινή υποκείμενη υποδομή όπως το Industrial Ethernet ή το MODBUS. Η αλληλεξάρτηση αυτή περιλαμβάνει όλους τους διάφορους τύπους αισθητήρων που χρησιμοποιούνται άμεσα από τα συστήματα για την παροχή πληροφοριών σχετικά με την κατάσταση λειτουργίας τους. Η αναγνώριση και κατανόηση αυτής της αλληλεξάρτησης και των απαιτήσεων ανταλλαγής δεδομένων ή πληροφοριών, μπορεί να οδηγήσει στην ανάπτυξη μιας αρχιτεκτονικής συστημάτων που να παρέχει τη βέλτιστη ασφάλεια χωρίς την ανάγκη προσθήκης κάποιας πρόσθετης τεχνολογίας. Μια τέτοια αρχιτεκτονική θα μπορούσε να διασφαλίσει την ύπαρξη διαχωρισμού μεταξύ των συστημάτων και την αδυναμία πρόσβασης από οποιονδήποτε εξωγενή παράγοντα.

Ο εντοπισμός και κατηγοριοποίηση των συστημάτων του πλοίου και η εύρεση της μεταξύ τους αλληλεξάρτησης δίνει επίσης τη δυνατότητα προσδιορισμού των απαιτήσεων και του σκοπού πρόσβασης. Η πρόσβαση αυτή, λόγω των ιδιαιτεροτήτων των συστημάτων των πλοίων, θα πρέπει να αφορά τα πλέον ευαίσθητα συστήματα για την εφαρμογή συγκεκριμένων ελέγχων. Η συνεχόμενη αυτοματοποίηση των πλοίων και η πολυπλοκότητα

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

των συστημάτων τους, οδηγεί στην ανάγκη παρακολούθησης της πρόσβασης σε όλα τα συστήματα προκειμένου να διεξαχθούν τυχόν έρευνες σε περίπτωση συμβάντος.

3.5.1 Συστήματα επικοινωνιών

Τα συστήματα επικοινωνιών των πλοίων (εσωτερικών, μεταξύ πλοίων και πλοίων – ξηράς) χρησιμοποιούνται για να ικανοποιήσουν διάφορες απαιτήσεις των ναυτιλιακών εταιριών, του πληρώματος ή των επιβατών. Μερικά από τα πιο συνηθισμένα συστήματα είναι:

- ***Δορυφορικές επικοινωνίες:*** Διάφορες εφαρμογές χρησιμοποιούν δορυφορικές επικοινωνίες για την επικοινωνία μεταξύ πλοίων ή μεταξύ πλοίου και ξηράς υποστηρίζοντας συστήματα φωνής και δεδομένων
- ***Συστήματα επικοινωνίας VHF/UHF:*** Τα συστήματα επικοινωνίας που χρησιμοποιούν αυτές τις ζώνες συχνοτήτων (156 – 162,025Mhz) λειτουργούν μέσω οπτικής επαφής ή διάδοσης και υποστηρίζουν την επικοινωνία μεταξύ πλοίων και πλοίων – ξηράς, με διαφορετική κατανομή καναλιών ανάλογα με τη θέση του πλοίου στον παγκόσμιο χάρτη. Το κανάλι VHF 70, για παράδειγμα, χρησιμοποιείται για ψηφιακή επιλεκτική κλήση (Digital Selective Calling - DSC), ένα σύστημα τηλεειδοποίησης που μεταδίδει και λαμβάνει κλήσεις δεδομένων για σκοπούς προειδοποίησης
- ***Συστήματα S-Band:*** Αφορούν συστήματα που χρησιμοποιούν τις ζώνες συχνοτήτων 2,4Ghz και 5Ghz και συχνά χρησιμοποιούνται για εφαρμογές Wi-Fi και Bluetooth
- ***Συστήματα PABX/GSM 3G, 4G & 5G:*** Αυτά τα συστήματα παρέχονται τοπικά ή μέσω απομακρυσμένης σύνδεσης εάν το πλοίο πλέει κοντά στην ξηρά, όπως τα οχηματαγωγά. Ο σταθμός βάσης PABX ή GSM μπορεί να είναι εγκατεστημένος σε κρουαζιερόπλοια για να παρέχει στους επιβάτες τη δυνατότητα χρήσης των κινητών τηλεφώνων τους, συνδεόμενος μέσω του συστήματος SatCom του πλοίου στην υποδομή ξηράς. Ένα οχηματαγωγό μπορεί επίσης να χρησιμοποιήσει δίκτυο 4G για την παροχή ψηφιακής διαδικτυακής επικοινωνίας στους επιβάτες

Ως εκ τούτου, ο σχεδιασμός μέτρων ασφάλειας στον κυβερνοχώρο που αφορά τα είδη επικοινωνιών των πλοίων που αναφέρθηκαν απαιτεί τη γνώση όλων αυτών των συστημάτων αλλά και των συστημάτων με τα οποία μπορούν να συνδεθούν και βρίσκονται στην ξηρά.

3.5.2 Συστήματα πλοήγησης

Όλα τα πλοία διαθέτουν συστήματα πλοήγησης και πρόωσης. Η σημαντική τεχνολογική πρόοδος σε αυτούς τους τομείς παρέχει στο πλήρωμα μια πιο ολοκληρωμένη εικόνα για το τι συμβαίνει μέσα και έξω από το πλοίο, συχνά σε πραγματικό χρόνο [4]. Τα συστήματα και βοηθήματα πλοήγησης των πλοίων σε πολλές περιπτώσεις διασυνδέονται με άλλα συστήματα επί του πλοίου. Τέτοια συστήματα είναι [28]:

- ***Καταγραφέας δεδομένων ταξιδιού (Voyager Data Recorder - VDR):*** Είναι ένα σύστημα καταγραφής δεδομένων σχεδιασμένο για όλα τα πλοία με βάση τις απαιτήσεις της διεθνούς σύμβασης SOLAS του Διεθνή Οργανισμού Ναυσιπλοΐας IMO

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

(IMO Res.A.861 (20)) για τη συλλογή δεδομένων από διάφορους αισθητήρες επί του πλοίου. Τα δεδομένα που καταγράφονται στο VDR ενδέχεται να περιλαμβάνουν ορισμένες ή όλες τις πληροφορίες (1) θέσης, ημερομηνίας και ώρας με χρήση του GPS, (2) ταχύτητας του πλοίου, (3) γυροσκοπικής πυξίδας, (4) ραντάρ, όπως εμφανίζονται από αυτό ή από δεδομένα του συστήματος AIS, (5) ECDIS, γραφημάτων πλοήγησης επί της οθόνης με συχνότητα ανανέωσης κάθε 15 δευτερόλεπτα ή όταν συμβαίνει μια αλλαγή χάρτη, (6) ηχητικών εντολών πλοήγησης από τη γέφυρα ή από την κόντρα-γέφυρα, (7) ραδιοεπικοινωνιών VHF, (8) βάθος βυθού μέσω του συστήματος echo sounder, (9) βασικών συναγερμών με βάση τη σύμβαση του IMO, (10) κατάστασης των θυρών κύτους όπως υποδεικνύεται στη γέφυρα, (11) κατάσταση στεγανών και πυρασφαλείας όπως υποδεικνύεται στη γέφυρα, (12) επιτάχυνσης κύτους, (13) εντολών και απόκρισης πηδαλίου, (14) εντολών και απόκρισης συστήματος μηχανής – έλικα, (15) κατάστασης, κατεύθυνσης, ποσότητας ώσης % ή RPM των προωθητών, και (16) ταχύτητας και κατεύθυνσης ανέμου με χρήση ψηφιακού ανεμόμετρου και πτερυγίου καιρού

- ***Το ηλεκτρονικό σύστημα απεικόνισης και πλοήγησης (ECDIS):*** Αυτό το σύστημα μπορεί να διασυνδεθεί με άλλα συστήματα όπως το σύστημα διεύθυνσης, πρόωσης, αυτόματου πιλότου, GPS και την γυροπυξίδα του πλοίου δημιουργώντας ένα κεντρικό σύστημα ελέγχου όλων των υπολοίπων
- ***Άλλα συστήματα πλοήγησης*** όπως Echo Sounder, AIS, LRIT, GNSS, NavTex, ραντάρ, αυτόματα βοηθήματα παρακολούθησης καθώς και τα φώτα πλοήγησης. Όλα αυτά τα συστήματα παρέχουν δυνατότητα απεικόνισης στη γέφυρα του πλοίου για μεγαλύτερο έλεγχο

3.5.3 Συστήματα εγκαταστάσεων

Τα συστήματα εγκαταστάσεων αποτελούν τη μεγαλύτερη κατηγορία και περιλαμβάνουν τα συστήματα που παραδοσιακά καλύπτονται από το μηχανοστάσιο, όπως τα συστήματα πρόωσης, πλοήγησης, παραγωγής και διανομής ενέργειας, εξαερισμού, νερού (πόσιμο και χρήσης), κλπ. Ιδιαίτερα τα κρουαζιερόπλοια περιλαμβάνουν ακόμα ισοδύναμα συστήματα διαχείρισης κτιρίων για τον έλεγχο του φωτισμού, της θέρμανσης, του εξαερισμού και του κλιματισμού (HVAC) κ.λπ.

Τα συστήματα εγκαταστάσεων των πλοίων είναι ισοδύναμα των παραδοσιακών συστημάτων βιομηχανικού ελέγχου (Industrial Control Systems - ICS) και λειτουργούν ως ανεξάρτητα. Με την προσθήκη πολλών αισθητήρων που χρησιμοποιούν ένα εύρος διαφορετικών πρωτοκόλλων σηματοδότησης, το παραδοσιακό σύστημα SCADA σπάνια απαντάται στα σύγχρονα πλοία. Το πιο σύνηθες είναι η χρήση ενός μείγματος πρωτοκόλλων ελέγχου, όπως το MODBUS, με συστήματα που αρχίζουν να χρησιμοποιούν το πρωτόκολλο Industrial Ethernet για την παροχή σύνδεσης και λειτουργικών εντολών και ελέγχων.

Τα δεδομένα των αισθητήρων μπορούν επίσης να χρησιμοποιηθούν ως δεδομένα σε περισσότερα από ένα συστήματα, που λειτουργούν ως αυτόνομα ή ως μέρη ενός μεγαλύτερου κεντρικού συστήματος, γεγονός που αναδεικνύει τη μεγάλη κρισιμότητα των αισθητήρων στη συνολική λειτουργία του πλοίου. Ένα σύστημα μπορεί επίσης να χρησιμοποιεί τα δεδομένα

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

των αισθητήρων και να τα ενσωματώνει ή/και να τα συγκεντρώνει με κάποιο τρόπο σε πολλαπλά σημεία δεδομένων, διαμορφώνοντας με τον τρόπο αυτό μια πλήρη εικόνα σχετικά με την κατάσταση λειτουργίας του συστήματος.

3.5.4 Συστήματα ασφαλείας

Ορισμένα συστήματα αυτής της κατηγορίας είναι υποχρεωτικά με βάση τις απαιτήσεις της σύμβασης SOLAS, ωστόσο αυτή η κατηγορία περιλαμβάνει οποιοδήποτε σύστημα που μπορεί να έχει αντίκτυπο στην ασφάλεια του πλοίου, του φορτίου, των επιβατών και του πληρώματος. Στα συστήματα ασφαλείας περιλαμβάνονται τα GMDSS (Global Maritime Distress & Safety System), AMVER (Automated Mutual-assistance Vessel Rescue), SSAS (Ship Security Alert System), NavTex, ραντάρ, σόναρ, γενικά συστήματα συναγερμού, VDR, TeleMed, πυρασφάλειας κ.λπ.

Τα συστήματα ασφαλείας συχνά συνδέονται με τα συστήματα παρακολούθησης εγκαταστάσεων των πλοίων για ενεργοποίηση όταν εντοπίζονται ορισμένες συνθήκες βλάβης. Στην περίπτωση αυτή, τα συστήματα ασφαλείας μπορεί να είναι σε θέση να υπερισχύουν των λειτουργικών συστημάτων, προκειμένου να περιοριστεί ο κίνδυνος για συγκεκριμένη περιοχή ή να τερματιστεί ένα σύστημα προκειμένου να σταματήσουν περαιτέρω ζημιές.

Πολλά από τα συστήματα ασφαλείας συνδέονται με τα συστήματα επικοινωνίας των πλοίων για την ειδοποίηση άλλων πλοίων ή υπηρεσιών που βρίσκονται στην ξηρά.

3.5.5 Συστήματα διαχείρισης φορτίου

Ο τύπος των συστημάτων διαχείρισης φορτίου που χρησιμοποιούνται εξαρτάται από τα είδη του φορτίου και την κατηγορία των πλοίων. Τα δεξαμενόπλοια πετρελαίου ή υγραερίου, για παράδειγμα, χρησιμοποιούν διαφορετικά συστήματα διαχείρισης φορτίου από εκείνα για μεταφορά εμπορευματοκιβωτίων. Αυτά τα συστήματα διαχείρισης φορτίου δεν χρησιμοποιούνται μόνο στις περιπτώσεις φόρτωσης ή εκφόρτωσης αλλά, για ορισμένα φορτία, παρέχουν επίσης μια συνεχή λειτουργία παρακολούθησης κατά τη διάρκεια της μεταφοράς τους [28].

Στα επιβατικά πλοία, τα συστήματα διαχείρισης φορτίου μπορεί επίσης να περιλαμβάνουν ισοδύναμα των συστημάτων χειρισμού αποσκευών που χρησιμοποιούνται στα αεροδρόμια, ενώ στα οχηματαγωγά, περιλαμβάνουν συστήματα παρακολούθησης οχημάτων πιθανώς συνδεδεμένα με τα συστήματα αυτόματης αναγνώρισης πινακίδων (ANPR) της ξηράς.

3.5.6 Συστήματα διαχείρισης επιβατών

Ο αριθμός και η πολυπλοκότητα των συστημάτων διαχείρισης επιβατών εξαρτάται από τον αριθμό και τη διάρκεια παραμονής των επιβατών στο πλοίο. Χρησιμοποιούνται για παροχή υπηρεσιών στους επιβάτες αλλά και για θέματα υγείας επιβατών και πληρώματος.

Το σύστημα TeleMed περιλαμβάνεται σε αυτή την κατηγορία αλλά και στην κατηγορία συστημάτων ασφαλείας καθώς είναι πιθανόν σε ορισμένα πλοία να χρησιμοποιηθεί ως σύστημα παροχής γενικής ιατρικής, πρώτων βοηθειών και τήρησης ιατρικών αρχείων

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

επιβατών και πληρώματος. Ένα τέτοιο σύστημα απαιτεί προσεκτική εξέταση όσον αφορά τον έλεγχο πρόσβασης.

Άλλα συστήματα διαχείρισης επιβατών μπορεί να περιλαμβάνουν συστήματα σημείων πώλησης (PoS) για καταστήματα και εστιατόρια, κεντρικά συστήματα κρατήσεων για θέατρα και άλλους χώρους, κατανομή και διάθεση κουκετών και διαχείριση άλλων χρηματοπιστωτικών συναλλαγών.

Τα συστήματα διαχείρισης επιβατών δεν μπορούν να προσπελαστούν από τους επιβάτες αλλά μόνο από μέλη του πληρώματος τα οποία είναι υπεύθυνα για τη χρήση τους εξ ονόματος των επιβατών.

3.5.7 Συστήματα πρόσβασης επιβατών

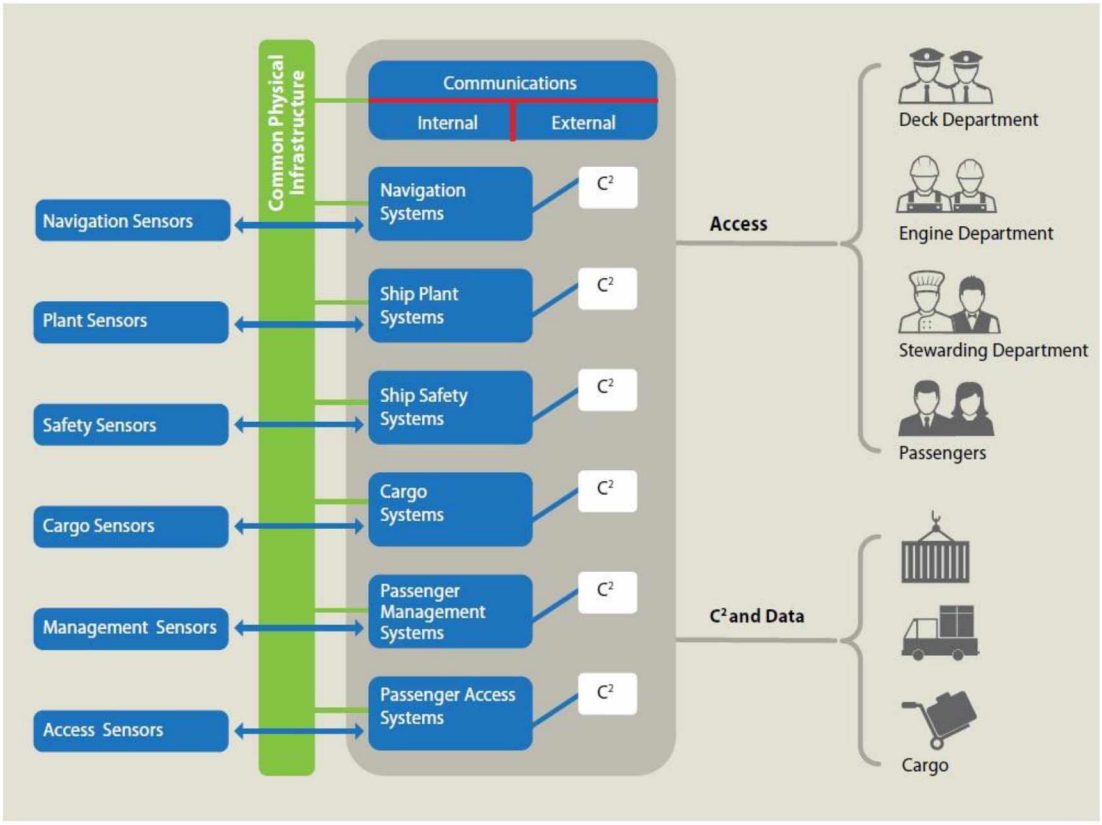
Ως συστήματα πρόσβασης των επιβατών θεωρούνται εκείνα στα οποία οι επιβάτες μπορεί να έχουν πρόσβαση ή να συνδέονται άμεσα μέσω μιας πύλης, όπως τα συστήματα online κρατήσεων ή πληρωμής υπηρεσιών, πρόσβασης σε υπηρεσίες πολυμέσων, όπως ταινίες ή μουσική και γενικότερα, συστήματα που επιτρέπουν τη σύνδεση στο Διαδίκτυο.

3.5.8 Σημασία της κυβερνο-ασφάλειας για τα πλοία

Η αδυναμία λειτουργίας ή η παραβίαση ενός ή περισσοτέρων από τα συστήματα λειτουργίας ενός πλοίου, που αναφέρθηκαν στις προηγούμενες υποενότητες, είναι σε θέση να έχει αρνητικές συνέπειες [29]:

- στην ασφάλεια του πληρώματος αλλά και των ατόμων ή των επιβατών που επηρεάζονται άμεσα από τις εργασιακές δραστηριότητες στους χώρους του πλοίου
- στην ασφαλή λειτουργία του πλοίου
- στην αύξηση της πιθανότητας να τεθούν σε κίνδυνο άλλα πλοία, ναυτιλιακές δομές στην ξηρά ή το περιβάλλον
- στην ταχύτητα και στην απόδοση λειτουργίας του πλοίου

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29



ΕΙΚΟΝΑ 7: Συστήματα του πλοίου που επηρεάζονται από την ασφάλεια στον κυβερνοχώρο [29]

Επιπλέον, η αποτυχία της ναυτιλιακής εταιρείας ή του προσωπικού του πλοίου να εκτιμήσει τη δομή και τη λειτουργία των συστημάτων και των συναφών διαδικασιών τους μπορεί να οδηγήσει σε έναν αριθμό ανεπιθύμητων καταστάσεων, όπως [29]:

- ακούσια έκθεση των ευαίσθητων συστημάτων, εφαρμογών ή δεδομένων σε μη εξουσιοδοτημένους χρήστες
- απώλεια ανθεκτικότητας ή αδυναμία λειτουργίας των συστημάτων
- ανεπανόρθωτες βλάβες που μπορούν να οδηγήσουν σε αλλεπάλληλη ή καταστροφική αστοχία κρίσιμων συστημάτων ή διαδικασιών

Οποιαδήποτε από τις ανεπιθύμητες αυτές καταστάσεις μπορεί επίσης να έχει σημαντικές οικονομικές απώλειες, διαταραχές στην επιχειρηματική λειτουργία, δυσφήμιση της ναυτιλιακής εταιρίας, περιβαλλοντικές συνέπειες, αλλά και τη δημιουργία νομικών ζητημάτων [4].

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

4 Κυβερνο-απειλές στη Ναυτιλία

4.1 Κυβερνο-απειλές σε λιμάνια & πλοία

Παραδοσιακά, οι επιθέσεις στα πλοία αφορούσαν την πειρατεία, την λαθραία επιβίβαση, την κλοπή και την καταστροφή. Αυτές οι επιθέσεις ήταν συχνά επιτυχημένες, καθώς κατά τη διάρκεια ταξιδιού ενός πλοίου η γρήγορη ανταπόκριση βοήθειας σε ένα εκπεμπόμενο σήμα SOS είναι δύσκολη. Παρά τη συνέχιση αυτού του είδους των απειλών, η καλή και μακροχρόνια γνώση τους έχει δημιουργήσει την ανάπτυξη στρατηγικών αντιμετώπισής τους. Αντίθετα, οι σύγχρονες επιθέσεις στον κυβερνοχώρο που αφορούν την ναυτιλία και ιδιαίτερα τα πλοία, είναι πολύ πιο καλά καμουφλαρισμένες ώστε να εκμεταλλεύονται τα τρωτά σημεία των συστημάτων των πλοίων και να τα παραβιάζουν για μεγαλύτερο χρονικό διάστημα και, ως εκ τούτου, με μεγαλύτερο όφελος [4].

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο οι συνέπειες των κυβερνο-επιθέσεων στα ναυτιλιακά συστήματα λιμανιών και πλοίων είναι πολλές. Ενώ κάποιες από τις επιθέσεις αυτές μοιάζουν σε μεγάλο βαθμό με αντίστοιχες παραδοσιακές επιθέσεις, οι υπόλοιπες είναι αρκετά καινοτόμες και βασίζονται στην σύγχρονη τεχνολογία, η οποία ναι μεν μπορεί να εξελίσσει τα συστήματα λιμανιών και πλοίων, αλλά ταυτόχρονα, δίνει τη δυνατότητα στους επιτιθέμενους εκμετάλλευσης των ευπαθειών τους και το σχεδιασμό πολλών διαφορετικών ειδών επιθέσεις.

4.2 Τρωτά σημεία λιμανιών και πλοίων

Στο προηγούμενο κεφάλαιο έγινε μια αναφορά στο πλήθος των συστημάτων που υπάρχουν στα σύγχρονα πλοία και λιμάνια. Από τα συστήματα αυτά κάποια είναι ιδιαίτερα κρίσιμα για την ίδια τη λειτουργικότητα των πλοίων ή των λιμανιών. Για το λόγο αυτό μια κυβερνο-επίθεση στα συστήματα αυτά μπορεί να οδηγήσει σε ανεπανόρθωτες βλάβες με όλες τις ήδη αναφερθείσες συνέπειες. Τα συστήματα αυτά είναι [4]:

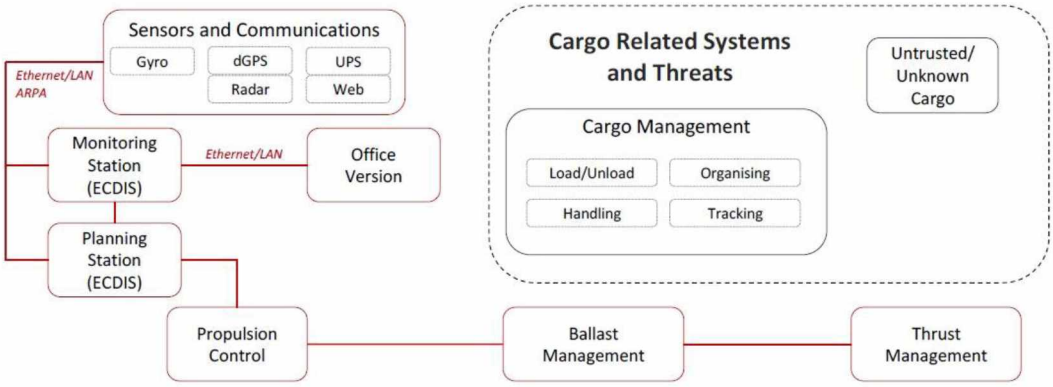
- τα συστήματα πλοήγησης και πρόωσης
- τα συστήματα διαχείρισης φορτίου

4.2.1 Συστήματα πλοήγησης και πρόωσης

Οι σημαντικές τεχνολογικές εξελίξεις έχουν δώσει τη δυνατότητα δημιουργίας συστημάτων πλοήγησης και πρόωσης, παρέχοντας στο πλήρωμα μια πιο ολοκληρωμένη εικόνα για το τι συμβαίνει μέσα και έξω από το πλοίο, συχνά σε πραγματικό χρόνο. Σκοπός των συστημάτων πλοήγησης και πρόωσης είναι η ανά πάσα στιγμή ένδειξη της ακριβούς θέσης του πλοίου, ώστε να βρίσκεται ευκολότερα η πορεία του και να αποφευχθεί πιθανή σύγκρουση με άλλα πλοία ή με την ξηρά. Η απόκτηση πρόσβασης σε αυτά τα συστήματα θα μπορούσε να επιτρέψει στους επιτιθέμενους να υπαγορεύσουν τη διαδρομή του σκάφους, είτε με την εξαπάτηση του πληρώματος μέσω ψευδών ενδείξεων των χρησιμοποιούμενων αισθητήρων ή με άμεσο έλεγχο του συστήματος πρόωσης.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Τα συστήματα πλοήγησης και πρόωσης συνήθως περιλαμβάνουν, χωρίς να περιορίζονται όμως, παγκόσμια συστήματα εντοπισμού θέσης (Global Positioning Systems - GPS), ναυτιλιακά αυτόματα συστήματα αναγνώρισης (marine Automatic Identification Systems - AIS) και ηλεκτρονικά συστήματα απεικόνισης και πληροφόρησης (Electronic Chart Display and Information Systems - ECDIS) (Εικ. 8). Η εφαρμογή τέτοιων συστημάτων, από τη μια πλευρά έχει ως αποτέλεσμα την ανάγκη για πληρώματα μικρότερου ανθρώπινου δυναμικού, από την άλλη όμως, αυτή η εξάρτηση από την τεχνολογία αυξάνει την παρουσία του πλοίου στον κυβερνοχώρο, και επομένως, τις πιθανότητες στο να γίνει στόχος προσφέροντας ευκαιρίες για κυβερνο-επιθέσεις.



ΕΙΚΟΝΑ 8: Απειλές στα συστήματα πλοήγησης και πρόωσης [4]

Τα σήματα παγκόσμιου δορυφορικού συστήματος πλοήγησης (Global Navigation Satellite System - GNSS) του GPS τείνουν να είναι πολύ αδύναμα από μεριάς ασφάλειας και συνεπώς οι σκόπιμες ή ακούσιες παρεμβολές μπορεί εύκολα να αποτρέψουν την ανάκτηση σήματος ή ακόμη και να δημιουργήσουν υπερφόρτωση στο κύκλωμα του δέκτη [30]. Κάτι τέτοιο, από μόνο του μπορεί να μην αποτελεί ζήτημα για ένα πλοίο που ταξιδεύει. Εάν όμως ένας εισβολέας εισάγει μια συσκευή δημιουργίας παρεμβολών, η οποία, για παράδειγμα, μπορεί να είναι κρυμμένη στο εμπόρευμα που μεταφέρει το πλοίο, αυτή η ευπάθεια του GPS μπορεί να γίνει εκμεταλλεύσιμη. Επιπλέον, λόγω του μικρού κόστους κατασκευής της, μια τέτοια συσκευή μπορεί εύκολα να αποκτηθεί και να χρησιμοποιηθεί ακόμα και από έναν άπειρο χάκερ. Ερευνητές του Πανεπιστημίου του Τέξας στο Όστιν, το 2013, κατάφεραν να εκμεταλλευτούν την έλλειψη αυθεντικότητας των δορυφορικών σημάτων GPS και να παρεκκλίνουν με επιτυχία την πορεία ενός σκάφους με μία συσκευή παραπλάνησης GPS (GPS spoofing) [31]. Από τη στιγμή που οι δέκτες GPS του σκάφους δεν επαλήθευσαν τα εισερχόμενα σήματα, οι «επιτιθέμενοι» είχαν τη δυνατότητα να παρακάμψουν την εισαγωγή των αυθεντικών σημάτων που έστελνε ο δορυφόρος, να στείλουν τα δικά τους «ψευδή» σήματα και τελικά να πάρουν τον πλήρη έλεγχο του συστήματος πλοήγησης του σκάφους χωρίς η παρουσία τους να ανιχνευθεί ή να προκαλέσει συναγερμούς.

Ένας εισβολέας είναι σε θέση να επιτεθεί σε ένα πλοίο για να παρέμβει ή να μεταβάλλει τις επικοινωνίες του, χρησιμοποιώντας το φορτίο που μεταφέρει το πλοίο. Το hardware υλικό του εισβολέα μπορεί να περάσει λαθραία στο πλοίο μέσω επιθέσεων στον κυβερνοχώρο, μεταβάλλοντας τα τιμολόγια, ελέγχοντας τα μηχανήματα φόρτωσης του φορτίου ή μολύνοντας το λογισμικό των λιμένων με χρήση κοινωνικής μηχανικής (social engineering).

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Μετά τη φόρτωσή του στο πλοίο, το φορτίο του χάκερ μπορεί να παραμείνει αδρανές μέχρι τον κατάλληλο χρόνο για επίθεση. Από τη στιγμή που όταν ένα πλοίο ταξιδεύει είναι πιο απομονωμένο, ο τρόπος αυτός επίθεσης θεωρείται μια εύλογη επιλογή [4].

Το σύστημα ECDIS που είναι υπεύθυνο για την προβολή ψηφιακών ναυτικών χαρτών μπορεί να παραβιαστεί με σκοπό την τροποποίηση των αρχείων και την εισαγωγή κακόβουλου περιεχομένου. Αυτό θα μπορούσε να αποτελέσει μια ισχυρή επίθεση, από την οποία δεν κινδυνεύουν μόνο τα εμπορικά πλοία [32]. Το 2013, αν και κατά λάθος, πολεμικό πλοίο των ΗΠΑ προσάραξε πάνω σε έναν κοραλλιογενή ύφαλο λόγω σφάλματος του ECDIS. Το συμβάν αυτό θα μπορούσε να συμβεί και μετά από κάποια κυβερνο-επίθεση στην οποία ο επιτιθέμενος θα μπορούσε να αλλάξει τους ψηφιακούς ναυτικούς χάρτες, πριν από την αναχώρηση του πλοίου ή κατά τη διάρκεια του ταξιδιού, με αποτέλεσμα την αναγκαστική προσάραξη του πλοίου σε κάποιου είδους φυσικό σχηματισμό (π.χ. ύφαλο) ή σε κάποια κακόβουλα δημιουργημένη ανθρώπινη κατασκευή. Η προκύπτουσα ζημία θα εξαρτιόταν σε μεγάλο βαθμό από το μέγεθος του πλοίου, το φορτίο και τον απώτερο στόχο της επίθεσης.

Μελέτες που έγιναν πάνω στο σύστημα ECDIS, έχουν διαπιστώσει ότι δεν έχει σχεδιαστεί με ασφάλεια και ότι τα συστήματα αυτά στα πλοία δεν ενημερώνονται συχνά και επομένως παρουσιάζουν ελλείψεις σε ανανεώσεις των patch ασφαλείας.

Μια άλλη ευπάθεια συστήματος έχει ανακαλυφθεί στο AIS, ένα ευρέως χρησιμοποιούμενο και υποχρεωτικό λογισμικό των πλοίων, που στοχεύει στην παρακολούθηση και την εύρεση της θέσης τους. Οι ερευνητές της ασφάλειας έχουν βρει τρόπους παραβίασης του συστήματος, μέσω δημιουργίας «έγκυρων» εντολών, αλλαγής της ρότας των πλοίων, επανάληψης εντολών και παρακολούθησης των πλοίων για πιθανές, φυσικές, επιθέσεις [33]. Και πάλι, το γενικό συμπέρασμα είναι ότι τα συστήματα AIS είναι κακώς σχεδιασμένα σε επίπεδο πρωτοκόλλου και σε επίπεδο υλοποίησης. Αυτή η αδυναμία μπορεί να οδηγήσει στην πειρατεία ενός πλοίου ή / και στη δημιουργία βλάβης σε άλλα πλοία ή σε χερσαίες υποδομές.

4.2.2 Συστήματα διαχείρισης φορτίου

Το σύστημα διαχείρισης φορτίου αποτελεί ένα ακόμα σύστημα ζωτικής σημασίας για τα πλοία καθώς είναι υπεύθυνο για το χειρισμό φόρτωσης και εκφόρτωσης, την παρακολούθηση και την οργάνωση των αγαθών που μεταφέρονται μέσω πλοίων. Εξαιρουμένων των επιβατών, αυτό ισχύει για πάνω από το 98,3% του παγκόσμιου στόλου [34]. Έτσι, η συντριπτική πλειοψηφία των 1,7 εκατομμυρίων πλοίων που διανέμουν αγαθά, απόβλητα και πόρους όπως το πετρέλαιο, είναι ευάλωτα μέσω των αυτοματοποιημένων συστημάτων τους για τη διαχείριση του φορτίου τους, καθώς και των λιμανιών που αλληλοεπιδρούν με αυτά τα συστήματα.

Για παράδειγμα, το 2013 ανακαλύφθηκε ότι διακινητές ναρκωτικών είχαν χακάρει το σύστημα πληροφορικής του λιμανιού της Αμβέρσας στο Βέλγιο. Αυτή η παραβίαση έδωσε στην ομάδα οργανωμένου εγκλήματος μια βαθιά γνώση των λεπτομερειών ασφάλειας και τη θέση κάθε εμπορευματοκιβωτίου που φθάνει στο λιμάνι, επιτρέποντάς τους να κλέψουν τα εμπορευματοκιβώτια πριν από την άφιξη του νόμιμου ιδιοκτήτη για την παραλαβή τους. Η συγκεκριμένη επίθεση ήταν ιδανική για την διακίνηση παράνομων ναρκωτικών ουσιών, κρυμμένων ανάμεσα σε νόμιμο φορτίο, πριν τη διεξαγωγή ερευνών σχετικά με το περιεχόμενο

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

των εμπορευματοκιβωτίων [35]. Επιπλέον, κάτι που δεν θα ήταν δυνατό στις παραδοσιακές φυσικές επιθέσεις, οι επιτιθέμενοι στον κυβερνοχώρο, παραβιάζοντας το συγκεκριμένο σύστημα διαχείρισης φορτίου, κατάφεραν να κρατήσουν αυτή την επίθεση μυστική για δύο ολόκληρα χρόνια.

Υπάρχουν δύο πιθανές μορφές επιθέσεων που σχετίζονται με την ανεξέλεγκτη και μυστική εκφόρτωση φορτίων. Πρώτον, το φορτίο μπορεί να κλαπεί αν ο κυβερνο-επιτιθέμενος είχε λεπτομέρειες σχετικά με τη διαδικασία εκφόρτωσης. Η μη ανακάλυψη κλοπής κοστίζει χρήματα, αλλά το πιο σημαντικό, θα μπορούσε να έχει ως αποτέλεσμα την κλοπή όπλων ή υλικών που μπορούν να χρησιμοποιηθούν με όπλα. Δεύτερον, τα ναρκωτικά και η διακίνηση ανθρώπων μπορούν να παραμείνουν ανεξέλεγκτα εάν τα συστήματα διαχείρισης φορτίου του λιμανιού αποστολής είτε του λιμανιού προορισμού ή και των δύο παραβιαστούν.

Άλλα σενάρια γύρω από επιθέσεις στον κυβερνοχώρο σε πλοία και λιμάνια όσον αφορά την απάτη, όπως η τροποποίηση ή η αποστολή πλαστών τιμολογίων, είναι επίσης δυνατά [36].

4.3 Πειρατεία

Οι επιθέσεις στον κυβερνοχώρο που εξαπολύονται εναντίον των διαφόρων συστημάτων των πλοίων ή των λιμανιών δίνουν τη δυνατότητα στους επιτιθέμενους να μπορούν να ελέγξουν τους στόχους τους, κάτι το οποίο μπορεί να έχει διάφορες συνέπειες ανάλογα με το είδος της επίθεσης. Για παράδειγμα, τα συστήματα πλοήγησης και πρόωσης μπορούν να παραβιαστούν μέσω ψευδών δεδομένων, παρεμβολών ή με κρυπτογράφηση βασικών αρχείων ή στοιχείων του συστήματος. Το ransomware είναι ένας τύπος κακόβουλου λογισμικού το οποίο όταν εγκατασταθεί σε έναν υπολογιστή κρυπτογραφεί τα αρχεία του και ζητάει από τον χρήστη την καταβολή κάποιου χρηματικού ποσού προκειμένου να τα αποκρυπτογραφήσει. Οι επιθέσεις ransomware είναι αρκετά κοινές στα παραδοσιακά συστήματα υπολογιστών, ενσύρματα ή ασύρματα, και μπορεί να χρησιμοποιηθούν ακόμα και στον τομέα της ναυτιλίας. Η εταιρεία McAfee διαπίστωσε ότι η χρήση του εν λόγω κακόβουλου λογισμικού σε επιθέσεις στον κυβερνοχώρο βρίσκεται σε έξαρση, έχοντας παρουσιάσει μια αύξηση της τάξης του 59% το 2017, στοιχείο που δείχνει ότι αποτελεί μια πολύ κερδοφόρα και αναπτυσσόμενη εφαρμογή εγκληματικής δραστηριότητας [37]. Μάλιστα, σύμφωνα με τους αναλυτές, το 2017 χαρακτηρίστηκε ως η «χρονιά του ransomware», αφού το περασμένο έτος χρήστες και επιχειρήσεις χρειάστηκε να αντιμετωπίσουν μαζικές επιθέσεις που επέφεραν απώλειες εκατοντάδων εκατομμυρίων [38].

Μέσω μια επίθεσης ransomware, ένα πλοίο θα μπορούσε να παραβιαστεί μέσω μιας μη ασφαλούς σύνδεσης δικτύου. Με πρόσβαση σε βασικά συστήματα, ο εισβολέας μπορεί να ελέγχει άμεσα το πλοίο ή να κρυπτογραφεί τα βασικά συστατικά του συστήματος έτσι ώστε να πλοίο να είναι στην ουσία ακυβέρνητο. Πλήρωμα και τυχόν επιβάτες θα μπορούσαν με τον τρόπο αυτό να κρατηθούν όμηροι στη θάλασσα μέχρι να πληρωθούν κάποια λύτρα. Αυτού του είδους η επίθεση είναι αναμφισβήτητα πολύ πιο επικίνδυνη από τις παραδοσιακές επιθέσεις ransomware λόγω της απομονωμένης φύση των πλοίων στη θάλασσα και την εξάρτησή τους από συστήματα που τους βοηθούν να γνωρίζουν τη θέση τους στον παγκόσμιο χάρτη και να μπορούν να ταξιδεύουν με ασφάλεια.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Εναλλακτικά, ένας χάκερ μπορεί να παραβιάσει ένα πλοίο για να το οδηγήσει πάνω σε άλλο στόχο, εμβολίζοντας άλλο πλοίο ή καταστρέφοντας άλλο επιθυμητό στόχο. Αυτού του είδους οι επιθέσεις μπορούν να έχουν ως απώτερο στόχο πετρελαϊκές εγκαταστάσεις, γέφυρες ή άλλες χερσαίες υποδομές. Αν και τέτοια γεγονότα δεν έχουν συμβεί μέχρι τώρα, λαμβάνοντας υπόψη την τάση που έχουν οι επιθέσεις εναντίων των πλοίων, τέτοιου είδους επιθέσεις δεν φαίνεται να είναι αδύνατες. Έτσι, η πειρατεία πλοίων μέσω επίθεσης στον κυβερνοχώρο, που περιέχουν υλικό βιολογικής επικινδυνότητας όπως επικίνδυνες χημικές ουσίες, πυρηνικά απόβλητα, κλπ. θα μπορούσαν να μην αποτελέσουν τον κύριο στόχο της επίθεσης αλλά να χρησιμοποιηθούν ως όπλο καταστροφής εξεδρών πετρελαίου βλάπτοντας σε μεγάλο βαθμό το περιβάλλον, την πανίδα της περιοχής, άλλους πολύτιμους πόρους και την τοπική οικονομία.

Ίδιου είδους επιθέσεις έχουν αναφερθεί και σε εξέδρες πετρελαίου, οι οποίες ακόμα και στην περίπτωση που είναι ανεπιτυχείς, υπάρχει η πιθανότητα πρόκλησης βλάβης μικρής έκτασης ή σημασίας στα συστήματα, η οποία εν ευθέτω χρόνο μπορεί να οδηγήσει σε πρόκληση ατυχήματος ή αδυναμία λειτουργίας του συστήματος. Κάτι τέτοιο θα μπορούσε τελικά να έχει ως αποτέλεσμα οικονομικές απώλειες, καταστροφή των υποδομών αλλά και απώλεια ανθρώπινων ζωών. Το 2010, αναφέρθηκε ότι μια εξέδρα πετρελαίου τερμάτισε τη λειτουργία της λόγω εισροής κακόβουλου λογισμικού. Ευτυχώς, η λειτουργία της εξέδρας τερματίστηκε πριν από την πολύ πιθανή έκρηξή της, αποτρέποντας όχι μόνο την καταστροφή της ίδιας της εξέδρας αλλά και τη μόλυνση της θάλασσας με πετρελαιοκηλίδα. Ωστόσο, χρειάστηκαν 19 ημέρες για την κατάργηση όλων των κακόβουλων προγραμμάτων, γεγονός που κόστισε ένα ποσό της τάξης των 700.000 δολαρίων την ημέρα [39].

4.4 Μη ενημερωμένο λογισμικό ασφάλειας

Οι λόγοι για τους οποίους τα συστήματα των πλοίων τείνουν να μην ενημερώνονται είναι πολλοί και διάφοροι. Ένας λόγος αφορά την κατασκευή του μεγαλύτερου μέρους του παγκόσμιου στόλου, ο οποίος ναυπηγήθηκε πολλά χρόνια πριν η ασφάλεια στον κυβερνοχώρο αποτελέσει ζήτημα ζωτικής σημασίας. Ένας δεύτερος, αφορά την παλαιότητα των συστημάτων των πλοίων η οποία επι το πλείστον είναι ασύμβατη με τα νέα λογισμικά. Ως εκ τούτου, ακόμα και σήμερα είναι συχνή η χρήση συστημάτων με μη ενημερωμένο λογισμικό ασφάλειας. Το εν λόγω θέμα μπορεί να γίνει πιο πολύ κατανοητό αν ληφθεί υπόψη ότι, εν έτη 2015, το πρόγραμμα SPAWAR του αμερικανικού πολεμικού ναυτικού περιλάμβανε πάνω από 100.000 σταθμούς εργασίας με λειτουργικό σύστημα Windows XP [40]. Για την ακρίβεια, αντί να ξοδέψει ένα σεβαστό ποσό στην ανανέωση των συστημάτων τους, από τη στιγμή μάλιστα που το λειτουργικό Windows XP έχει σταματήσει να υποστηρίζεται από την Microsoft, το αμερικανικό ναυτικό επέλεξε να πληρώσει 9 εκατομμύρια δολάρια το χρόνο για να λαμβάνει υποστήριξη για την συγκεκριμένη έκδοση των Windows. Η ιδέα του αμερικανικού ναυτικού βασίστηκε στον ισχυρισμό ότι αυτό αποτελεί προσωρινό μέτρο μέχρι την πλήρη αναβάθμιση του υπάρχοντος hardware υλικού και των συστημάτων υποστήριξης. Μια τέτοια αναβάθμιση είναι εκ των ουκ άνευ καθώς τα μη ανανεωμένα λογισμικά ασφάλειας παρουσιάζουν πολλά και σοβαρά τρωτά σημεία.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Μελέτη από εταιρεία θαλάσσιου κυβερνοχώρου διαπίστωσε ότι το 37% των διακομιστών που εκτελούσαν λογισμικό της Microsoft απέτυχαν να κατεβάσουν το σωστό patch και ήταν ευάλωτοι σε επιθέσεις [41]. Αυτό καταδεικνύει ότι, παρόλο που τα ίδια τα συστήματα μπορεί να είναι ενημερωμένα, εξακολουθούν να είναι ευάλωτα σε επιθέσεις κυβερνοχώρου αν δεν μπορούν να λάβουν και να εφαρμόσουν τα διαθέσιμα patch ασφάλειας. Σε αντίθεση με τα παραδοσιακά δίκτυα υπολογιστών της ξηράς, το συγκεκριμένο ζήτημα είναι ιδιαίτερα σοβαρό για τα συστήματα των πλοίων. Με δεδομένο ότι λόγω των περιβαλλοντικών επιπτώσεων, οι χρόνοι ταξιδιού των μεγάλων πλοίων τείνουν να είναι μεγαλύτεροι και όχι μικρότεροι, το παράθυρο επίθεσης μπορεί να διαρκέσει εβδομάδες [42].

Εάν εντοπιστεί ευπάθεια λογισμικού ακριβώς μετά την έναρξη του ταξιδιού ενός πλοίου που έχει ήδη στοχοποιηθεί, είναι πολύ πιθανή η αποστολή ενός μη επανδρωμένου σκάφους (drone) για την εκμετάλλευση αυτής της ευπάθειας, πριν το πλοίο μπορέσει να κατεβάσει και να κάνει εφαρμογή μιας ενημερωμένης έκδοσης patch ασφαλείας,. Κάτι ανάλογο έχει πραγματοποιηθεί από το αμερικανικό ναυτικό, το οποίο έστειλε με επιτυχία ένα μη επανδρωμένο υποβρύχιο, σε μια υποθαλάσσια αποστολή, το 2015 [43]. Με τον τρόπο αυτό, η χρήση μη επανδρωμένου σκάφους θα μπορούσε να πραγματοποιηθεί για την εξ αποστάσεως εγκατάσταση κακόβουλου λογισμικού σε αργά κι ευάλωτα πλοία.

4.5 Οικονομικά οφέλη

Οι σύγχρονες εξελίξεις στο χώρο της πληροφορικής έχουν δημιουργήσει το κατάλληλο υπόβαθρο για την ευκολότερη και φθηνότερη δημιουργία κακόβουλων προγραμμάτων. Η ανεύρεση εργαλείων στο Διαδίκτυο για την ανάπτυξη κακόβουλων λογισμικών με απώτερο σκοπό την εκμετάλλευση των τρωτών σημείων, είναι πλέον μια πολύ απλή διαδικασία που δίνει στους επιτιθέμενους τη δυνατότητα, ακόμα κι αν δεν έχουν μεγάλη γνώση και εμπειρία προγραμματισμού, να προκαλέσουν σημαντικές ζημιές σε μεμονωμένους υπολογιστές, δίκτυα και συστήματα [44]. Όσον αφορά το χώρο της ναυτιλίας, το hardware υλικό που απαιτείται για το χακάρισμα των συστημάτων των πλοίων, στο πλείστο των περιπτώσεων, είναι σχετικά φθηνό, καθώς τα προς επίθεση συστήματα είναι συχνά ξεπερασμένα και λιγότερο εξελιγμένα από άλλους στόχους. Επιπλέον, τα κίνητρα πραγματοποίησης μιας επίθεσης σε πλοία είναι πολλά και έχουν να κάνουν σε μέγιστο βαθμό με οικονομικά οφέλη, καθώς πάνω από το 90% του παγκόσμιου εμπορίου γίνεται μέσω των θαλάσσιων συγκοινωνιών [34].

Επιπλέον, αυτές οι μεγάλες αποστολές πολύτιμων αγαθών ταξιδεύουν για μεγάλες χρονικές περιόδους χωρίς το μέγιστο της προστασίας και μερικές φορές χωρίς ανθρώπινη επίβλεψη. Το οικονομικό όφελος των επιθέσεων στον κυβερνοχώρο είναι συνεπώς υψηλό, ενώ παράλληλα παρέχεται ο απαραίτητος χρόνος εξαφάνισης των αποδεικτικών στοιχείων του εγκλήματος. Τέτοιες επιθέσεις είναι επίσης ιδιαίτερα κερδοφόρες, όπως αναφέρθηκε σε προηγούμενες ενότητες, όταν ο στόχος τους είναι το λαθρεμπόριο και η απάτη.

Επομένως, με δεδομένο ότι κάποια πλοία ή συστήματα ενδέχεται να διατρέχουν μεγαλύτερο κίνδυνο σε σχέση με άλλα, ανάλογα με την πιθανότητα επίθεσης και την αξία του ίδιου του πλοίου και του φορτίου που μεταφέρει, η σωστή διαχείριση των κινδύνων και η κατανόηση της καταλληλότητας των τεχνικών αντιμετώπισης των κινδύνων αυτών, καθίσταται σημαντικό στοιχείο της ασφάλειας στον κυβερνοχώρο στον τομέα της ναυτιλίας.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

5 Αντιμετώπιση των Κυβερνο-επιθέσεων στο χώρο της Ναυτιλίας

5.1 Τρόποι αντιμετώπισης

Ένας ουσιαστικός τρόπος αντιμετώπισης των επιθέσεων στον κυβερνοχώρο στον τομέα της ναυτιλίας, και ειδικότερα στα πλοία, είναι η κατά καιρούς ενημέρωση των λειτουργικών των υφιστάμενων συστημάτων των πλοίων. Πιο σημαντικός όμως τρόπος αντιμετώπισης θα μπορούσε να αποτελέσει ο σχεδιασμός των συστημάτων των πλοίων με γνώμονα την αυξημένη ασφάλεια στον κυβερνοχώρο. Ένας τέτοιος σχεδιασμός, δεν απαιτεί απαραιτήτως αλλαγή της υποδομής με κάποιο ακριβότερο εξοπλισμό, αλλά μπορεί να επιτευχθεί μέσω έξυπνης «απομόνωσης» των διαφόρων συστημάτων με πιο ασφαλείς κωδικούς πρόσβασης ή με χρήση εικονικών δικτύων τα οποία θα μπορούσαν να μη επιτρέπουν την άμεση διασύνδεση των συστημάτων με το Διαδίκτυο. Ο σχεδιασμός αυτός θα πρέπει επίσης να τροποποιήσει τα συστήματα με τέτοιο τρόπο ώστε να γίνεται συνεχής έλεγχος πρόληψης ή ανίχνευσης και επισήμανσης κάθε πιθανής απόπειρας παραβίασης ή άλλου τρόπου επίθεσης στον κυβερνοχώρο, χωρίς όμως να επηρεάζεται η λειτουργικότητα των συστημάτων και η ταχύτητα απόκρισής τους, καθώς η ανθεκτικότητα των εντολών και των λειτουργικών ελέγχων των συστημάτων αποτελούν σημαντικότατα στοιχεία.

Με βάση αυτή τη φιλοσοφία, οι μηχανικοί του αμερικανικού Πολεμικού Ναυτικού έχουν σχεδιάσει ένα σύστημα προστασίας στον κυβερνοχώρο με την ονομασία RHIMES (Resilient Hull, Mechanical, and Electrical Security), ένα σύστημα που βρίσκεται σήμερα σε φάση δοκιμών. Στόχος του συστήματος είναι η προστασία των πολεμικών πλοίων από χακάρισμα μέσω Διαδικτύου [45]. Το RHIMES έχει σχεδιαστεί ειδικά για την προστασία των βασικών συστημάτων του πλοίου από απομακρυσμένο έλεγχο ή ακόμη και απενεργοποίηση. Το σύστημα λειτουργεί με τη χρήση ενσωματωμένων συστημάτων αντιγράφων ασφαλείας του πλοίου για την αποτροπή βλάβης σε κρίσιμες στιγμές, εφαρμόζοντας την διαφορετικότητα στον προγραμματισμό αυτών των συνιστωσών. Με αυτό τον τρόπο, ακόμα και αν ένας εισβολέας αποκτήσει πρόσβαση σε μια κύρια συνιστώσα, το αντίγραφο ασφαλείας δεν επηρεάζεται και θα μπορούσε να πάρει εύκολα τη θέση της. Αυτό θα δώσει χρόνο στο πλήρωμα ώστε να μετριάσει την επίθεση, χωρίς να χρειάζεται να ανησυχεί για την γενική ασφάλεια των βασικών συστημάτων του πλοίου. Ενώ, η βασική φιλοσοφία των συστημάτων αντιμετώπισης των κυβερνο-επιθέσεων επικεντρώνεται συνήθως στην πρόληψη, το RHIMES βασίζεται στην πολυεπίπεδη αρχιτεκτονική των πλοίων η οποία παρέχει τον απαραίτητο χρόνο επανεκκίνησης με ασφάλεια των hardware συνιστωσών των συστημάτων, έτσι ώστε κατά την επιστροφή του πλοίου στο λιμάνι, να δοθεί η δυνατότητα δημιουργίας και εγκατάστασης των patch ασφαλείας στα πληγέντα συστήματα [47].

Ωστόσο, με δεδομένο ότι συστήματα όπως το RHIMES είναι επί του παρόντος περιορισμένα, μια πιο συνετή επιλογή αντιμετώπισης των επιθέσεων στον κυβερνοχώρο στον τομέα της ναυτιλίας είναι η αξιοποίηση του υφιστάμενου ανθρώπινου δυναμικού. Ο

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

ανθρώπινος παράγοντας μπορεί να καταστεί επωφελής από πολλές απόψεις όσον αφορά την ασφάλεια. Πρώτον, μπορεί ανά πάσα στιγμή να ελέγχει τα συστήματα ως προς την προβλεπόμενη λειτουργία τους. Δεύτερον, εάν τα συστήματα τροποποιηθούν με τέτοιο τρόπο ώστε να μην λειτουργούν αυτόνομα αλλά να έχουν μια αλληλεπίδραση με τους χειριστές τους κατά τη διάρκεια πιθανών επιθέσεων στον κυβερνοχώρο, τότε είναι πιο δύσκολο για έναν εισβολέα να παραμείνει μη ανιχνεύσιμος. Η εκπαίδευση του ανθρώπινου δυναμικού σε θέματα διατήρησης της ασφάλειας στα συστήματα είναι επίσης σημαντική. Η χρήση και προστασία των κωδικών πρόσβασης και των κλειδιών πρόσβασης, η σωστή χρήση του συστήματος, τα πιθανά συμπτώματα μιας επίθεσης και ο τρόπος απενεργοποίησης, επανεκκίνησης ή αναστολής ορισμένων συστημάτων είναι επίσης χρήσιμες πληροφορίες για την ασφαλή φύλαξη των ναυτιλιακών συστημάτων ξηράς και θάλασσας.

5.2 Ανθρώπινος παράγοντας

Η επίδραση του ανθρώπινου παράγοντα στην ασφάλεια στον κυβερνοχώρο δεν μπορεί να υποτιμηθεί. Το ανθρώπινο στοιχείο διαδραματίζει σημαντικό ρόλο στην πλειονότητα των περιστατικών στον κυβερνοχώρο [47]. Λόγω του υψηλού επιπέδου συνδεσιμότητας που παρουσιάζουν τα ναυτιλιακά συστήματα ξηράς και θάλασσας, ακόμη και μικρά ανθρώπινα σφάλματα, για παράδειγμα από τον χειριστή ενός συστήματος, μπορεί να έχουν σοβαρές συνέπειες. Η εκπαίδευση του προσωπικού πάνω σε θέματα ασφάλειας στον κυβερνοχώρο κρίνεται εξαιρετικά απαραίτητη και θα μπορούσε να βοηθήσει στην αποφυγή περιστατικών που προκαλούνται, για παράδειγμα, από επιθέσεις κοινωνικής μηχανικής ή από την παρουσία εξωγενών ανθρώπινων παραγόντων στις ναυτιλιακές εγκαταστάσεις ή ακόμα και από την πιθανότητα ύπαρξης εσωτερικών απειλών ή αθέλητων σφαλμάτων.

Παρά το προηγμένο της τεχνολογίας των συστημάτων και συσκευών, ο χειρισμός τους γίνεται μέσω κάποιου ανθρώπινου παράγοντα, επομένως το ανθρώπινο λάθος στην περίπτωση της ασφάλειας στο κυβερνοχώρο, μπορεί να έχει σοβαρές συνέπειες. Άλλωστε, σύμφωνα με τους Hansen & Rahman, η ασφάλεια στον κυβερνοχώρο, δεν αποτελεί μόνο τεχνολογικό θέμα αλλά είναι εξίσου ζήτημα πολιτισμού και στάσης ζωής. Οι καλύτεροι αλγόριθμοι κρυπτογράφησης στον κόσμο είναι άχρηστοι αν κάποιος γράψει τον κωδικό πρόσβασης του σε ένα χαρτί σημειώσεων και το κολλήσει πάνω στον υπολογιστή που χρησιμοποιεί [48]. Επομένως, η εκπαίδευση του προσωπικού με σκοπό τη χρήση των όποιων εργαλείων με αποτελεσματικό και ασφαλή τρόπο, αποτελεί το κλειδί για την αποφυγή ατυχημάτων.

Η ολιστική προσέγγιση δίνει τη δυνατότητα περιγραφής με αποτελεσματικό τρόπο της σημασίας του ανθρώπινου παράγοντα όσον αφορά την ασφάλεια στον κυβερνοχώρο [49]. Για παράδειγμα, η απενεργοποίηση των περιττών θυρών USB ενός φορητού υπολογιστή μπορεί να είναι μια τεχνική μέθοδος ελέγχου για την ασφάλεια στον κυβερνοχώρο, καθώς μειώνει την πιθανότητα εισαγωγής κακόβουλων λογισμικών στο σύστημα μέσω του συγκεκριμένου υπολογιστή. Ο φορητός υπολογιστής μπορεί να θεωρηθεί ότι βρίσκεται στο κέντρο αυτής της πολυεπίπεδης ολιστικής προσέγγισης. Ο εν λόγω φορητός υπολογιστής βρίσκεται εντός ενός ερμαρίου ή πάνω σε ένα γραφείο, τα οποία αντιπροσωπεύουν το επόμενο επίπεδο της ολιστικής προσέγγισης. Το ερμάριο βρίσκεται σε μια καμπίνα ενός πλοίου ή το γραφείο βρίσκεται σε ένα δωμάτιο ενός κτηρίου του λιμανιού, τα οποία αντιπροσωπεύουν τα επόμενα

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

επίπεδα. Η πρόσβαση από το ένα επίπεδο στο άλλο είναι εξασφαλισμένη - για παράδειγμα, η είσοδος στο πλοίο ή στο κτήριο επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα και, στη συνέχεια, μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στην καμπίνα ή στο δωμάτιο, αντίστοιχα. Τέλος, το κλειδί εισόδου στην καμπίνα ή στο γραφείο μπορεί να είναι προσβάσιμο σε μικρό αριθμό ατόμων. Με όλες αυτές τις δικλείδες ασφαλείας, ο επίδοξος επιτιθέμενος, για να έχει πρόσβαση στις θύρες USB του φορητού υπολογιστή, θα πρέπει να μπει σε μια διαδικασία βημάτων τα οποία θα του δώσουν τη δυνατότητα να τις ξεπεράσει, γεγονός που σημαίνει ότι θα πρέπει να έχει κάποιου είδους επαφή με ανθρώπινο παράγοντα. Ο επιτιθέμενος μπορεί, για παράδειγμα, να αφεθεί να εισέλθει εντός του πλοίου ή εντός του κτηρίου του λιμανιού μέσω της κοινωνικής μηχανικής, η οποία ενεργοποιείται από ανθρώπινο σφάλμα. Επομένως, αν τα μέτρα προστασίας είναι επιτυχημένα σε όλα τα επίπεδα της ολιστικής αυτής προσέγγισης, ο επιτιθέμενος δεν θα μπορέσει να αποκτήσει ποτέ πρόσβαση στο φορητό υπολογιστή. Σε αυτήν την περίπτωση, η απενεργοποίηση των περιττών θυρών USB θα πρέπει να γίνεται απλά και μόνο για την ολοκλήρωση των μέτρων προστασίας και επομένως η σημασία του είναι απλά τυπική. Το σενάριο αυτό αντικατοπτρίζει τη συνολική σημασία του σχεδιασμού και της υλοποίησης μέτρων για την ασφάλεια στον κυβερνοχώρο, ξεκινώντας από το υψηλότερο επίπεδο.

5.3 Σύνοψη των προσεγγίσεων αντιμετώπισης των κυβερνο-επιθέσεων

Μια ανασκόπηση στη βιβλιογραφία δείχνει καθαρά ότι το ζήτημα της ασφάλειας στον κυβερνοχώρο στον ναυτιλιακό τομέα απασχολεί ολοένα και περισσότερο όλους τους εμπλεκόμενους φορείς. Η τάση αυτή αποδεικνύεται από το γεγονός ότι συνεχώς εμφανίζονται νέες μελέτες και έρευνες από διάφορους φορείς στις οποίες παρουσιάζονται προσεγγίσεις και βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο. Στις μελέτες αυτές αναγνωρίζεται επίσης η ανάγκη ανάπτυξης μιας κοινής τυποποίησης της ασφάλειας στον κυβερνοχώρο. Τέλος, ανεξάρτητα από τον φορέα έκδοσης, η κυρίαρχη προσέγγιση στις προαναφερόμενες μελέτες και έρευνες αφορά τους κινδύνους και τα τρωτά σημεία που μπορούν να εντοπιστούν στα συστήματα λιμανιών και πλοίων.

5.3.1 Διεθνή πρότυπα

Στο διεθνές προσκήνιο έχουν παρουσιαστεί διάφορα βιομηχανικά πρότυπα σχετικά με την ασφάλεια στον κυβερνοχώρο. Η μελέτη των προτύπων αυτών δείχνει την κοινή τους σύγκλιση σε προσεγγίσεις υψηλού επιπέδου στην γενικότερη έννοια της ασφάλειας. Οι διεθνείς οργανισμοί που έχουν δημιουργήσει τα περισσότερα πρότυπα πάνω στο θέμα της ασφάλειας είναι η Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission – IEC) και ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization – ISO). Διεθνώς αναγνωρισμένα, από τον βιομηχανικό κλάδο, πλαίσια έχουν δημοσιευθεί επίσης από οργανισμούς όπως το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (Information Systems Audit and Control Association – ISACA), ο ανεξάρτητος Οργανισμός Information Security Forum (ISF) και το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST).

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Οι περισσότερες οδηγίες που έχουν δημοσιευτεί και αφορούν τον τομέα της ασφάλειας στον κυβερνοχώρο ακολουθούν κοινά αναγνωρισμένα διεθνή πρότυπα όπως η οικογένεια προτύπων ISO / IEC 27000 (2016) και το πρότυπο IEC 15408 (2008 & 2009) για την ασφάλεια των πληροφοριακών τεχνολογιών (Information Technology - IT) των ISO και IEC. Το πρότυπο IEC 62443 (2016) χρησιμοποιείται από τη Διεθνή Ένωση Νηογνωμόνων (International Association of Classification Societies - IACS) για την ασφάλεια, ενώ το πρότυπο λειτουργικής ασφάλειας ηλεκτρονικών συστημάτων IEC 61508 (2010) παρέχει καθοδήγηση για την ασφάλεια των λειτουργικών τεχνολογιών (Operational Technology – OT). Επίσης έχουν δημοσιευτεί εμπορικά ή εν μέρει εμπορικά πλαίσια για ολιστική διαχείριση των καθολικών πληροφοριακών τεχνολογιών, όπως το πρότυπο COBIT 5 (2012) και το πρότυπο Information Security Forum (ISF) Standard of Good. Practice (2016), το οποίο καλύπτει τα πρότυπα ISO / IEC 27002: 2013 και COBIT 5 [50].

Ιδιαίτερο ενδιαφέρον παρουσιάζει το NIST Framework (2017), ένα πλαίσιο το οποίο εμφανίστηκε ως ένα επιλεκτικό κριτήριο αξιολόγησης της ασφάλειας στον κυβερνοχώρο [51]. Παρουσιάζοντας μια προσέγγιση βασισμένη στον κίνδυνο, αυτό το ευέλικτο και τεχνολογικά ουδέτερο πλαίσιο συμπληρώνει τη διαδικασία διαχείρισης κινδύνου και το πρόγραμμα ασφάλειας στον κυβερνοχώρο των τομέων στους οποίους εφαρμόζεται. Το πλαίσιο βασίζεται στη σύγκριση της παρούσας κατάστασης της ασφάλειας στον κυβερνοχώρο σε σχέση με αυτή που έχει επιλεχθεί ως στόχος, εντοπίζοντας και δίνοντας προτεραιότητα στις ευκαιρίες βελτίωσής της. Παρέχει επίσης έναν πλήρη κατάλογο αποδεκτών από τη βιομηχανία προτύπων με σκοπό την παροχή καθοδήγησης εφαρμογών βελτίωσης των προσεγγίσεων ασφάλειας στον κυβερνοχώρο.

5.3.2 Δημοσιεύσεις του διεθνούς ναυτιλιακού τομέα

Σε αντίθεση με τα διεθνή πρότυπα που ασχολούνται με την ασφάλεια στον κυβερνοχώρο σε γενικότερο πλαίσιο, διεθνείς οργανισμοί και κρατικοί φορείς έχουν παρουσιάσει κατά καιρούς δημοσιεύσεις που αφορούν την ασφάλεια στον κυβερνοχώρο στον ναυτιλιακό τομέα. Τέτοιες δημοσιεύσεις έχουν εκδοθεί από τον Ευρωπαϊκό Οργανισμό Δικτύων και Πληροφοριών (ENISA), από τον Διεθνή Ναυτιλιακό Οργανισμό (IMO), από το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο (BIMCO) και από την κυβέρνηση του Ηνωμένου Βασιλείου.

Η ανάλυση του ENISA (2011) επεσήμανε τις βασικές προκλήσεις που καλείται να αντιμετωπίσει ο ναυτιλιακός τομέας: την ευρωστία των τεχνολογιών πληροφοριών και επικοινωνιών που χρησιμοποιούνται στα συστήματα των πλοίων και των λιμανιών κατά των επιθέσεων στον κυβερνοχώρο, τον διαχωρισμό του ναυτιλιακού τομέα σε διαφορετικά επίπεδα και την χαμηλή ευαισθητοποίηση του ναυτιλιακού τομέα στο θέμα της ασφάλειας στον κυβερνοχώρο [17]. Οι συστάσεις του ENISA αφορούν μια ολιστική προσέγγιση πρακτικών διαχείρισης της ασφάλειας που να βασίζεται στην πρόληψη των κινδύνων του κυβερνοχώρου και των πληροφοριών. Κύριο σημείο των πρακτικών αυτών είναι η εφαρμογή εκστρατειών ευαισθητοποίησης και η ανάπτυξη μιας κοινής στρατηγικής και βέλτιστων πρακτικών με την προσθήκη της ασφάλειας στον κυβερνοχώρο στις πολιτικές φυσικής ασφάλειας της ναυτιλιακής βιομηχανίας. Ο ENISA τόνισε τη σημασία της κοινής πληροφόρησης μεταξύ διαφόρων παραγόντων και την εναρμόνιση και ευθυγράμμιση των πολιτικών ασφάλειας.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Οι κατευθυντήριες γραμμές για τη διαχείριση των κινδύνων του κυβερνοχώρου στον ναυτιλιακό τομέα, μια έκδοση του IMO (2017), στην οποία προσαρμόζεται το πρότυπο NIST Framework, μπορεί να θεωρηθεί ως απάντηση στην ανάλυση του ENISA. Οι κατευθυντήριες γραμμές του IMO εισήγαγαν πέντε λειτουργικά στοιχεία για αποτελεσματική και συνεχή διαχείριση των κινδύνων του κυβερνοχώρου [18]:

- ***Προσδιορισμός:*** Καθορισμός των ρόλων και των ευθυνών του προσωπικού διαχείρισης των κινδύνων στον κυβερνοχώρο και εντοπισμός των συστημάτων, επί μέρους στοιχείων, δεδομένων και δυνατοτήτων που η διατάραξή τους ενέχει κινδύνους για τη λειτουργία του πλοίου
- ***Προστασία:*** Εφαρμογή διαδικασιών και μέτρων ελέγχου κινδύνων και σχεδίαση πλάνου έκτακτης ανάγκης προστασίας από απρόσμενο περιστατικό στον κυβερνοχώρο που να εξασφαλίζει την ανεπηρέαστη συνέχιση των ναυτιλιακών δραστηριοτήτων
- ***Εντοπισμός:*** Ανάπτυξη και υλοποίηση δραστηριοτήτων απαραίτητες για τον εντοπισμό ενός περιστατικού στον κυβερνοχώρο σε όσο το δυνατόν μικρότερο χρόνο
- ***Απόκριση:*** Ανάπτυξη και υλοποίηση δραστηριοτήτων και σχεδίων για την παροχή ανθεκτικότητας και αποκατάστασης των συστημάτων που απαιτούνται για ναυτιλιακές δραστηριότητες από απρόσμενο περιστατικό στον κυβερνοχώρο
- ***Ανάκτηση:*** Προσδιορισμός των μέτρων δημιουργίας αντίγραφων ασφαλείας και επαναφοράς των απαραίτητων πληροφοριακών συστημάτων που απαιτούνται για ναυτιλιακές δραστηριότητες από απρόσμενο περιστατικό στον κυβερνοχώρο

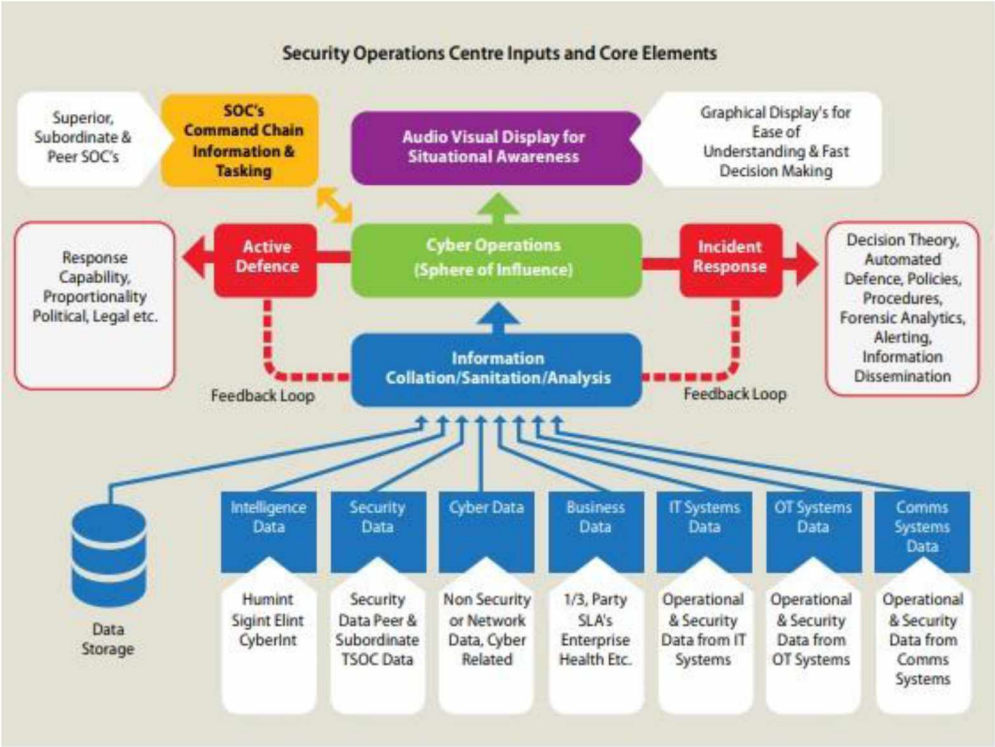
Ως συνέχεια και σε απόλυτη συμφωνία με τις κατευθυντήριες γραμμές του IMO και του προτύπου NIST Framework, το BIMCO δημοσίευσε πιο περιεκτικές και λεπτομερείς κατευθυντήριες γραμμές σχετικά με την ασφάλεια στον κυβερνοχώρο των πλοίων (2016). Στην προσέγγιση του BIMCO, διακρίνονται έξι βασικές έννοιες της αποτελεσματικής διαχείρισης των κινδύνων του κυβερνοχώρου (Εικ. 9) [52]: εντοπισμός απειλών και τρωτών σημείων, αξιολόγηση της έκθεσης σε κίνδυνο, ανάπτυξη μέτρων προστασίας και ανίχνευσης, θέσπιση σχεδίων έκτακτης ανάγκης και απόκριση σε / ανάκαμψη από περιστατικό στον κυβερνοχώρο.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

ΕΙΚΟΝΑ 9: Οι 6 βασικές έννοιες της αποτελεσματικής διαχείρισης των κινδύνων του κυβερνοχώρου του BIMCO [52]

Το 2017, η κυβέρνηση του Ηνωμένου Βασιλείου εξέδωσε το «Κώδικας Πρακτικής – Κυβερνο-Ασφάλεια για Πλοία», μια έκδοση που μπορεί να θεωρηθεί ως παράδειγμα απάντησης σε επίπεδο κράτους στο θέμα της ασφάλειας στον κυβερνοχώρο στον ναυτιλιακό τομέα [29]. Ο Κώδικας αυτός παρέχει ένα ολοκληρωμένο πακέτο πληροφοριών που αφορούν το πλαίσιο διαχείρισης και μείωσης των κινδύνων στον κυβερνοχώρο. Ο Κώδικας αντιπροσωπεύει επίσης μια προσέγγιση αξιολόγησης της ασφάλειας στον κυβερνοχώρο των πλοίων και καθορίζει ένα σχέδιο αντιμετώπισης των κυβερνο-επιθέσεων με βάση την ασφάλεια των πλοίων στον κυβερνοχώρο. Σε αντίθεση με προηγούμενες δημοσιεύσεις, δεν αναφέρεται στο πρότυπο NIST Framework σε κανένα σημείο, αλλά παρέχεται μια περιγραφή όλων των υπεύθυνων φορέων και ατόμων για την ασφάλεια στον κυβερνοχώρο και συστήνεται η ίδρυση ενός κέντρου επιχειρήσεων ασφαλείας (Εικ. 10) όπως επίσης και μιας πρωτοβουλίας ανταλλαγής πληροφοριών σχετικά με την ασφάλεια στον κυβερνοχώρο, όπως η CiSP (Cyber Information Sharing Partnership).

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29



ΕΙΚΟΝΑ 10: Κέντρο επιχειρήσεων ασφαλείας [29]

5.3.3 Δημοσιεύσεις Νηογνωμόνων

Κάποιες από τις σημαντικότερες δημοσιεύσεις νηογνωμόνων διεθνούς επιπέδου έχουν εκδοθεί από τους Lloyd's Register, DNV GL και ABS. Στις δημοσιεύσεις αυτές, οι νηογνώμονες συμπληρώνουν τους κανόνες τους με συνιστώμενες πρακτικές οδηγίες.

Η προσέγγιση του βρετανικού νηογνώμονα Lloyd's Register για τη διασφάλιση της ασφάλειας στον κυβερνοχώρο, στη δημοσίευση "Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping" (2016), προσδιορίζει έξι βασικούς τομείς κινδύνου[53]:

- σύστημα
- ανθρώπινος παράγοντας
- λογισμικό
- δίκτυο και επικοινωνίες
- διασφάλιση δεδομένων
- ασφάλεια στον κυβερνοχώρο

Στη δημοσίευση αυτή συνιστάται η χρήση μια προσέγγισης βάσει κινδύνου, όπως το NIST Framework ή η διαδικασία ARBD (Assessment of Risk Based Design) που παρουσιάζεται από τον ίδιο τον βρετανικό νηογνώμονα, καθώς και η διαρθρωμένη προσέγγιση ανθρωποκεντρικού χαρακτήρα του προτύπου ISO 9241-210 (2010). Μια τέτοια προσέγγιση διευκολύνει την εξέταση των ζητημάτων του ανθρώπινου παράγοντα που προκύπτουν από τη χρήση των τεχνολογιών πληροφοριών και επικοινωνιών αντί των κλασικών, αμιγώς ναυτικών,

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

συστημάτων. Στη δημοσίευση του Lloyd's Register υπογραμμίζεται επίσης η αυξανόμενη σημασία της συνεχούς ενημέρωσης του λογισμικού, λόγω της ενσωμάτωσης του στο ολοκληρωμένο σύστημα δικτύων και επικοινωνιών, κάτι που θα μπορούσε να αυξήσει την ασφάλεια στο σύνολο των συστημάτων που χρησιμοποιούνται. Για την εφαρμογή αυτής της συνεχούς ενημέρωσης, απαιτούνται σωστές μηχανικές διαδικασίες και συμμόρφωση με το πρότυπο IEC 61508 (2010). Σύμφωνα, τέλος, με τον βρετανικό νηογνώμονα, η ασφάλεια στον κυβερνοχώρο αποτελεί ζήτημα ζωής που απαιτεί αποτελεσματική εκπαίδευση και ισχυρή οργανωτική κουλτούρα, χωρίς την παράληψη των ειδικών παραγόντων της ναυτιλιακής βιομηχανίας, όπως οι συνδέσεις Inmarsat και η απομακρυσμένη συνδεσιμότητα που καθιστούν το ναυτιλιακό περιβάλλον μοναδικό για περιστατικά στον κυβερνοχώρο.

Η συνιστώμενη πρακτική του νορβηγικού νηογνώμονα DNV GL (2016) κάνει αναφορά στις κατευθυντήριες γραμμές των IMO και BIMCO καθώς και στο NIST Framework και εισάγει τρεις παράγοντες βελτίωσης της ασφάλειας στον κυβερνοχώρο [54]:

- αξιολόγηση
- βελτίωση
- επαλήθευση και επικύρωση

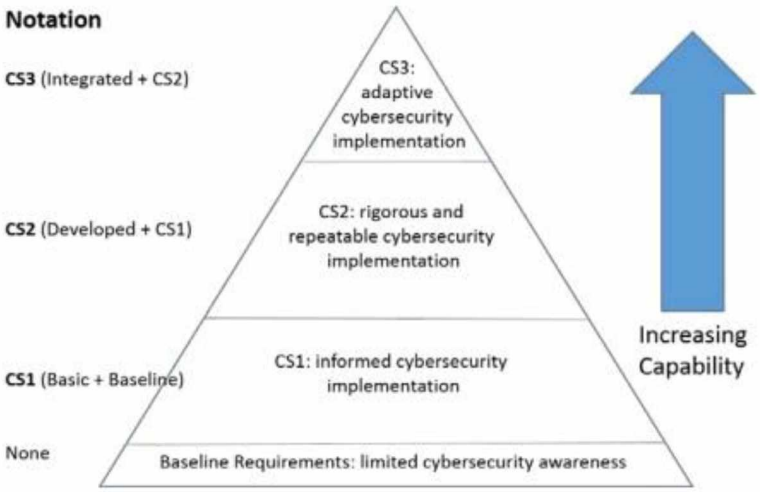
Σύμφωνα με τον DNV GL, ο συντονισμός για τη διαχείριση της ποιότητας είναι επιτακτικής ανάγκης, η σημασία του οποίου εξηγείται μέσω του παραδείγματος του κύκλου PDCA (Plan-Do-Check-Act). Η προσέγγιση του νορβηγικού νηογνώμονα διαιρεί τον παράγοντα της αξιολόγησης σε υψηλού επιπέδου, εστιασμένη και ολοκληρωμένη, καθώς και σε βάθος αξιολόγηση που μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς. Επίσης στοχεύει στην αξιολόγηση των στοιχείων των συστημάτων με βάση τον κίνδυνο ασφάλειας στον κυβερνοχώρο και τη σύγκριση της υφιστάμενης με την επιθυμητή ασφάλεια, χρησιμοποιώντας εργαλεία όπως οι μήτρες κινδύνου, η μέθοδος bow-tie και το μοντέλο CIA (Curriculum, Instruction and Assessment). Κατά την επιλογή των τεχνικών βελτίωσης μεγάλη σημασία έχει η ανάλυση του λόγου κόστους / ωφέλειας. Δίνεται επίσης έμφαση στη σημασία του ανθρώπινου παράγοντα καθώς η επιθυμητή συμπεριφορά και η ευαισθητοποίηση των ατόμων θα πρέπει να αξιολογούνται όπως ακριβώς και οποιοσδήποτε άλλος στόχος. Τέλος, ο παράγοντας της επαλήθευσης και επικύρωσης πραγματοποιείται μέσω του σωστού ελέγχου του συστήματος και των συνιστωσών του καθώς και μέσω πιστοποίησης ορθής λειτουργίας που λαμβάνεται από τρίτα μέρη.

Ο αμερικάνικος νηογνώμονας ABS (American Bureau of Shipping) ήταν ο πρώτος που ξεκίνησε πρόγραμμα διαχείρισης των κινδύνων στον κυβερνοχώρο, τη σειρά CyberSafety (2016) [55]. Οι τέσσερις βασικές περιοχές του κυβερνοχώρου που προσδιορίζονται από τον ABS είναι:

- η ασφάλεια στον κυβερνοχώρο
- η ασφάλεια των αυτόματων συστημάτων
- η διαχείριση δεδομένων και
- η διασφάλιση του λογισμικού

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Η προσφορά του προγράμματος του νηογνώμονα ABS είναι το μοντέλο ικανότητας, το οποίο αποτελείται από τρία επίπεδα (ονομασίες κλάσης CS): τη βασική, την αναπτυγμένη και την ολοκληρωμένη δυνατότητα (Εικ. 11). Οι 37 συνολικά δυνατότητες που περιέχονται σε αυτά τα επίπεδα είναι πρωταρχικά, μετρήσιμα στοιχεία που θα πρέπει να χρησιμοποιούνται κατά την εφαρμογή ενός προγράμματος ασφάλειας στον κυβερνοχώρο. Το πρόγραμμα συνδέει τη μηχανική του συστήματος με την ασφάλεια στον κυβερνοχώρο και παρέχει μια σειρά απαιτήσεων που αποτελούν ικανή και αναγκαία συνθήκη κάλυψης κάθε επιπέδου του μοντέλου ικανότητας καθώς και έναν κατάλογο προτύπων αναφοράς. Όσο μεγαλύτερος είναι ο αριθμός των δυνατοτήτων που επιτυγχάνονται, τόσο υψηλότερο είναι το επίπεδο CS του προγράμματος. Ένας οργανισμός ή μια εταιρεία που συμμορφώνεται με τις απαιτήσεις αυτές, μπορεί να λάβει πιστοποίηση με τη σήμανση (CS1, CS2 ή CS3) για την εξεταζόμενη εγκατάσταση. Η πιστοποίηση αυτή υποδεικνύει το επίπεδο ετοιμότητας του οργανισμού ή της εταιρείας, όσον αφορά τις ανησυχίες για την ασφάλεια στον κυβερνοχώρο και το επίπεδο της ωριμότητάς του σχετικά με το περιβάλλον του κυβερνοχώρου.



ΕΙΚΟΝΑ 11: Ιεραρχία επιπέδων δυνατοτήτων με σήμανση ασφάλειας στον κυβερνοχώρο [55]

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Συμπεράσματα

Η ασφάλεια στον κυβερνοχώρο είναι αναμφισβήτητα ένα από τα πλέον σημαντικά ζητήματα που αντιμετωπίζει σήμερα η παγκόσμια ναυτιλιακή βιομηχανία. Καθώς η εκθετική πορεία αύξησης του IOT και των συστημάτων που συνδέονται με το κυβερνοχώρο συνεχίζεται, το ζήτημα αυτό τείνει να επηρεάσει σε μεγαλύτερο βαθμό και τον ναυτιλιακό τομέα.

Σε γενικές γραμμές, τα συστήματα που υφίστανται σε πλοία και λιμάνια, και ιδιαίτερα στα πλοία, χρησιμοποιούν παρωχημένο λογισμικό και hardware υλικό που δεν σχεδιάστηκε με βάση την παροχή ασφάλειας στον κυβερνοχώρο. Το χαρακτηριστικό αυτό των ναυτιλιακών συστημάτων έχει ως αποτέλεσμα την, σε μεγάλο βαθμό, δημιουργία ευάλωτων συστημάτων. Οι επιτυχημένες επιθέσεις που έχουν γίνει μέχρι τώρα στον κυβερνοχώρο και έχουν στόχο τα συστήματα αυτά έχουν εκμεταλλευτεί τις αδυναμίες και τα τρωτά τους σημεία. Πιο συγκεκριμένα, υπήρξαν αρκετές επιτυχημένες επιθέσεις στον κυβερνοχώρο, που ξεκίνησαν από τα συστήματα πλοήγησης των πλοίων. Ωστόσο, καθώς τα συστήματα αυτά δεν σχεδιάστηκαν για να είναι απομονωμένα με ασφάλεια, φαίνεται εύλογο το γεγονός ότι τα παρωχημένα συστήματα προώθησης και χειρισμού φορτίων ενδέχεται επίσης να παραβιαστούν από τους επιτιθέμενους στον κυβερνοχώρο.

Στα πλαίσια της παρούσας πτυχιακής εργασίας αναφέρθηκε ένα πλήθος διαφορετικών μεθόδων τις οποίες ένας εισβολέας μπορεί να χρησιμοποιήσει για να αποκτήσει πρόσβαση στα συστήματα των πλοίων και των λιμανιών. Τέτοιες μέθοδοι είναι η απροστάτευτη σύνδεση του συστήματος στο Διαδίκτυο, η μη ενημέρωση των λογισμικών ασφαλείας των συστημάτων, η λαθραία εγκατάσταση συσκευών χακαρίσματος σε πλοίο, κτλ. Σκοπός των επιθέσεων αυτών είναι το λαθρεμπόριο, η κλοπή, η πειρατεία και η χρήση ενός πλοίου ως μέσο επίθεσης σε κάποιον άλλο στόχο.

Στην παρούσα φάση, παρουσιάζεται μια σχετική κατάσταση άγνοιας όσον αφορά τα απαραίτητα πρωτόκολλα και προγράμματα που είναι ζωτικής σημασίας για τη διασφάλιση των διαδικασιών, των ανθρώπων, αλλά και των υποδομών κρίσιμης σημασίας καθώς και των χρησιμοποιούμενων συστημάτων από πλοία και λιμάνια. Παρόλα αυτά, υπάρχουν εύκολοι τρόποι αντιμετώπισης των επιθέσεων στον κυβερνοχώρο στον ναυτιλιακό τομέα. Η αύξηση της ευαισθητοποίησης προσωπικού και πληρωμάτων σε θέματα ασφαλείας στον κυβερνοχώρο και οι καλές πρακτικές παροχής των απαραίτητων εργαλείων για την πρόληψη και τον τερματισμό κάποιων επιθέσεων στον κυβερνοχώρο, θα μπορούσαν να αποτελέσουν κάποιους από τους τρόπους αυτούς. Επίσης, η συγχώνευση των πρωτοβουλιών σε επίπεδο κρατών με τις συστάσεις και οδηγίες διεθνούς επιπέδου, είναι απαραίτητη για να εξασφαλιστεί ότι η ναυτιλιακή βιομηχανία θα συνεχίσει να εξελίσσεται παρά τις τρέχουσες και αναδυόμενες απειλές που αντιμετωπίζει στον κυβερνοχώρο. Όλοι αυτοί οι τρόποι αντιμετώπισης των κυβερνο-επιθέσεων, θα μπορούσαν να οδηγήσουν σε μεγάλο ποσοστό στην διατήρηση αυτής της ασφάλεια χωρίς να επηρεαστεί ουσιαστικά η λειτουργικότητα των ναυτιλιακών διαδικασιών στο σύνολό τους.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Η υφιστάμενη τεχνογνωσία στον κυβερνοχώρο από άλλους τομείς, όπως τα συστήματα βιομηχανικού ελέγχου και ο τομέας των μεταφορών, θα μπορούσε επίσης να εφαρμοστεί ως μέτρο άμβλυνσης των ζητημάτων ασφάλειας και στον τομέα της ναυτιλίας. Φυσικά, λόγω της ιδιαιτερότητας που παρουσιάζει ο ναυτιλιακός τομέας αλλά και της κρισιμότητάς του ακόμα και για τη διατήρηση της οικονομίας κάποιων κρατών, θα πρέπει, μακροπρόθεσμα, να δημιουργηθεί μια θεμελιώδης διαφορετική προσέγγιση για την ασφάλεια ολόκληρης της ναυτιλιακής υποδομής, πράγμα που σημαίνει ότι υπάρχει μεγάλη ανάγκη έρευνας για την ανάπτυξη προγραμμάτων ασφάλειας στον κυβερνοχώρο που να επικεντρώνονται αποκλειστικά στον ναυτιλιακό τομέα.

Η αντιμετώπιση των προκλήσεων που τίθενται από το ζήτημα της ασφάλειας στον κυβερνοχώρο θα πρέπει να αποτελέσει θέμα υψίστης προτεραιότητας, προκειμένου να διασφαλιστεί η συνεχής εκμετάλλευση των θαλάσσιων οδών από μια ασφαλή και αποτελεσματική ναυτιλίας.

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

Βιβλιογραφία

[1] Cristian González García, Vicente García-Díaz, B. Cristina Pelayo García-Bustelo & Juan Manuel Cueva Lovelle (2018, April) "Protocols and Applications for the Industrial Internet of Things", Chapter 7: A Framework for Modernizing Non-Mobile Software: A Model-Driven Engineering Approach, pp: 193, ISBN: 978-1-522-53805-9

[2] Boyes H., Isbell R. & Luck A. (2016, June) "Code of Practice. Cyber Security for Ports and Port Systems", Institution of Engineering and Technology, (IET), United Kingdom https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546160/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

[3] Fok E. (2013, July) "An Introduction to Cybersecurity Issues in Modern Transportation Systems", ITE Journal, Vol. 83, Issue 7, pp:18-21 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.447.6764&rep=rep1&type=pdf

[4] Jones K. D., Tam K. & Papadaki M. (2016, April) "Threats and Impacts in Maritime Cyber Security", Engineering & Technology Reference (IET), PEARL, University of Plymouth https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/4387/Jones_Tam_Papadaki_2016_Threats_and_%20Impacts_in_Maritime_Cyber_Security_Final.pdf?sequence=3

[5] Craigen D., Diakun-Thibault N. & Purse R. (2014, October) "Defining Cybersecurity", Technology Innovation Management Review, Vol. 4, Issue 10, pp: 13–21 https://www.researchgate.net/profile/Nadia_Diakun-Thibault/publication/267631801_Defining_Cybersecurity/links/54550d9f0cf26d5090a6fa6c.pdf

[6] Kosub T. (2015, April) "Components and challenges of integrated cyber risk management", Zeitschrift für die gesamte Versicherungswissenschaft, Vol. 104, No. 5, pp: 615-634 https://www.vwrm.rw.fau.de/files/2016/05/Cyber_Risk_2015-04-03.pdf

[7] Lee R. M. (2013, February) "The interim years of cyberspace", Air & Space Power Journal, Vol. 27, Issue 1, pp: 58-79 http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-27_Issue-1/F-Lee.pdf

[8] Hanska J. & Limnéll J. (2013, April) "The Driving Forces in Cyberspace are Changing the Reality of Security", White Paper, Stonesoft Corporation International Helsinki, Finland - Stonesoft Inc. Americas Headquarters Atlanta, USA http://stonesoft-security.co.uk/pdf/whitepapers/Driving%20Forces%20in%20Cyberspace%20whitepaper.pdf

[9] Colesniuc D. (2013) "Cyberspace and critical information infrastructures", Informatica Economica, Vol. 17, No. 4, pp: 123-132 http://www.revistaie.ase.ro/content/68/11%20-%20Colesniuc.pdf

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

[10] Babcock C. (2015, November) “Preparing for the cyber battleground of the future”, 50th Space Communications Squadron Schriever AFB United States, Air & Space Power Journal, Vol. 29, No. 6, pp: 61–73 http://www.airpower.au.af.mil/apjinternational/apj-s/2016/2016-3/2016_3_07_babcock_s_eng.pdf

[11] Lewis J. A. (2006, January) “Cybersecurity and critical infrastructure protection”, Center for Strategic and International Studies http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf

[12] Ciolan I. M. (2014, June) “Defining Cybersecurity As The Security Issue of The Twenty First Century”, A Constructivist Approach, Revista de Administratie Publica si Politici Sociale, Vol. 12, Issue 1, pp: 120-136 http://revad.uvvg.ro/files/nr12/8.Ionela_Ciolan.pdf

[13] Shackleford D. (2015, September) “Combatting cyber risks in the supply chain”, SANS Institute https://www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_273005.pdf

[14] Graham C. (2017, May) “NHS cyber-attack: Everything you need to know about ‘biggest ransomware’ offensive in history”, The Telegraph https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

[15] NIST (2014, February) “Framework for Improving Critical Infrastructure Cybersecurity”, Framework, Version 1.0 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[16] CyberEdge Group (2016) “2015 Cyberthreat Defense Report North America and Europe” https://cyber-edge.com/wp-content/uploads/2016/08/CyberEdge-2015-CDR-Report1-1.pdf

[17] Cimpean D., Meire J., Bouckaert V., Vande Casteele S., Pelle A. & Hellebooge L. (2011, November) “Analysis of Cyber Security Aspects in the Maritime Sector”, European Network and Information Security Agency (ENISA) https://www.maritimecybertraining.online/sheet/enisa

[18] IMO (2016, June) “Interim Guidelines on Maritime Cyber Risk Management”, International Maritime Organization, MSC. 1/Circ. 1526, London, United Kingdom http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf

[19] Lewis J. A. (2002, December) “Assessing the risks of cyber terrorism, cyber war and other cyber threats”, Washington, DC: Center for Strategic & International Studies (CSIS) https://www.steptoe.com/images/content/4/5/v1/4586/231a.pdf

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

[20] Prezelj I. & Žiberna A. (2013) “Consequence-, time-and interdependency-based risk assessment in the field of critical infrastructure”, Risk Management, Vol. 15, Issue 2, pp: 100-131 https://link.springer.com/article/10.1057/rm.2013.1 (Πρόσβαση την 10 ΑΠΡ 2018)

[21] Khan O. & Burnes B. (2007) “Risk and supply chain management: creating a research agenda”, The international journal of logistics management, Vol. 18, Issue 2, pp: 197-216 http://www.husdal.com/2009/05/05/risk-and-supply-chain-management-creating-a-research-agenda/ (Πρόσβαση την 10 ΑΠΡ 2018)

[22] Düerkop S. & Huth M. (2016) “Risk analysis and evaluation for critical logistical infrastructure”, Ekonomski vjesnik/Econviews-Review of Contemporary Business, Entrepreneurship and Economic Issues, Vol. 29, Issue 2, pp: 11-19 https://hrcak.srce.hr/ojs/index.php/ekonomski-vjesnik/article/view/4619/2647

[23] Afful-Dadzie A. & Allen T. T. (2014, July) “Data-driven cyber-vulnerability maintenance policies”, Journal of Quality Technology, Vol. 46, No. 3, pp: 234-250 https://www.researchgate.net/profile/Theodore_Allen2/publication/306169401_Data-driven_cyber-vulnerability_maintenance_policies/links/59bdc667458515e9cfcd537b/Data-driven-cyber-vulnerability-maintenance-policies.pdf

[24] Homeland Security (2016, March) “Consequences to Seaport Operations from Malicious Cyber Activity”, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA), Critical Infrastructure Security and Resilience Note https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf

[25] Platt V. (2012) “Still the fire-proof house? An analysis of Canada's cyber security strategy”, International journal, Vol. 67, No. 1, pp: 155-167 https://s3.amazonaws.com/academia.edu.documents/12701498/Victor_Platt_%283%29_PUBLISHED.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523448537&Signature=39zzenowOwoizdlA9ykoQYt7RpY%3D&response-content-disposition=inline%3B%20filename%3DStill_the_fire_proof_house_An_analysis_o.pdf

[26] Ahokas J., Kiiski T., Malmsten J. & Ojala L. (2017) “Cybersecurity in ports: a conceptual approach”, Proceedings of the Hamburg International Conference of Logistics (HICL), pp: 343-359 https://tubdok.tub.tuhh.de/bitstream/11420/1451/1/ahokas_kiiski_malmsten_ojala_cybersecurity_hicl_2017.pdf

[27] Boyes H. (2015, April) “Cybersecurity and cyber-resilient supply chains”, Technology Innovation Management Review, Vol. 5, Issue 4, pp: 28-34 http://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=28

[28] DiRenzo J., Goward D. A. & Roberts F. S. (2015, July) “The little-known challenge of maritime cyber security”, IEEE 6th International Conference on Information, Intelligence, Systems and Applications (IISA), pp: 1-5

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

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

[29] Boyes H. & Isbell R. (2017, September) "Ship security: cyber security code of practice", Institution of Engineering and Technology, (IET), United Kingdom https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

[30] Thomas M., Norton J., Jones A., Hopper A., Ward N., Cannon P., ... & Unwin M. (2011, March) "Global navigation space systems: reliance and vulnerabilities", The Royal Academy of Engineering, London, ISBN: 1-903496-62-4 https://www.raeng.org.uk/publications/reports/global-navigation-space-systems

[31] naftemporiki.gr (2013, Ιούλιος) "«Κούρσεμα» πλοίου μέσω παραπλάνησης GPS" http://m.naftemporiki.gr/story/681919/koursema-ploiou-meso-paraplanisis-gps (Πρόσβαση την 18 ΑΠΡ 2018)

[32] Dyryavyy Y. (2014, March) "Preparing for cyber battleships–electronic chart display and information system security", NCC Group Publication https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

[33] Balduzzi M., Wihoit K. & Pasta A. (2013) "Hey captain, where's your ship? attacking vessel tracking systems for fun and profit", Hack in the Box (HITB) Security Conference in Asia https://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf

[34] UNCTAD (2017) "Review of Maritime Transport", United Nations Conference on Trade And Development (UNCTAD) http://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf

[35] Bateman T. (2013, October) "Police warning after drug traffickers' cyber-attack", BBC News http://www.bbc.co.uk/news/world-europe-24539417 (Πρόσβαση την 18 ΑΠΡ 2018)

[36] Ott C. (2014, September) "Fraud in the Maritime Industry", Skuld http://www.safety4sea.com/wp-content/uploads/2014/09/pdf/Fraud_in_the_maritime_industry.pdf

[37] McAfee (2018, March) "Threats Report" https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2018.pdf

[38] Lipovský R. & Štefanko L. (2018) "Android Ransomware: From Android Defender to DoubleLocker", ESET, White Paper https://www.welivesecurity.com/wp-content/uploads/2018/02/Android_Ransomware_From_Android_Defender_to_Doublelocker.pdf

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

[39] Shauk Z. (2013, April) “Malware offshore: Danger lurks where the chips fail”, FuelFix https://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/ (Πρόσβαση την 19 ΑΠΡ 2018)

[40] Gallagher S. (2015, June) “Navy re-ups with Microsoft for more Windows XP support”, ArsTechnica https://arstechnica.com/information-technology/2015/06/navy-re-ups-with-microsoft-for-more-windows-xp-support/ (Πρόσβαση την 19 ΑΠΡ 2018)

[41] Kaspersky Lab (2015, May) “Maritime industry is easy meat for cyber criminals” https://www.kaspersky.com/blog/maritime-cyber-security/8796/ (Πρόσβαση την 20 ΑΠΡ 2018)

[42] Vidal J. (2010, July) “Modern cargo ships slow to the speed of the sailing clippers”, The Guardian https://www.theguardian.com/environment/2010/jul/25/slow-ships-cut-greenhouse-emissions (Πρόσβαση την 20 ΑΠΡ 2018)

[43] Martin A. (2015, July) “Rise of the swimming machines: US sub launches and recovers a drone”, The Register https://www.theregister.co.uk/2015/07/21/us_submarine_launches_and_returns_underwater_drone/ (Πρόσβαση την 20 ΑΠΡ 2018)

[44] Cannell J. (2013, February) “Tools of the Trade”, Malwarebytes https://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/ (Πρόσβαση την 20 ΑΠΡ 2018)

[45] Kiriakidis K., Severson T. & Connett B. (2016, July) “Detecting and isolating attacks of deception in networked control systems”, 2016 IEEE International Conference on Autonomic Computing (ICAC), pp: 269-274 http://web.cse.ohio-state.edu/~stewart.962/feedbackcomputing16/papers/FC16_paper_8.pdf

[46] SecNews (2015, Σεπτέμβρης) “Πολεμικό Ναυτικό ΗΠΑ: Anti-Hacking σύστημα για τα πλοία της” https://secnews.gr/96859/%CF%80%CE%BF%CE%BB%CE%B5%CE%BC%CE%B9%CE%BA%CF%8C-%CE%BD%CE%B1%CF%85%CF%84%CE%B9%CE%BA%CF%8C-%CE%B7%CF%80%CE%B1-anti-hacking-%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%80%CE%BB/ (Πρόσβαση την 27 ΑΠΡ 2018)

[47] DNV GL (2016, September) “Cyber security resilience management for ships and mobile offshore units in operation”, Recommended Practice, DNVGL-RP-0496 http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf

[48] Hansen K & Rahman A. (2013) “Cyber threat to ships – real but manageable”, ABB Group https://library.e.abb.com/public/b9d267b4767c582f85257ca1003280e9/106_Cyber_threat_to_ships_real_but_manageable.pdf

[49] Pajunen, N. (2017, January) “Overview of Maritime Cybersecurity”, Bachelor’s Thesis Marine Technology, South-Eastern Finland University of Applied Sciences

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29

https://www.theseus.fi/bitstream/handle/10024/123045/Overview%20of%20Maritime%20Cybersecurity_Final.pdf?sequence=1

[50] Peura R. (2017, November) "Maritime Cybersecurity and Improvement of Project Execution Process", Master of Science Thesis, Master's Degree Programme in Automation Technology, Tampere University of Technology https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/25339/peura.pdf?sequence=1

[51] NIST (2017, January) "Framework for Improving Critical Infrastructure Cybersecurity", Draft Version 1.1, National Institute of Standards and Technology https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

[52] BIMCO (2016, June) "The Guidelines on Cyber Security Onboard Ships", Version 2.0, Baltic and International Maritime Council http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

[53] Lloyd's Register (2016, February) "Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping – Lloyd's Register's Approach to Assurance", Guidance Note, First edition https://www.arbitrage-maritime.org/fr/Gazette/G43complement/lloyds.pdf

[54] DVN GL (2016, September) "Cyber security resilience management for ships and mobile offshore units in operation", Reccomended Practise, DNVGL-RP-0496 http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf

[55] ABS (2016, September) "Cybersecurity – Guidance Notes for the Marine and Offshore Industries", American Bureau of Shipping, ABS CyberSafetyTM VOLUME 2 https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety_V2_Cybersecurity_Guide_e.pdf

Institutional Repository - Library & Information Centre - University of Thessaly
19/05/2024 00:26:41 EEST - 13.59.234.29