ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΝΑΥΠΗΓΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική εργασία

Τίτλος στα ελληνικά

Κυβερνοασφάλεια στη ναυτιλία- εφαρμογή σχετικών κανονισμών σε πλοίο

Title in English

Cyber security in shipping- application of relevant regulations on vessel

Συγγραφέας:

Γεδεών Σαββίνα- Εφραιμία

Α.Μ.: 15011

Επιβλέπων: Δρ. Σέρρης Μιχαήλ

Αιγάλεω, 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΝΑΥΠΗΓΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική εργασία

Τίτλος

Κυβερνοασφάλεια στη ναυτιλία- εφαρμογή σχετικών κανονισμών σε πλοίο

Συγγραφέας

Γεδεών Σαββίνα- Εφραιμία (Α.Μ.: 15011)

Επιβλέπων

Σέρρης Μιχαήλ,

Λέκτορας ΠΑ.Δ.Α.

Ημερομηνία εξέτασης

28/02/2022

Εξεταστική Επιτροπή

SERRIS MICHAIL Digitally signed by SERRIS MICHAIL Date: 2022.03.08 06:23:32 +02'00'

Σέρρης Μιχαήλ,

Λέκτορας ΠΑ.Δ.Α.

Nikolaos Sgouros Digitally signed by Nikolaos Sgouros Date: 2022.03.08 00:23:18 +02'00'

Σγουρός Νικόλαος,

Ακαδημαϊκός υπότροφος ΠΑ.Δ.Α.

Digitally signed by Dimitrios Nikolaos Pagonis Date: 2022.03.04 23:36:16 +02'00'

Δημήτριος Παγώνης,

Αναπληρωτής Καθηγητής ΠΑ.Δ.Α.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Γεδεών Σαββίνα-Εφραιμία του Εμμανουήλ , με αριθμό μητρώου 51115011 φοιτήτρια του Πανεπιστημίου Δυτικής Αττικής της Σχολής μηχανικών του Τμήματος ναυπηγών μηχανικών , δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Η Δηλούσα

Γεδεών Σαββίνα

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, Δρ. Μιχαήλ Σέρρη λέκτορα ΠΑΔΑ, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντας το συγκεκριμένο θέμα, την καθοδήγησή του, τις υποδείξεις του, την συμπαράσταση του, τη συνεχή υποστήριξή του και το ενδιαφέρον που έδειξε από ην αρχή ως το τέλος.

Επίσης ευχαριστώ τους καθηγητές Δρ. Νικόλαο Σγουρό και τον Δρ. Δημήτριο Παγώνη για την πολύτιμη συμβολή τους στην ολοκλήρωση αυτής της εργασίας, ως μέλη της τριμελούς επιτροπής.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου για όλη τη στήριξη, τη συμπαράσταση και την κατανόηση τους καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Στη παρούσα διπλωματική εργασία γίνεται αναλυτική μελέτη για τα ζητήματα κυβερνοασφάλειας στα πλοία. Στο πρώτο κεφάλαιο παρουσιάζονται οι κίνδυνοι και οι απειλές που προκύπτουν από ενδεχόμενες κυβερνοεπιθέσεις, ενώ παρουσιάζονται οι τύποι κυβερνοεπιθέσεων και τα στάδια μιας τέτοιας επίθεσης. Στο δεύτερο κεφάλαιο γίνεται αναλυτική περιγραφή των τρωτών σημείων του πλοίου. Στο τρίτο κεφάλαιο γίνεται αναφορά στο διεθνές νομοθετικό πλαίσιο για την προστασία από κυβερνοεπιθέσεις. Στο τέταρτο κεφάλαιο γίνεται αναφορά στα μέτρα προστασίας ενάντια σε μια κυβερνοεπίθεση. Στο πέμπτο κεφάλαιο παρουσιάζεται η διαδικασία αντιμετώπισης περιστατικών κυβερνοεπίθεσης. Στο έκτο κεφάλαιο παρουσιάζονται τα συμπεράσματα και οι μελλοντικές προτάσεις. Στο παράρτημα της εργασίας παρουσιάζεται η διαχείριση στρατηγικής άμυνας.

Λέξεις κλειδιά: *<<κυβερνοεπίθεση>>, <<κυβερνοασφάλεια>>, <<συστήματα πληροφορικής>>, <<συστήματα επιχειρησιακής τεχνολογίας>>, <<τρωτά σημεία>>, <<ηλεκτρονικό ψάρεμα>>, <<ιοί>>*

Abstract

In this diploma thesis the issues about cybersecurity on ships are carried out. In the first chapter the dangers and threats that arise from a possible cyber-attack are represented, while presenting the types of cyber-attacks and the stages of such an attack. The second chapter provides a detailed description of the ship's vulnerabilities. The third chapter refers to the international legal framework for protection against cyber-attacks. The fourth chapter refers to the protection measures against a cyber-attack. The fifth chapter presents the process of dealing with cyber-attack incidents. The sixth chapter presents the conclusions and future proposals. The appendix of the paper presents the management of strategic defense.

Key words: <<cyberattack>>, <<cybersecurity>>, <<information technology systems>>, <<operational technology systems>>, <<vulnerabilities>>, <<cyber phising>>, <<viruses>>

Πίνακας περιεχομένων

Λίστα εικόνων

Κεφάλαιο 1: Κίνδυνοι και απειλές

1.1 Εισαγωγή

Με την εξέλιξη της τεχνολογίας, ειδικότερα στους τομείς της πληροφορικής και των επικοινωνιών, τα συστήματα λογισμικού των πλοίων και τα συστήματα ελέγχου πλέον ενσωματώνονται παρέχοντας την δυνατότητα παρέμβασης σε αυτά από συστήματα που δεν βρίσκονται στο πλοίο. Τα προηγούμενα χρόνια τα συστήματα πληροφορικής / *Information Technology Systems (IT)* και τα συστήματα επιχειρησιακής τεχνολογίας / *Operational Technology Systems (OT)* λειτουργούσαν ανεξάρτητα το ένα από το άλλο και δεν υπήρχε η δυνατότητα παρέμβασης από σημείο εκτός πλοίου. Η δεδομένη εξέλιξη της τεχνολογίας αναπόφευκτα δημιούργησε νέες απειλές για την ομαλή λειτουργία του πλοίου που κατ' επέκταση είναι απαραίτητη η δημιουργία και ανάπτυξη συστημάτων κυβερνοασφάλειας. Για την ασφαλή λειτουργία του πλοίου, την ασφάλεια του πληρώματος και των επιβατών αλλά και την προστασία του φορτίου, έχουν αναπτυχθεί αρκετά συστήματα που κατά την λειτουργία τους η σύνδεση στο διαδίκτυο είναι απαραίτητη. Αυτά τα συστήματα οφείλουν να ικανοποιούν διεθνή πρότυπα προδιαγραφών λειτουργίας και να ακολουθούν κανονισμούς, όμως η διασύνδεση αυτών των συστημάτων μπορεί παρόλα αυτά να δημιουργήσει επιπρόσθετους κινδύνους ασφαλείας. Στην παρούσα εργασία θα μελετήσουμε τους κανονισμούς ασφαλείας, τα συστήματα κυβερνοασφάλειας, καθώς και τις πιθανές απειλές και κινδύνους.

1.2 Τμήμα διαχείρισης κινδύνου

Ο ορισμός του κινδύνου ή του ρίσκου αφορά την ανθρώπινη δραστηριότητα η οποία μπορεί να επιφέρει διάφορες επιπτώσεις στο μέλλον *(Aven et al, 2015)*[1]. Οι επιπτώσεις είναι αβέβαιες και το αποτέλεσμα τους μπορεί να είναι είτε θετικό είτε αρνητικό. Θεωρώντας μια δραστηριότητα ή μια ανθρώπινη πράξη ως ρίσκο πρέπει να ληφθεί υπόψιν το ίδιο το γεγονός και οι πιθανές επιπτώσεις, καθώς επίσης, η αβεβαιότητα του γεγονότος και οι πληροφορίες που ήδη κατέχουμε όσον αφορά αυτό το γεγονός.

[1] *Aven, T. & Renn, O. & Rosa, E. (2015), 'On the ontological status of the concept of risk', Safety Science 49*

Οι πληροφορίες πάντα περιέχουν ένα ποσοστό αβεβαιότητας και γι' αυτόν το λόγο είναι μπορεί να είναι λανθασμένες, οπότε σε κάθε απόφαση δεν γίνεται ο ανθρώπινος παράγοντας να είναι 100% βέβαιος για το αποτέλεσμα. Στην περίπτωση που το ρίσκο ή ο κίνδυνος είναι υψηλά, οι επιπτώσεις των αποφάσεων του ανθρώπινου παράγοντα δύναται να μην είναι προβλέψιμες, γεγονός που έχει αντίκτυπο στην διαδικασία αξιολόγησης του κινδύνου.

Η διαχείριση κινδύνου στον κυβερνοχώρο πρέπει να αποτελεί αναπόσπαστο μέρος της ασφάλειας και αποτελεσματικότητας μιας εταιρείας. Η σωστή διαχείριση κινδύνου ευνοεί την ασφαλή και αποτελεσματική λειτουργία του πλοίου και εφαρμόζεται σε διάφορα επίπεδα του συμπεριλαμβανομένου του ανώτερου διευθυντικού στελέχους στην ξηρά και του προσωπικού. Η διαχείριση κινδύνου στον κυβερνοχώρο πρέπει:

1. Να ξεχωρίζει τους ρόλους και τις αρμοδιότητες του αρμόδιου προσωπικού και της διεύθυνσης διαχείρισης στην ξηρά και εν πλω.
2. Να προσδιορίζει τα συστήματα, τα περιουσιακά στοιχεία, τα δεδομένα και τις δυνατότητες τις εταιρείας, όπου εάν κάποιο από αυτά διαταραχθεί θα προκληθεί κίνδυνος για τις λειτουργίες του πλοίου καθώς και για την ασφάλεια του.
3. Να εκτελεί τα απαραίτητα τεχνικά και διαδικαστικά μέτρα για την έγκαιρη αντιμετώπιση ενός συμβάντος στον κυβερνοχώρο, καθώς επίσης να ανιχνεύει τις πιθανές δραστηριότητες που ενδέχεται να είναι επικίνδυνες για την ασφάλεια του πλοίου και ταυτόχρονα να διασφαλίζει την ομαλή συνέχεια των εργασιών.
4. Να φροντίζει για την τακτική εφαρμογή του σχεδίου έκτακτης ανάγκης για πιθανούς κινδύνους.

Ορισμένες πτυχές της διαχείρισης κινδύνου στον κυβερνοχώρο μπορεί να περιλαμβάνουν εμπορικά ευαίσθητες ή εμπιστευτικές πληροφορίες, για παράδειγμα την εκτίμηση κινδύνου στον κυβερνοχώρο και το σχετικό υλικό και λογισμικό που περιλαμβάνει πληροφορίες για τα αποθέματα καθώς και χάρτες δικτύου. Οι εταιρείες συνεπώς πρέπει να εξετάσουν το ενδεχόμενο προστασίας αυτών των πληροφοριών με κατάλληλο και στο μέτρο του δυνατού, τρόπο ώστε να μην περιλαμβάνονται ευαίσθητες πληροφορίες στα συστήματα ασφαλείας τους (*SMS)*[2].

[2] *SMS=Safety Management System*

Η διαχείριση κινδύνου στις ναυτιλιακές εταιρίες πρέπει να αναλαμβάνεται από ανώτερα στελέχη της εταιρείας και όχι για παράδειγμα από τον υπεύθυνο ασφαλείας τους πλοίου ή τον διευθυντή του τμήματος *IT*. Οι λόγοι είναι οι ακόλουθοι:

- Υπάρχουν περιπτώσεις όπου ο κίνδυνος και οι επιπτώσεις μιας κυβερνοεπίθεσης να είναι τόσο μεγάλες που να είναι ικανές να επηρεάσουν την φήμη της εταιρείας, ή να προκαλέσουν περιβαλλοντική καταστροφή. Γεγονός που καταδεικνύει πως τα ζητήματα κυβερνοασφάλειας δεν αποτελούν απλώς ζητήματα και προκλήσεις ασφαλείας, άλλα επιχειρηματικές προκλήσεις που απαιτούν την συμμετοχή της ηγεσίας της εταιρείας.
- Οι πρωτοβουλίες για την ενίσχυση της ασφάλειας στον κυβερνοχώρο ενδέχεται να επηρεάσουν τις τυπικές επιχειρηματικές διαδικασίες και λειτουργίες καθιστώντας τις πιο χρονοβόρες και δαπανηρές. Ως εκ τούτου, είναι αναγκαία η συμμετοχή ανώτερων στελεχών της διαχείρισης, για την αξιολόγηση και την κατανομή των απαραίτητων πόρων, για τον προσδιορισμό της διαχείρισης του κινδύνου.
- Αρκετές από τις πρωτοβουλίες που αναλαμβάνει η διαχείριση κινδύνου μπορεί να αλλάξουν τον τρόπο που η εταιρεία αλληλοεπιδρά με τους πελάτες, τους προμηθευτές, τα συνδικάτα των εργαζομένων καθώς και τις εκάστοτε κρατικές αρχές. Το αποτέλεσμα είναι η δημιουργία νέων απαιτήσεων στην συνεργασία μεταξύ των μερών.

Το τμήμα της διαχείρισης κινδύνου πρέπει να είναι σε θέση να προβλέψει ποια περιουσιακά στοιχεία της εταιρείας είναι πιο πιθανό να δεχθούν κάποια κυβερνοεπίθεση. Επίσης απαραίτητη είναι η πρόβλεψη για τις πιθανές επιπτώσεις μιας κυβερνοεπίθεσης στην εταιρεία, στους πελάτες, στους συνεργάτες και κατ' επέκταση στους μετόχους της εταιρείας. Το τμήμα διαχείρισης κινδύνου οφείλει να καθορίσει ποιος έχει την τελική ευθύνη για την διαχείριση κυβερνοεπίθεσης. Το τμήμα διαχείρισης κινδύνου οφείλει να παρακολουθεί αν τα συστήματα *OT* καθώς και το περιβάλλον εργασίας τους είναι προστατευμένα από μη εξουσιοδοτημένη πρόσβαση. Η απομακρυσμένη πρόσβαση στα συστήματα *OT* πρέπει να παρακολουθείται και να ελέγχεται, ομοίως για τα συστήματα *IT*.

Με την εξέλιξη της τεχνολογίας κάθε εταιρία χρησιμοποιεί όλο και περισσότερα ψηφιακά εργαλεία για την λειτουργία της, γεγονός που αυξάνει τον κίνδυνο για κυβερνοεπίθεση. Οι κίνδυνοι διαρκώς αλλάζουν, οπότε η ομάδα διαχείρισης κινδύνου οφείλει να είναι πάντα ενήμερη για τους πιθανούς κινδύνους. Ένα μεγάλο και άγνωστο γεγονός του οποίου οι συνέπειες μπορεί να είναι ιδιαιτέρως άσχημες ή μη ευνοϊκές για τους ανθρώπους ή το περιβάλλον χαρακτηρίζεται ως 'μαύρος κύκνος'. *(Aven et al, 2014)*

Τα χαρακτηριστικά του ‘μαύρου κύκνου’ είναι τρία:

1. Είναι ένα γεγονός που κινείται εκτός των προσδοκιών καθώς κανένα στοιχείο του παρελθόντος δεν μπορεί να δώσει την πληροφορία πως θα ήταν πιθανή η εμφάνιση του.

2. Έχει σημαντικές επιπτώσεις στον άνθρωπο και το περιβάλλον.

3. Μετά το πρώτο καταγεγραμμένο συμβάν σχεδόν πάντα υπάρχει κάποια εξήγηση που αδυνατεί να προσεγγίσει το τυχαίο του συμβάντος.

Στην περίπτωση μιας απρόβλεπτης κυβερνοεπίθεσης εναντίον μιας ναυτιλιακής εταιρείας τα όρια αντοχής και ανεκτικότητας της εταιρείας μεταβάλλονται με την πάροδο του χρόνου. Το τμήμα διαχείρισης του κινδύνου οφείλει στις μελέτες του να προβλέπει όσο το δυνατόν μεγαλύτερο εύρος από πιθανούς κινδύνους ώστε να μειώνεται το ρίσκο. Η περίπτωση ενός ‘μαύρου κύκνου’ είναι απρόβλεπτη αλλά οφείλει το τμήμα να έχει σχέδιο άμεσης αντιμετώπισης των επιπτώσεων μιας τέτοιας κυβερνοεπίθεσης

1.2.1 Αρμοδιότητες τμήματος διαχείρισης κινδύνου

Απαραίτητο στοιχείο για την αποτελεσματικότητα της διαχείρισης κινδύνου είναι η σαφή και διακριτή κατανομή των αρμοδιοτήτων και των καθηκόντων του προσωπικού της εταιρείας καθώς και τρίτων που αναλαμβάνουν συγκεκριμένες εργασίες. Οι ευθύνες και τα καθήκοντα για τις εκάστοτε αρμοδιότητες πρέπει να αντιστοιχούν στις περιγραφές και τον ρόλο κάθε εργασίας όπως ακριβώς περιγράφονται στα συστήματα *SMS*. Ο προγραμματισμός και η εκτέλεση της διαχείρισης κινδύνου στον κυβερνοχώρο περιλαμβάνει όλη την ναυτιλιακή εταιρεία, οπότε για την βέλτιστη λειτουργία είναι απαραίτητο να γίνεται χαρτογράφηση των εργασιών, ώστε να διευκρινιστεί ποιο άτομο είναι υπεύθυνο για κάθε εργασία.

Στον πίνακα 1 που ακολουθεί παρουσιάζεται ένα παράδειγμα χαρτογράφησης αρμοδιοτήτων.

Πίνακας 1: παράδειγμα χαρτογράφησης αρμοδιοτήτων (Πηγή: The guidelines on cyber security onboard ships)

Εργασία/ ρόλος	**Πολιτική ασφαλείας**	**Αξιολόγηση διαχείρισης κινδύνου στα συστήματα ΟΤ του πλοίου**	**Αξιολόγηση διαχείρισης κινδύνου στα συστήματα ΙΤ του πλοίου**	**Διαχείριση της υποδομής του συστήματος ΙΤ του πλοίου**	**Εκπαίδευση του πληρώματος σε θέματα κυβερνοασφάλειας**
Διευθύνων σύμβουλος	Υπεύθυνος				
Εταιρικός διευθυντής ΙΤ	Υποστήριξη		Υποστήριξη		
Διευθυντής ΙΤ εν πλω	Υποστήριξη	Υπεύθυνος	Υπεύθυνος	Υπεύθυνος	
Διαχειριστής ασφαλείας	Υποστήριξη	Υποστήριξη	Υποστήριξη	Υποστήριξη	Υποστήριξη
Διαχειριστής προμηθειών	Υποστήριξη			Υποστήριξη	
Διαχειριστής στόλου		Υποστήριξη	Υποστήριξη	Υποστήριξη	Υποστήριξη
Διαχειριστής εκπαίδευσης			Υποστήριξη		Υποστήριξη
Διευθυντής του ναυτικού τμήματος ανθρώπινου δυναμικού			Υποστήριξη		Υπεύθυνος

1.3 Τύποι κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις δύναται να πάρουν διάφορες μορφές ανάλογα με το μέγεθος της ζημιάς που προκαλούν, διακρίνονται σε δύο κατηγορίες: α) στοχευμένες επιθέσεις β) μη στοχευμένες επιθέσεις

Στις στοχευμένες επιθέσεις ο στόχος της επίθεσης είναι το πλοίο ή η εταιρεία ενώ στις μη στοχευμένες εκτός από το πλοίο και την εταιρεία τα πιθανά θύματα μπορεί να είναι και άλλα.

Οι στοχευμένες επιθέσεις χρησιμοποιούν τα ακόλουθα μέσα/ εργαλεία για να επιτύχουν τον στόχο τους:

- **εξαντλητικές δοκιμές:** είναι το είδος επίθεσης όπου οι εγκληματίες χρησιμοποιούν αρκετούς κωδικούς με την ελπίδα να μαντέψουν τον σωστό.
- **Άρνηση εισόδου:** είναι η επίθεση με κακόβουλο λογισμικό που έχει εγκατασταθεί στο δίκτυο υπολογιστών της εταιρείας ή του πλοίου το οποίο αυτόματα γίνεται μέρος ενός δικτύου *botnet*. Η λέξη *botnet* προέρχεται από τις λέξεις *robot* και *network*. Ουσιαστικά με τη χρήση του δικτύου botnet τα άτομα που ελέγχουν το κακόβουλο λογισμικό υπερφορτώνουν το δίκτυο της εταιρείας και του πλοίου με αποτέλεσμα την άρνηση της εισόδου σε αυτό διακόπτοντας με αυτόν τον τρόπο τη λειτουργίας τους. Για την αποφυγή τέτοιου είδους επίθεσης είναι απαραίτητη η χρήση ενημερωμένου λογισμικού *firewall*.
- **Στοχευμένο ηλεκτρονικό ψάρεμα (*spear phishing*):** είναι η εξέλιξη και αρκετά πιο επικίνδυνη μέθοδος επίθεσης του 'ηλεκτρονικού ψαρέματος', ο εισβολέας συλλέγει τις πληροφορίες που θέλει σχετικά με το θύμα χρησιμοποιώντας μεθόδους κοινωνικής μηχανικής. Η πιο συνηθισμένη μέθοδος προσέγγισης είναι η αποστολή ηλεκτρονικού μηνύματος όπου ο εισβολέας υποδύεται μια αξιόπιστη οντότητα και περιέχει ηλεκτρονικό σύνδεσμο σε κακόβουλο λογισμικό.
- **Πλήρωση πιστοποιητικών (*credential stuffing*):** είναι η επίθεση όπου ο επιτιθέμενος χρησιμοποιεί πιστοποιητικά που έχει παραβιάσει στο παρελθόν ή συγκεκριμένους κοινούς κωδικούς πρόσβασης με σκοπό την απόπειρα μη εξουσιοδοτημένης πρόσβασης σε συστήματα του πλοίου.

Στην περίπτωση των μη στοχευμένων επιθέσεων ο επιτιθέμενος συνήθως χρησιμοποιεί εργαλεία και τεχνικές που παρέχουν πληροφορίες για τους πιθανούς στόχους ανακαλύπτοντας τα ευάλωτα σημεία του πλοίου. Παραδείγματα εργαλείων και επιθέσεων που χρησιμοποιούν είναι τα ακόλουθα:

- **Χρήση κακόβουλου λογισμικού *(malware)*:** ο όρος *malware* χρησιμοποιείται για τον ορισμό του κακόβουλου λογισμικού το οποίο έχει κατασκευαστεί με σκοπό την πρόσβαση ή την πρόκληση βλάβης σε υπολογιστικά συστήματα χωρίς την γνώση και άδεια του ιδιοκτήτη. Υπάρχουν διάφοροι τύποι κακόβουλου λογισμικού όπως:

1. Δούρειοι ίπποι *(Trojans)*: ο συγκεκριμένος τύπος κακόβουλου λογισμικού μεταμφιέζονται σε ακίνδυνες εφαρμογές με αποτέλεσμα την παραπλάνηση/ εξαπάτηση του χρήστη ο

οποίος τα εγκαθιστά στο υπολογιστικό του σύστημα. Μόλις τεθούν σε λειτουργία ο επιτιθέμενος αποκτά την δυνατότητα πρόσβασης στο υπολογιστικό σύστημα του πλοίου ή της εταιρείας στη στεριά, συνήθως χρησιμοποιούνται για την παρακολούθηση δραστηριοτήτων της εταιρείας, υποκλοπής δεδομένων ή ακόμα και καταστροφή κάποιου συστήματος.

2. Ιοί *(viruses and worms)*: οι συγκεκριμένοι τύποι κακόβολου λογισμικού έχουν σχεδιαστεί με σκοπό να μολύνουν τα υπολογιστικά συστήματα της εταιρείας και να διασκορπιστούν σε όσο το δυνατό μεγαλύτερο μέρος των υπολογιστικών συστημάτων του πλοίου ή της εταιρείας. Η διαφορά μεταξύ *virus* και *worm* είναι πως στην περίπτωση του virus απαιτείται πράξη και εκτέλεση του χρήστη ώστε να ξεκινήσει ο διασκορπισμός του κακόβουλου λογισμικού ενώ στην περίπτωση του worm δεν είναι απαραίτητη κάποιου είδους πράξη από τον χρήστη. Αμφότερες οι περιπτώσεις φέρουν τμήμα κακόβουλο κώδικα με σκοπό να προκαλέσουν ζημιά στα συστήματα του πλοίου.

3. Λογισμικά απαίτησης λύτρων *(ransomware)*: ο συγκεκριμένος τύπος κακόβουλου λογισμικού είναι από τα πιο διαδεδομένα συστήματα στις περιπτώσεις που ο επιτιθέμενος απαιτεί λύτρα από το θύμα. Όταν εγκατασταθεί στον υπολογιστή του θύματος το συγκεκριμένο κακόβουλο λογισμικό κρυπτογραφεί τα αρχεία, έπειτα ο επιτιθέμενος επικοινωνεί με το θύμα με σκοπό την καταβολή λύτρων για να επιστρέψει τα αρχεία.

4. Κατασκοπευτικά λογισμικά *(spyware)*: ο συγκεκριμένος τύπος κακόβουλου λογισμικού ο οποίος μετά την εγκατάσταση του στα υπολογιστικά συστήματα του θύματος μεταδίδει προσωπικές πληροφορίες και λεπτομερή στοιχεία από την περιήγηση του στο διαδίκτυο. Παρέχει την δυνατότητα στον επιτιθέμενο παρακολούθηση και υποκλοπής όλων των μορφών επικοινωνίας του θύματος.

- **Νερόλακκος *(Watering hole)*:** ονομάζονται οι επιθέσεις που σκοπό έχουν την υποκλοπή δεδομένων, παραβιάζοντας την ασφάλεια του υπολογιστή. Ο επιτιθέμενος γνωρίζει ή ανακαλύπτει ιστοσελίδες τις οποίες επισκέπτεται ο χρήστης και στη συνέχεια εγκαθιστά κακόβουλο λογισμικό σε αυτές. Δεν είναι συχνές επιθέσεις, ειδικά στον τομέα της ναυτιλίας γι’ αυτόν το λόγο δεν ανιχνεύονται εύκολα.

- **Κοινωνική μηχανική *(Social engineering)*:** ο συγκεκριμένος τύπος επίθεσης αναφέρεται στις περιπτώσεις όπου ο επιτιθέμενος υποδυόμενος κάποιον αξιόπιστο ρόλο χειραγωγεί τον χρήστη ώστε να αποκτήσει πρόσβαση σε προσωπικά δεδομένα. Ένα σύνηθες κόλπο είναι η αποστολή μαζικού ηλεκτρονικού μηνύματος αναφέροντας πχ πως αύριο θα υπάρχει πρόβλημα στο δίκτυο της εταιρείας, για οποιαδήποτε διευκρίνηση ή βοήθεια επικοινωνήστε με αυτό το νούμερο, σε τέτοιες περιπτώσεις ο επιτιθέμενος κερδίζει την εμπιστοσύνη του χρήστη.
- **Ψάρεμα *(Phising)*:** ο επιτιθέμενος αποστέλλει μαζικά e-mails στα οποία είτε περιέχεται επιβλαβής σύνδεσμος είτε κάποιο αρχείο. Σε αμφότερες τις περιπτώσεις αν κάνει το λάθος ο χρήστης και είτε κατευθυνθεί στον σύνδεσμο είτε εγκαταστήσει το κακόβουλο λογισμικό, ο επιτιθέμενος θα αποκτήσει πρόσβαση στα δεδομένα του χρήστη.

1.4 Στάδια κυβερνοεπίθεσης

Το χρονικό διάστημα για την προετοιμασία μιας επίθεσης στον κυβερνοχώρο μπορεί να καθοριστεί από τα κίνητρα και τους στόχους του επιτιθέμενου καθώς και την ασφάλεια και ανθεκτικότητα των τεχνικών και διαδικαστικών ελέγχων κινδύνου στον κυβερνοχώρο που υλοποιούνται από την εταιρεία. Στους ελέγχους συμπεριλαμβάνονται και εκείνοι που γίνονται στα πλοία της και όχι μόνο στα υπολογιστικά συστήματα της εταιρείας στην στεριά. Στην περίπτωση των στοχευμένων κυβερνοεπιθέσεων, τα στάδια εξέλιξης ενός συμβάντος είναι τα ακόλουθα:

1. **Παρακολούθηση και αναγνώριση**

Ο επιτιθέμενος συλλέγει πληροφορίες και δεδομένα για αρκετό καιρό χρησιμοποιώντας τα ανοικτά/ ελεύθερα κοινωνικά δίκτυα μελών του πληρώματος και της εταιρείας. Στο πλαίσιο της προετοιμασίας για την κυβερνοεπίθεση παρακολουθούνται συζητήσεις στο διαδίκτυο όπως σε forums, καταγράφονται πληροφορίες για τεχνικά ζητήματα αλλά και για διαδικασίες ρουτίνας του πλοίου. Επίσης οι επιτιθέμενοι αναζητούν έγγραφα και δεδομένα του πλοίου που περιγράφουν είτε σχέδια του πλοίου είτε πληροφορίες για το φορτίο που μεταφέρουν και στη συνέχεια τα μελετούν με σκοπό να ανακαλύψουν τα ευάλωτα σημεία του πλοίου ή της εταιρείας.

2. **Μεταφορά/διανομή**

Μετά την ολοκλήρωση της παρακολούθησης ο επιτιθέμενος αναζητεί τρόπους να εισχωρήσει στα συστήματα του πλοίου και της εταιρείας, αφού έχει εντοπίσει τα τρωτά σημεία στο δίκτυο είτε του πλοίου είτε της εταιρείας. Οι πιθανοί τρόποι επίθεσης είναι οι ακόλουθοι:

- Μέσω των συστημάτων της εταιρείας που είναι συνδεδεμένα στο διαδίκτυο, όπως για παράδειγμα σύστημα παρακολούθησης φορτίου
- Αποστολή ηλεκτρονικού μηνύματος σε υπαλλήλους της εταιρείας με κακόβουλο λογισμικό
- Τοποθέτηση προγράμματος υποκλοπής δεδομένων κατά τη διαδικασία αναβάθμισης συστημάτων του πλοίου
- Δημιουργία ψευδών/ παραπλανητικών ιστοσελίδων που σκοπό έχουν την υποκλοπή ευαίσθητων δεδομένων όπως κωδικούς.

3. Παραβίαση

Το εύρος του ρήγματος που μπορεί να προκαλέσει ο επιτιθέμενος στα συστήματα καθώς και της σημαντικότητας του ποικίλλει και εξαρτάται από το είδος του τρωτού σημείου που ανακάλυψε ο επιτιθέμενος αλλά και από τον τρόπο επίθεσης που επέλεξε. Στην πλειοψηφία των κυβερνοεπιθέσεων η παραβίαση δεν είναι άμεσα εμφανής διότι δεν προβαίνει σε προφανείς αλλαγές στην κατάσταση του συστήματος ή δεν προκαλεί αλλαγή στην ομαλή λειτουργία του πλοίου. Ανάλογα με την σημασία της παραβίασης ο επιτιθέμενος δύναται να έχει αποκτήσει την δυνατότητα:

- Να προβεί σε αλλαγές που επηρεάζουν την ομαλή λειτουργία συστημάτων του πλοίου, όπως να διακόψουν ή να αλλάξουν πληροφορίες σχετικά με την πλοήγηση του πλοίου
- Να αποκτήσει πρόσβαση σε δεδομένα της εταιρείας και να υποκλέψει για παράδειγμα πληροφορίες για το φορτίο του πλοίου ή πληροφορίες για τους επιβάτες του πλοίου
- Να αποκτήσει τον έλεγχο των συστημάτων πρόωσης του πλοίου, γεγονός που θα του δώσει τον πλήρη έλεγχο του πλοίου.

4. Pivot

Ο όρος *'pivot'* αναφέρεται στην διαδικασία όπου ο επιτιθέμενος αφού έχει αποκτήσει πρόσβαση σε κάποιο από τα συστήματα του πλοίου, χρησιμοποιεί το παραβιασμένο σύστημα

ή μέρος αυτού με σκοπό την παραβίαση άλλων συστημάτων του πλοίου. Αρχικά παραβιάζεται το πιο ευάλωτο σύστημα του πλοίου, αυτό με το χαμηλότερο επίπεδο ασφαλείας. Τις περισσότερες φορές ο επιτιθέμενος χρησιμοποιεί εργαλεία τα οποία θα τον βοηθήσουν στο επόμενο στάδιο της επίθεσης. Επίσης χρησιμοποιείται για την χαρτογράφηση του συστήματος του πλοίου. Σε αυτό το στάδιο της επίθεσης ο επιτιθέμενος αποσκοπεί στην εγκατάσταση κατάλληλων εργαλείων που δεν θα είναι εύκολα ανιχνεύσιμα και θα του δώσουν τη δυνατότητα να επιτεθεί στο μέλλον.

5. Αποτέλεσμα

Το αποτέλεσμα της δράσης του επιτιθέμενου καθορίζεται τόσο από τα κίνητρά του όσο και από τους στόχους του, παραδείγματος χάριν μπορεί να θέλει να αποκτήσει πρόσβαση σε ευαίσθητα εμπορικά δεδομένα που είναι εξαιρετικά εμπιστευτικά ή να χρησιμοποιήσει/ ξεγελάσει το πλήρωμα καθώς και να αλλάξει ή να υποκλέψει δεδομένα σχετικά με το φορτίο. Είναι πολύ σημαντικό να εκπαιδεύονται και να επιμορφώνονται τα μέλη του πληρώματος του πλοίου ώστε να είναι σε θέση να γνωρίζουν το είδος και το εύρος των κινδύνων που υπάρχουν και επιπλέον πώς να αντιδράσουν εάν συμβεί κάτι προκειμένου να μετριαστούν οι επερχόμενες συνέπειες.

1.5 Παραδείγματα κυβερνοεπιθέσεων

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις με χρήση κακόβουλου λογισμικού έχουν ενταθεί, από αυτές τις επιθέσεις η πλειοψηφία είναι επιθέσεις στα συστήματα των εταιρειών στη στεριά που συνδέονται με το πλοίο. Ειδικότερα οι περισσότερες επιθέσεις στοχεύουν εφαρμογές διαχείρισης των εμπορευματοκιβωτίων.

Η περίπτωση του λιμανιού της Αμβέρσας

Στο λιμάνι της Αμβέρσας μόνο το 5% των εμπορευματοκιβωτίων επιθεωρείται με φυσικά μέσα, αυτό είχε ως αποτέλεσμα να αποτελέσει στόχο επίθεσης από εμπόρους ναρκωτικών. Η κυβερνοεπίθεση είχε πολλαπλά στάδια εφαρμογής, η συνολική διάρκεια της επίθεσης ήταν περίπου 2 έτη. Το συγκεκριμένο παράδειγμα κυβερνοεπίθεσης αποκαλύπτει τους κινδύνους στους οποίους είναι ευάλωτα τα συστήματα *IT*, σύμφωνα με τους ειδικούς στον τομέα της κυβερνοασφάλειας. Η επίθεση ξεκίνησε στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου *(e-mail)* με συνδέσμους κακόβουλων λογισμικών, έπειτα από λάθος του προσωπικού του λιμένα η ομάδα των εγκληματιών απέκτησε απομακρυσμένη πρόσβαση σε δεδομένα του λιμένα. Με τα δεδομένα που υπέκλεψαν απέκτησαν την δυνατότητα αναγνώρισης

εμπορευματοκιβωτίων, οπότε είχαν τη δυνατότητα αναγνώρισης και παρακολούθησης των τρωτών σημείων. Στη συνέχεια καταλάμβαναν τα εμπορευματοκιβώτια και τα χρησιμοποιούσαν για διακίνηση ναρκωτικών. Η κυβερνοεπίθεση ανακαλύφθηκε έπειτα από την εξαφάνιση εμπορευματοκιβωτίων, μετά την ανακάλυψη του κακόβουλου λογισμικού και εξουδετέρωση του, οι εγκληματίες διέρρηξαν κάποια γραφεία του λιμένα και εγκατέστησαν τεχνολογικό εξοπλισμό σε διάφορα μηχανήματα καθημερινής χρήσης με σκοπό την υποκλοπή δεδομένων. Η περίπλοκη και συνεχής επίθεση οδήγησε τους εμπειρογνώμονες ασφαλείας να προβούν σε προειδοποιήσεις σε θέματα κυβερνοασφάλειας καθώς οι επιθέσεις σε ναυτιλιακές και λιμενικές υποδομές θα συνεχίσουν να εξελίσσονται και η προστασία της αλυσίδας εφοδιασμού είναι υψίστης σημασίας. Ο *Alex Fidgen*, διευθυντής της *IT* εταιρείας ασφάλειας πληροφορικής *MWR InfoSecurity*, δήλωσε, "αφού οι υπεύθυνοι ασφαλείας του λιμένα εντόπισαν με επιτυχία την επίθεση εναντίον των υπολογιστικών συστημάτων τους, απέτυχαν να χαρτογραφήσουν άλλες διαδρομές επίθεσης που επέτρεψαν στους επιτιθέμενους να επιτύχουν τους στόχους τους σε αυτήν την περίπτωση. Αυτό δείχνει πόσο σημαντικό είναι η κυβερνοασφάλεια δεν πρέπει μόνο να επικεντρωθεί σε μεμονωμένα συστήματα, αλλά να πάρει μια πλήρη επισκόπηση του οργανισμού και τις πιθανές αδυναμίες στις ασκήσεις δοκιμών διείσδυσης.

Σομαλοί πειρατές

Οι Σομαλοί πειρατές έχουν εξελίξει τα μέσα και τους τρόπους επιχείρησης τους, χρησιμοποιούν *hackers* οι οποίοι διεισδύουν στο δίκτυο υπολογιστών της εταιρείας και του πλοίου με σκοπό υποκλοπής δεδομένων του συστήματος *AIS*[3]. Σύμφωνα με στοιχεία από το https://safety4sea.com/ το 2011 οι Σομαλοί πειρατές διπλασίασαν τα χρήματα από τα καταβληθέντα λύτρα από 80 εκατομμύρια δολάρια σε 160. Οι πειρατές χρησιμοποίησαν δεδομένα που υπέκλεψαν για το φορτίο του κάθε πλοίου με αποτέλεσμα να στοχεύουν σε πλοία που μετέφεραν φορτίο μεγαλύτερης αξίας.

Επίθεση σε πλατφόρμα εξόρυξης πετρελαίου στον κόλπο του Μεξικό

[3] *Automated information system*

Οι πλατφόρμες εξόρυξης δεν προστατεύονται επαρκώς από κυβερνοεπιθέσεις, υπάλληλοι της πλατφόρμας κατεβάζοντας παράνομο υλικό πολυμέσων εγκατέστησαν κακόβουλο λογισμικό. Το αποτέλεσμα ήταν πως το κακόβουλο λογισμικό απενεργοποίησε τα συστήματα δυναμικής ευστάθειας (dynamic positioning thrusters) της πλατφόρμας. Η πλατφόρμα πήρε κλίση με αποτέλεσμα για λόγους ασφαλείας να διακοπεί η λειτουργία της πλατφόρμας. Η συγκεκριμένη κυβερνοεπίθεση ανέδειξε τις καταστροφικές επιπτώσεις μιας κυβερνοεπίθεσης σε υπεράκτιες κρίσιμες κατασκευές.

Επίθεση στη MAERSK το 2017

Στις 27 Ιουνίου 2017 στην Ουκρανία ένας ιός με όνομα *NotPetya* χτύπησε τα συστήματα υπολογιστών της εταιρείας διεθνώς. Όπως αποδείχτηκε μετά την έρευνα ο ιός εγκαταστάθηκε στο δίκτυο της εταιρείας έπειτα από λανθασμένη ενέργεια υπαλλήλου ο οποίος άνοιξε τον σύνδεσμο σε μη αναγνωρισμένο *e-mail*. Επιπλέον οι επιπτώσεις ήταν αρκετές καθώς πάνω από 80.000 υπολογιστές προσβλήθηκαν από τον ιό με αποτέλεσμα πολλά συστήματα *IT* να παρουσιάσουν αποτυχία συστήματος. Μετά από αυτήν την επίθεση η εταιρεία αναβάθμισε τα συστήματα ασφαλείας της, στις 20 Σεπτεμβρίου του 2018 αρκετοί διακομιστές της εταιρείας στο λιμάνι της Βαρκελώνης δέχτηκαν κυβερνοεπίθεση αλλά οι επιχειρήσεις των πλοίων δεν επηρεάστηκαν.

Κεφάλαιο 2: Τρωτά σημεία του πλοίου

2.1 Ποσοτικοποίηση της απειλής

Με την ποσοτικοποίηση της απειλής επιτυγχάνεται ένας καλύτερος προσδιορισμός της πιθανότητας επίθεσης, γεγονός που συνεισφέρει τα μέγιστα στην διαχείριση κινδύνου και

εκτίμησης του εύρους της ζημιάς που θα προκαλέσει η εκάστοτε επίθεση. Είναι αναγκαία για την καλύτερη προετοιμασία του τμήματος ασφαλείας της εταιρείας καθώς και για τον προσδιορισμό των βέλτιστων πρακτικών αντιμετώπισης της ενδεχόμενης κρίσης.

2.1.1 Απειλές εναντίον συστημάτων *OT*

Η έλλειψη σημαντικού όγκου δεδομένων από καταγραφές κυβερνοεπιθέσεων καθώς και στατιστικών στοιχείων αποτελεί έναν ιδιαιτέρως σημαντικό παράγοντα που δυσχεραίνει το έργο της ασφάλειας και προστασίας του τμήματος διαχείρισης κινδύνου μιας ναυτιλιακής εταιρίας. Ακόμα δεν επαρκούν τα δεδομένα ώστε να είναι πλήρως γνωστός ο αντίκτυπος διαφορετικών κυβερνοεπιθέσεων στην ναυτιλία. Οι πρώτες ενδείξεις από τα υπάρχοντα δεδομένα είναι πως οι επιθέσεις εναντίον των συστημάτων *OT* είναι λιγότερο συχνές, αν και τις περισσότερες φορές τέτοιες επιθέσεις δεν γίνονται γνωστές καθώς οι εταιρίες αποφεύγουν να δημοσιοποιούν αναφορές για στοχευμένες επιθέσεις στα συστήματα *OT*.

Οι λόγοι για τις λιγότερο συχνές επιθέσεις είναι οι εξής:

1. Τα περισσότερα συστήματα *OT* στην θαλάσσια βιομηχανία εξακολουθούν να μην συνδέονται με εξωτερικά δίκτυα, γεγονός που καθιστά αδύνατη την απομακρυσμένη πρόσβαση. Οπότε η έκθεση σε απειλές κυβερνοεπιθέσεων ελαχιστοποιείται. Προφανώς υπάρχουν και εξαιρέσεις.
2. Τα συστήματα *OT* δεν σχετίζονται άμεσα με οικονομικά οφέλη για τους εγκληματίες.
3. Μια επίθεση στα συστήματα *OT* μπορεί να επιφέρει σημαντικούς κινδύνους για την ασφάλεια των επιβατών του πλοίου, γεγονός που αποτρέπει μια μερίδα των εγκληματιών καθώς οι συνέπειες θα είναι πολύ μεγαλύτερες σε σχέση με μια οικονομική απάτη.

Παρά τους παραπάνω λόγους, οι κίνδυνοι από μια κυβερνοεπίθεση στα συστήματα *OT* του πλοίου δεν πρέπει να υποτιμηθούν καθώς όπως θα αναφέρουμε παρακάτω υπάρχουν τρωτά σημεία και διαδικασίες στο πλοίο τα οποία αν δεχθούν επίθεση μπορούν να διακόψουν τη λειτουργία τους, γεγονός που μπορεί να είναι πολύ επικίνδυνο για την ασφάλεια του πλοίου και του πληρώματος.

2.1.2 Απειλές εναντίον συστημάτων *IT*

Η ποσοτικοποίηση των απειλών κατά των συστημάτων *IT* είναι εφικτή, καθώς υπάρχει σημαντικός όγκος δεδομένων, από ιστορικά στοιχεία ατυχημάτων που έλαβαν χώρα στον χώρο της ναυτιλίας τόσο γενικά αλλά και ειδικά. Συνήθως τα αποτελέσματα μιας επίθεσης στα συστήματα *IT* του πλοίου δεν προκαλεί άμεσα βλάβη στους ανθρώπους του πλοίου, το

περιβάλλον ή τα περιουσιακά στοιχεία τη εταιρίας, παρ' όλα αυτά δεν πρέπει να υποτιμηθεί μια τέτοια επίθεση. Τα αποτελέσματα τέτοιων επιθέσεων έχουν οικονομικό αντίκτυπο κατά κύριο λόγο. Βέβαια υπάρχουν περιπτώσεις όπου η επίθεση στοχεύει στα συστήματα διαχείρισης φορτίου και μπορεί να καταστεί ιδιαιτέρως επικίνδυνη όταν το πλοίο μεταφέρει επικίνδυνο φορτίο.

2.2 Συστήματα του πλοίου που είναι ευάλωτα σε κυβερνοεπιθέσεις

Στην παρούσα ενότητα θα παρουσιαστούν τα ευάλωτα συστήματα του πλοίου

Τα ευάλωτα συστήματα του πλοίου σε κυβερνοαπειλές είναι τα ακόλουθα:

1. Τα συστήματα της γέφυρας.
2. Τα συστήματα χειρισμού και διαχείρισης φορτίου.
3. Τα συστήματα πρόωσης του πλοίου που διαχειρίζονται την ισχύ.
4. Τα συστήματα ελέγχου πρόσβασης.
5. Τα συστήματα εξυπηρέτησης επιβατών.
6. Τα εγκατεστημένα δημόσια κοινωνικά δίκτυα για την εξυπηρέτηση των επιβατών.
7. Τα συστήματα για την ευημερία του πληρώματος.
8. Τα συστήματα επικοινωνίας.

Ειδικότερα

Συστήματα της γέφυρας: τα συστήματα της γέφυρας είναι ευάλωτα σε κυβερνοεπιθέσεις καθώς χρησιμοποιούν ψηφιακά συστήματα για την ναυσιπλοΐα που αλληλοεπιδρούν με συστήματα στην στεριά. Ακόμα και τα συστήματα της γέφυρας που δεν είναι συνδεδεμένα σε άλλα συστήματα είναι ευάλωτα σε κυβερνοεπιθέσεις.

Συστήματα χειρισμού και διαχείρισης φορτίου: τα συγκεκριμένα συστήματα αλληλοεπιδρούν με συστήματα της στεριάς που παρακολουθούν το φορτίο, την θέση του και παρέχουν πληροφορίες για τη κατάσταση του. Η αλληλεπίδραση με ψηφιακά συστήματα εκτός πλοίου τα καθιστά ιδιαίτερα ευάλωτα σε κυβερνοεπιθέσεις.

Συστήματα πρόωσης πλοίου: τα συγκεκριμένα συστήματα χρησιμοποιούν αισθητήρες και ψηφιακά συστήματα με σκοπό την παρακολούθηση και τον έλεγχο του μηχανολογικού εξοπλισμού του πλοίου καθώς και την πηδαλιούχηση του πλοίου. Γι' αυτό τον λόγο είναι

ευάλωτα σε κυβερνοεπιθέσεις, ειδικά όταν όλος ο απαιτούμενος εξοπλισμός χρησιμοποιείται εξ' αποστάσεως.

Συστήματα ελέγχου πρόσβασης: τα συγκεκριμένα συστήματα ελέγχουν ποιος έχει πρόσβαση σε οποιοδήποτε μέρος του πλοίου, είναι ψηφιακά συστήματα σχεδιασμένα για την ασφάλεια και προστασία των επιβατών και του φορτίου του πλοίου. Έχουν τη δυνατότητα επιτήρησης του πλοίου και ενεργοποίησης του συναγερμού ασφαλείας του πλοίου.

Συστήματα εξυπηρέτησης επιβατών: είναι ψηφιακά συστήματα που χρησιμοποιούνται για την επιβίβαση και τον έλεγχο πρόσβασης τον επιβατών. Όλες οι ηλεκτρονικές 'έξυπνες' συσκευές που χρησιμοποιούν οι επιβάτες μπορούν να αποτελέσουν απειλή για την κυβερνοασφάλεια στο πλοίο καθώς υπάρχει η δυνατότητα υποκλοπής δεδομένων και πληροφοριών κατά την σύνδεση τους στο διαδίκτυο.

Εγκατεστημένα δημόσια κοινωνικά δίκτυα για την εξυπηρέτηση των επιβατών: αφορούν διάφορα εγκατεστημένα προγράμματα στα οποία συνδέονται οι επιβάτες. Κατά τη σύνδεση των επιβατών σε αυτά τα συστήματα δεν υπάρχει έλεγχος από το προσωπικό του πλοίου και σε περίπτωση που δεν υπάρχει διαχωρισμός με κρίσιμα συστήματα του πλοίου υπάρχει σοβαρός κίνδυνος για την κυβερνοασφάλεια του πλοίου.

Συστήματα για τη ευημερία του πληρώματος: αποτελούν ίσως τα πιο ευάλωτα συστήματα του πλοίου για κυβερνοεπιθέσεις. Είναι εγκατεστημένα συστήματα που εξασφαλίζουν την ασφάλεια, τα δικαιώματα και την όσο το δυνατόν καλύτερη διαβίωση του πληρώματος εν πλω.

Συστήματα επικοινωνίας: αποτελούν τον μεγαλύτερο κίνδυνο για κυβερνοεπιθέσεις.

2.3 Τρωτά σημεία

Στην παρούσα ενότητα παρουσιάζονται τα συνηθέστερα τρωτά σημεία που βρίσκονται είτε πάνω στο πλοίο είτε αφορούν διεργασίες που σχετίζονται με τη λειτουργία του πλοίου.

1. Μη αναβαθμισμένα ή παλαιότερης τεχνολογίας λειτουργικά συστήματα αποτελούν πάντα μια πιθανή απειλή για κυβερνοεπίθεση, ειδικά στη περίπτωση που το λειτουργικό σύστημα δεν υποστηρίζεται πλέον από τον κατασκευαστή του.
2. Ένα μη ενημερωμένο σύστημα προστασίας από ιούς και κακόβουλο λογισμικό ή ακόμα και η έλλειψη αυτού αποτελεί σημαντικό τρωτό σημείο για την προστασία του πλοίου από κυβερνοεπιθέσεις. Όταν συστήματα του πλοίου συνδέονται σε δίκτυα εκτός πλοίου, η προστασία από κακόβουλο λογισμικό είναι απαραίτητη.

3. Η χρήση προεπιλεγμένων λογαριασμών διαχειριστή καθώς και κωδικών πρόσβασης αποτελούν σημαντικά τρωτά σημεία για την ασφάλεια του πλοίου. Επίσης υπάρχει πιθανότητα να μην χρησιμοποιούνται οι βέλτιστες πρακτικές ασφαλείας, όπως και η ανεπαρκής διαμόρφωση του συστήματος ασφαλείας.
4. Τα τοπικά δίκτυα υπολογιστών στο πλοίο όταν δεν διαθέτουν τα κατάλληλα μέτρα προστασίας και δεν είναι κατάλληλα χωρισμένα σε διαφορετικά δίκτυα ανάλογα με τον τομέα λειτουργίας τους.
5. Η χρήση λογισμικού χωρίς τη χρήση των πρόσθετων αναβαθμίσεων που διορθώνουν τα όποια ανθρώπινα σφάλματα ή αστοχίες που υπήρχαν κατά την κατασκευή του.
6. Τα συστήματα του πλοίου που συνδέονται με συστήματα στην ακτή είναι πιθανά τρωτά σημεία σε ένα πλοίο.
7. Ο ανεπαρκής έλεγχος πρόσβασης στον κυβερνοχώρο και σε εξωτερικά δίκτυα τρίτων.
8. Η ανεπαρκής εκπαίδευση του προσωπικού ασφαλείας στην αντιμετώπιση κυβερνοεπιθέσεων.
9. Τέλος το ίδιο το σχέδιο και το πρωτόκολλο αντιμετώπισης κρίσεων και ζητημάτων κυβερνοασφάλειας είναι πιθανό να είναι ανεπαρκές οπότε αποτελεί από τα σημαντικότερα τρωτά σημεία του πλοίου σε ζητήματα κυβερνοασφάλειας.

2.4 Επαφή του πλοίου με συστήματα στην ακτή

Με την εξέλιξη της τεχνολογίας των επικοινωνιών η σύνδεση των πλοίων με τις επιχειρήσεις στη στεριά έχει αυξηθεί σημαντικά. Η επαφή με τα γραφεία της εταιρείας έχει γίνει απαραίτητη για τη διεξαγωγή κάποιων επιχειρήσεων και τη διαχείριση λειτουργιών. Πολλά από τα συστήματα ασφαλείας και διαχείρισης φορτίου έχουν ψηφιοποιηθεί με αποτέλεσμα η επαφή με ψηφιακά συστήματα στη στεριά να είναι απαραίτητη για την σωστή λειτουργία τους. Οι λειτουργίες που είναι απαραίτητο να εκτελεστούν με σύνδεση στο διαδίκτυο είναι οι εξής:

Παρακολούθηση της απόδοσης του κινητήρα: Τα συστήματα παρακολούθησης της απόδοσης του κινητήρα θα αποτελούν αναπόσπαστο μέρος των (περισσότερων) συστημάτων που εγκαθίστανται στα πλοία στο άμεσο μέλλον, επειδή η διαδικασία λήψης αποφάσεων γίνεται ευκολότερη και πιο απλή όταν βασίζεται σε δεδομένα πλοίων που συλλέγονται σε πραγματικό χρόνο, σε αντίθεση με τα δεδομένα που συλλέγονται με μη αυτόματο τρόπο, όπως οι μεσημεριανές αναφορές. Τα συστήματα παρακολούθησης της απόδοσης αποτελούν ουσιαστικά την εξέλιξη και βελτίωση του συστήματος παρακολούθησης κατανάλωσης καυσίμου, το οποίο χρησιμοποιεί δεδομένα για την ροπή, την ταχύτητα και την ισχύ των κινητήρων του πλοίου. Επίσης το σύστημα καταγράφει και επεξεργάζεται δεδομένα από τα σήματα *NMEA (National Marine Electronics Association)* όπως από το σύστημα *GPS, echo sounder* και το γυρόμετρο. Η κύρια αρχή λειτουργίας του συστήματος παρακολούθησης απόδοσης του κινητήρα είναι η μέτρηση της ροής καυσίμου σε όλα τα στάδια λειτουργίας των κινητήρων του πλοίου και σε συνδυασμό με τις μετρήσεις της ταχύτητας του πλοίου, της θέσης του, της ροπής στις προπέλες, την ισχύ των γεννητριών και του ανεμομέτρου να υπολογίσει την απόδοση του κινητήρα και την αποτελεσματικότητα της κατανάλωσης καυσίμου. Όλες οι μετρήσεις του συστήματος μεταφέρονται μέσω του δικτύου *Modbus*[4], για να φτάσουν όμως τα αποτελέσματα των υπολογισμών στα γραφεία της εταιρείας στη στεριά είναι απαραίτητη η σύνδεση των δύο βάσεων δεδομένων (η μία βρίσκεται στο πλοίο και η άλλη στην εταιρεία) μέσω διαδικτύου. Όπως είναι λογικό λόγο της σύνδεσης στο διαδίκτυο είναι στόχος κυβερνοεπίθεσης με σκοπό την υποκλοπή δεδομένων του πλοίου.

Απομακρυσμένος έλεγχος αντιμετώπισης προβλημάτων: η εξέλιξη της τεχνολογίας δίνει τη δυνατότητα στις ναυτιλιακές εταιρείες να μπορούν απομακρυσμένα να παρακολουθούν διαμέσου εγκατεστημένου εξοπλισμού στο πλοίο τις κύριες λειτουργίες του. Υπάρχουν αρκετά συστήματα στην αγορά που χρησιμοποιούν οι ναυτιλιακές εταιρίες, τα συστήματα αυτά συνδέονται μέσω διαδικτύου με συστήματα του πλοίου και παρέχουν τη δυνατότητα άμεσης παρακολούθησης και ελέγχου των συστημάτων του πλοίου στους υπεύθυνους της εταιρείας στη στεριά. Έχουν αισθητήρες που ενεργοποιούν συναγερμούς ασφαλείας για την άμεση ενημέρωση του πληρώματος. Επίσης με χρήση οπτικών μέσων το κατάλληλο προσωπικό στη στεριά μπορεί να αντιμετωπίσει και να διαγνώσει αρκετά προβλήματα και βλάβες. Η σύνδεση στο διαδίκτυο καθώς και η πρόσβαση στα συστήματα του πλοίου σε

[4] Πρωτόκολλο επικοινωνίας που βασίζεται στην αρχιτεκτονική *master-slave*

συνδυασμό με τη χρήση οπτικών μέσων αποτελεί ένα εν δυνάμει τρωτό σημείο στο πλοίο, το οποίο θα μπορούσε να δεχθεί κυβερνοεπίθεση.

Συντήρηση και διαχείριση ανταλλακτικών: για την προληπτική συντήρηση του μηχανολογικού εξοπλισμού του πλοίου χρησιμοποιούνται τεχνολογίες πληροφορικής και παρακολούθησης, οι οποίες συλλέγουν δεδομένα σε πραγματικό χρόνο. Τα δεδομένα αυτά σχετίζονται με την ομαλή λειτουργία του κινητήρα καθώς και τα συστήματα ασφαλείας του πλοίου. Χρησιμοποιούνται λοιπόν συστήματα τα οποία επεξεργάζονται τα δεδομένα αυτά και κάνουν εκτίμηση για τον χρόνο ζωής των μηχανών του πλοίου καθώς και των ανταλλακτικών. Τα συστήματα αυτά έχουν τη δυνατότητα προειδοποίησης του χρήστη για πιθανή ενδεχόμενη βλάβη κάποιου εξαρτήματος. Η προγραμματισμένη συντήρηση εξαρτημάτων του πλοίου στηρίζεται στα συγκεκριμένα συστήματα. Όταν τα συστήματα αυτά συνδέονται με προγράμματα στη στεριά υπάρχει ο κίνδυνος υποκλοπής δεδομένων, γι' αυτό τον λόγο κατατάσσονται και αυτά στα πιθανά τρωτά σημεία του πλοίου.

Συστήματα διαχείρισης επιμελητείας *(logistics)*: τα συστήματα που παρακολουθούν και διαχειρίζονται το φορτίο και τα εμπορευματοκιβώτια του πλοίου καθώς και τον σχεδιασμό φόρτωσης- εκφόρτωσης και αποθήκευσης. Η βασική λειτουργία των συγκεκριμένων συστημάτων είναι ο έλεγχος και εύρεση της βέλτιστης κατανομής χώρου, με σκοπό τα εμπορευματοκιβώτια και το φορτίο του πλοίου να φορτωθούν σε συγκεκριμένο λιμάνι και να μην χρειαστεί να αλλάξει η θέση τους καθ' όλη τη διάρκεια του ταξιδιού μέχρι το λιμάνι εκφόρτωσης. Για τη λειτουργία του συστήματος είναι απαραίτητη η λήψη δεδομένων για το είδος και το μέγεθος του φορτίου, ο αριθμός των εμπορευματοκιβωτίων και γενικότερα πληροφορίες για τον χώρο αποθήκευσης του πλοίου, όπως επίσης τα χρονοδιαγράμματα εκφορτώσεων. Αποτελούν τρωτό σημείο του πλοίου καθώς τα συγκεκριμένα συστήματα συνδέονται στο διαδίκτυο με συστήματα της εταιρείας στη στεριά και διαχειρίζονται πληροφορίες για το φορτίο του πλοίου και τη διαδρομή του που αποτελούν πιθανό στόχο κυβερνοεπιθέσεων.

Συστήματα διαχείρισης γερανών και αντλιών: τα συστήματα του πλοίου που διαχειρίζονται την ηλεκτρική ισχύ που καταναλώνουν οι γερανοί και ελέγχουν τη σωστή λειτουργία των αντλιών του πλοίου. Ελέγχουν τις αντλίες πυρασφάλειας του πλοίου και στέλνουν δεδομένα στην στεριά, οπότε αποτελούν στόχο κυβερνοεπιθέσεων.

Συστήματα παρακολούθησης τήρησης περιβαλλοντικών κανονισμών: τα τελευταία χρόνια οι κανονισμοί για την προστασία του περιβάλλοντος έχουν γίνει αρκετά πιο αυστηροί με

αποτέλεσμα οι εταιρείες να εγκαθιστούν συστήματα παρακολούθησης των εκπομπών καυσαερίων, μόλυνσης του θαλάσσιου περιβάλλοντος είτε από διαρροή καυσίμου είτε από αποθέσεις έρματος ή υπολειμμάτων δεξαμενών. Τα συγκεκριμένα συστήματα στέλνουν αναφορές στην εταιρεία μέσω διαδικτύου με αποτέλεσμα να υπάρχει ο κίνδυνος υποκλοπής, γι' αυτό το λόγο κατατάσσονται στα τρωτά σημεία του πλοίου.

Συστήματα παρακολούθησης της απόδοσης του ταξιδιού: με την εξέλιξη της τεχνολογίας έχουν δημιουργηθεί συστήματα που παρακολουθούν σε πραγματικό χρόνο τα δεδομένα για το βέλτιστο ταξίδι του πλοίου. Συλλέγουν δεδομένα και υπολογίζουν τη βέλτιστη διαδρομή, την βέλτιστη ταχύτητα, χρησιμοποιούν δεδομένα για τη θέση του πλοίου, την ταχύτητα του, τις καιρικές συνθήκες, το φορτίο του πλοίου, τη κατανάλωση καυσίμου, την ταχύτητα του ανέμου, το ύψος των κυμάτων με σκοπό τον υπολογισμό των βέλτιστων συνθηκών για το ταξίδι σύμφωνα με τους προκαθορισμένους χρόνους πλεύσης. Όπως είναι αναμενόμενο είναι από τα σημαντικότερα συστήματα που είναι πιθανόν να δεχτούν κυβερνοεπίθεση.

Όλα τα παραπάνω παραδείγματα αποτελούν πιθανούς στόχους εγκληματιών με σκοπό την υποκλοπή δεδομένων. Η εξέλιξη της τεχνολογίας είναι γεγονός πως προσθέτει πιθανά τρωτά και ευάλωτα σημεία στα πλοία, ειδικότερα όταν τα δίκτυα δεν είναι σωστά σχεδιασμένα και δεν υπάρχει έλεγχος στην πρόσβαση στο διαδίκτυο. Μία επιπλέον παράμετρος για την κυβερνοασφάλεια είναι πως σε κάποιες περιπτώσεις ενδέχεται κατασκευαστές μηχανολογικού εξοπλισμού και συστημάτων λογισμικού να μπορούν να έχουν πρόσβαση στον εξοπλισμό και το σύστημα του πλοίου και το προσωπικό της εταιρείας να μην το γνωρίζει. Η άγνωστη και μη συντονισμένη απομακρυσμένη πρόσβαση στις λειτουργίες του πλοίου πρέπει να λαμβάνεται υπόψιν από τους υπεύθυνους ασφαλείας του πλοίου καθώς αποτελεί έναν από του σημαντικότερους κινδύνους για ενδεχόμενη κυβερνοεπίθεση.

2.5 Επίσκεψη τρίτων στο πλοίο

Στις περιπτώσεις όπου επισκέπτονται το πλοίο τρίτοι οι οποίοι έχουν πρόσβαση στα υπολογιστικά συστήματα του πλοίου καθώς και σύνδεση στο δίκτυο του πλοίου, το αποτέλεσμα είναι το πλοίο να συνδέεται με συστήματα στη στεριά και να προκύπτουν τα τρωτά σημεία που παρουσιάστηκαν στην προηγούμενη ενότητα. Στις περιπτώσεις ανάγκης επίσκεψης τεχνικού συνεργείου για την επισκευή κάποιου προβλήματος είναι σύνηθες οι υπάλληλοι του συνεργείου κατά την επιβίβαση τους να συνδέουν φορτιστές κινητών ή ηλεκτρονικών συσκευών, το ίδιο δύναται να συμβεί και κατά την επιβίβαση πιλότων,

αξιωματούχων λιμένων και γενικότερα αντιπροσώπους θαλασσίων οργανισμών. Ορισμένοι τεχνικοί για την επίλυση του όποιου προβλήματος ενδέχεται να χρησιμοποιήσουν αφαιρούμενα οπτικά μέσα για ενημέρωση λογισμικού, λήψη δεδομένων ή εκτέλεση άλλων εργασιών, επίσης οι αξιωματούχοι λιμένων ζητούν χρήση υπολογιστή ώστε να εκτυπώσουν επίσημα έγγραφα μετά από εισαγωγή άγνωστου στο πλοίο αφαιρούμενου οπτικού μέσου. Όλα τα παραπάνω δημιουργούν ευάλωτα σημεία στα συστήματα του πλοίου, αποτελούν τρωτά σημεία για ενδεχόμενες κυβερνοεπιθέσεις.

Επειδή πολλές φορές δεν είναι δυνατόν να υπάρχει έλεγχος για το ποιος από τους τρίτους που έχει επιβιβαστεί στο πλοίο έχει πρόσβαση στα συστήματα του και αν εγκαταστάθηκε κακόβουλο λογισμικό κατά την παραμονή τους στο πλοίο συνίσταται η κατάργηση ευαίσθητων δεδομένων και επανεγκατάσταση τους μετά το πέρας της επίσκεψης των τρίτων. Είναι αναγκαίο να υπάρχει αντίγραφο ασφαλείας και πριν την εκκίνηση των συστημάτων του πλοίου να γίνεται σάρωση από λογισμικό ασφαλείας για την ανίχνευση κακόβουλου λογισμικού και έλεγχος των *OT* συστημάτων για την σωστή λειτουργία τους.

2.6 Απομακρυσμένη πρόσβαση

Υπάρχουν συστήματα *IT* και *OT* του πλοίου που διαθέτουν τη λειτουργία απομακρυσμένης πρόσβασης και λειτουργούν με συνεχή σύνδεση τους στο διαδίκτυο ώστε να γίνεται παρακολούθηση της λειτουργίας των συστημάτων του πλοίου και η συλλογή δεδομένων για τις λειτουργίες συντήρησης και ασφάλειας καθώς και προστασίας. Τα συγκεκριμένα συστήματα λειτουργούν ως *'third party systems'* όπου ο κατασκευαστής παρακολουθεί την σωστή λειτουργία του συστήματος απομακρυσμένα. Τα συστήματα αυτά μπορούν να περιλαμβάνουν αμφίδρομη ροή δεδομένων, τέτοια συστήματα μπορούν να είναι τα εξής:

- Υπολογιστές και σταθμοί εργασίας εγκατεστημένοι στη γέφυρα ή στο μηχανοστάσιο.
- Ειδικά φορτία και εμπορευματοκιβώτια που έχουν εγκατεστημένα συστήματα παρακολούθησης ελέγχου θερμοκρασίας ή εξειδικευμένα φορτία που απαιτούν παρακολούθηση από απόσταση.
- Συστήματα υποστήριξης της ευστάθειας του πλοίου.
- Συστήματα παρακολούθησης καταπονήσεων της γάστρας του πλοίου.

- Συστήματα παρακολούθησης πλεύσης όπως *Electronic Navigation Chart (ENC), Voyage Data Recorder (VDR), dynamic positioning (DP).*
- Συστήματα σχεδιασμού, διαχείρισης και αποθήκευσης φορτίου.
- Συστήματα παρακολούθησης του κινητήρα.
- Συστήματα ασφαλείας και προστασίας όπως *CCTV (Closed circuit television).*
- Εξειδικευμένα συστήματα για διαφορετικού τύπου πλοία.

Κεφάλαιο 3: Διεθνές νομοθετικό πλαίσιο

3.1 Η συνθήκη της Βουδαπέστης

Στις 23/11/2001 τα κράτη μέλη του συμβουλίου της Ευρώπης υπέγραψαν την διεθνή σύμβαση για το έγκλημα στον κυβερνοχώρο. Σκοπός της συνθήκης της Βουδαπέστης ήταν η επιδίωξη μιας κοινής αντί εγκληματικής πολιτικής και υιοθέτηση κατάλληλης νομοθεσίας και η ενίσχυση της διεθνούς συνεργασίας. Από το 2000 είχε γίνει αντιληπτό πως η χρησιμοποίηση

των δικτύων και των πληροφοριών θα αποτελέσει στόχο εγκληματιών που θα αποσκοπούν στην υποκλοπή ευαίσθητων στοιχείων. Κατά την συνθήκη της Βουδαπέστης αναζητήθηκε ο βέλτιστος συνδυασμός ώστε να διασφαλιστεί η σωστή ισορροπία μεταξύ των συμφερόντων της επιβολής του νόμου άλλα και ο σεβασμός των θεμελιωδών ανθρωπίνων δικαιωμάτων, όπως αυτά προστατεύονται από τη Σύμβαση του Συμβουλίου της Ευρώπης του 1950 και τη Διεθνή Σύμβαση των Ηνωμένων Εθνών του 1966 για τα Αστικά και Πολιτικά Δικαιώματα, σε συνδυασμό με άλλες ισχύουσες συμβάσεις για την προστασία των ανθρωπίνων δικαιωμάτων. Επίσης όλες οι ενέργειες για την προστασία από το έγκλημα στον κυβερνοχώρο πρέπει να λαμβάνουν υπόψιν το δικαίωμα προστασίας των προσωπικών δεδομένων.

Με βάση τα ανωτέρω καθώς και το Σχέδιο Δράσης που υιοθέτησαν οι Αρχηγοί Κρατών και Κυβερνήσεων του Συμβουλίου της Ευρώπης μετά την Δεύτερη Διάσκεψη Κορυφής που έλαβε χώρα στο Στρασβούργο το 1977 για την αναζήτηση κοινά αποδεκτών λύσεων στην ανάπτυξη της τεχνολογίας της πληροφορικής με βάση τα πρότυπα και τις αξίες του Συμβουλίου της Ευρώπης συμφώνησαν τα εξής:

Κεφάλαιο 1

Στο πρώτο κεφάλαιο συμφωνήθηκε η ορολογία, στο πρώτο άρθρο καθορίστηκαν οι ορισμοί όρων όπως σύστημα υπολογιστή, δεδομένα υπολογιστή, πάροχος υπηρεσιών κ.α.

Κεφάλαιο 2

Στο δεύτερο κεφάλαιο συμφωνήθηκαν τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο. Καθορίστηκε το ουσιαστικό ποινικό δίκαιο που αφορά τα εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών, εγκλήματα σχετικά με υπολογιστές και με το περιεχόμενο. Καθορίστηκε η εξαρτημένη ευθύνη νομικών προσώπων και οι κυρώσεις και το δικονομικό πλαίσιο.

Με την Συνθήκη της Βουδαπέστης καθορίστηκε η διαδικασία και οι όροι για την συλλογή δεδομένων υπολογιστή σε πραγματικό χρόνο καθώς και για την άρση του απορρήτου των δεδομένων περιεχομένου. Καθορίστηκαν οι όροι εμπιστευτικότητας και περιορισμού.

Συνολικά η Συνθήκη της Βουδαπέστης αποτελείται από 48 άρθρα και δεσμεύει κάθε συμβαλλόμενο μέλος της να θεσπίσει νομοθεσία και μέτρα που είναι απαραίτητα για τον καθορισμό της δικαιοδοσίας για κάθε αδίκημα που διαπράττεται στον κυβερνοχώρο και σχετίζεται με πλοία που είναι συμβαλλόμενα με την εν λόγω σύμβαση. Ο κυριότερος στόχος της συνθήκης ήταν ο καθορισμός κοινής πολιτικής με στόχο την προστασία της κοινωνίας και

των πολιτών από πιθανά εγκλήματα στον κυβερνοχώρο θεσπίζοντας την κατάλληλη νομοθεσία και ενθαρρύνοντας την διεθνή συνεργασία.

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

Τον Ιούνιο του 2017 η 98η σύνοδος της Επιτροπής Ναυτικής Ασφάλειας *(Maritime Safety Committee)* ενέκρινε τις κατευθυντήριες οδηγίες για την διαχείριση κινδύνου στον θαλάσσιο κυβερνοχώρο οι οποίες δημοσιεύτηκαν με τίτλο MSC98. Η συγκεκριμένη εγκύκλιος προς τους πλοιοκτήτες παραμένει και σήμερα μη υποχρεωτική. Στην ίδια σύνοδο υιοθετήθηκε το ψήφισμα για τα συστήματα διαχείρισης ασφαλείας (SMS). Σύμφωνα με την σύνοδο αποφασίστηκε πως ένα εγκεκριμένο *SMS* πρέπει να λαμβάνει υπόψη την διαχείριση κινδύνου στον κυβερνοχώρο σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις της Διεθνούς Διαχείρισης Ασφαλείας (*ISM*), οι συγκεκριμένοι στόχοι περιλαμβάνουν την παροχή ασφαλών πρακτικών στη λειτουργία των πλοίων και ασφαλούς περιβάλλοντος εργασίας. Επίσης γίνεται εκτίμηση όλων των εντοπισμένων κινδύνων για τα πλοία, το προσωπικό και το περιβάλλον.

Στην συγκεκριμένη σύνοδο δόθηκε ο ορισμός του κινδύνου στον κυβερνοχώρο, το είδος της απειλής καθώς και τα τρωτά σημεία του συστήματος ασφαλείας του πλοίου. Επίσης δόθηκαν κατευθυντήριες οδηγίες στις ναυτιλιακές εταιρείες ώστε να θεσπίσουν διαδικασίες, κανόνες καθώς και να προχωρήσουν στην απαιτούμενη εκπαίδευση του προσωπικού τους με σκοπό την μείωση της πιθανότητας εμφάνισης κυβερνοεπίθεσης, είτε εξωτερική είτε εσωτερική.

Σύμφωνα με τις απαιτήσεις του κώδικα *ISM* κάθε ναυτιλιακή εταιρεία οφείλει να δημιουργήσει και εφαρμόσει το σύστημα *SMS* το οποίο θα ικανοποιεί τα εξής:

1. Πολιτική προστασίας του περιβάλλοντος και ασφαλείας.
2. Οι οδηγίες και διεργασίες οφείλουν να είναι σύμφωνες με τη νομοθεσία του κράτους σημαίας αλλά και με την διεθνή νομοθεσία για την ασφαλή λειτουργία πλοίων και την προστασία του περιβάλλοντος.
3. Καθορισμό σαφών επιπέδων αρμοδιοτήτων και καναλιών επικοινωνίας μεταξύ πλοίου και ξηράς.
4. Διαδικασίες αναφοράς ατυχήματος ή επίθεσης καθώς και μη συμμόρφωσης στις διατάξεις του κώδικα.
5. Διαδικασίες προετοιμασίας και αντιμετώπισης καταστάσεων έκτακτης ανάγκης.
6. Διαδικασίες εσωτερικού ελέγχου και αναθεωρήσεων.

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

Ο διεθνής ναυτιλιακός οργανισμός *IMO* το 2002 ενέκρινε τις κατευθυντήριες γραμμές για την πρόληψη έκνομων πράξεων σε πλοία και λιμενικές εγκαταστάσεις καθορίζοντας τον διεθνή κώδικα *I.S.P.S.* Ο κώδικας έχει ισχύ για πλοία που εκτελούν διεθνή δρομολόγια, συμπεριλαμβανομένων των επιβατηγών και φορτηγών πλοίων των οποίων η χωρητικότητα ξεπερνά τους 500 κόρους, δεν έχει ισχύ όμως σε πολεμικά πλοία και κυβερνητικά πλοία που εκτελούν μη εμπορικές υπηρεσίες.

Εφαρμόστηκε πρώτα στην Ευρώπη το 2004 και αποτελείται από δύο μέρη, το πρώτο μέρος περιλαμβάνει τις υποχρεωτικές διατάξεις και το δεύτερο μέρος τις προαιρετικές.

Οι κύριοι στόχοι του είναι οι ακόλουθοι:

1. Η θέσπιση διεθνούς πλαισίου συνεργασίας ανάμεσα στις τοπικές αρχές, τις κυβερνήσεις καθώς και τις κυβερνητικές υπηρεσίες με τις ναυτιλιακές και λιμενικές εταιρείες με σκοπό την αντιμετώπιση απειλών που μπορούν να θέσουν σε κίνδυνο την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων.

2. Ο καθορισμός ενός διεθνούς πλαισίου το οποίο θα καθορίζει με σαφήνεια τις αρμοδιότητες σε συνδυασμό με τις υποχρεώσεις όλων των εμπλεκόμενων μερών για την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων.

3. Η εξασφάλιση ασφαλούς ανταλλαγής πληροφοριών που αφορούν την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων.

4. Η σχεδίαση και ανάπτυξη της απαιτούμενης μεθοδολογίας για την εκτίμηση της ασφάλειας και διασφάλιση ύπαρξης σχεδίων δράσης και αντιμετώπισης σε περίπτωση αλλαγής των επιπέδων ασφαλείας.

5. Η διασφάλιση της επαρκούς και αναγκαίας λήψης όλων των απαραίτητων μέτρων ναυτικής ασφάλειας.

Επίπεδα ασφαλείας

Τα πλοία είναι υποχρεωμένα να εφαρμόζουν μέτρα ασφαλείας τα οποία να κατηγοριοποιούνται σύμφωνα με τρία επίπεδα ασφαλείας.

Επίπεδο ασφαλείας 1: όταν εφαρμόζονται τα ελάχιστα κατάλληλα μέτρα προστασίας

Επίπεδο ασφαλείας 2: όταν εφαρμόζονται πρόσθετα κατάλληλα μέτρα προστασίας για ορισμένο χρονικό διάστημα λόγω περιστατικού ασφαλείας που κρίνεται ως αυξημένου κινδύνου

Επίπεδο ασφαλείας 3: όταν εφαρμόζονται ειδικά μέτρα προστασίας για περιορισμένο χρονικό διάστημα όταν ένα περιστατικό είναι πιθανό ή άμεσο

Τα προληπτικά μέτρα σε περίπτωση **ασφαλείας 1** είναι τα ακόλουθα:

1. Διασφάλιση της επιτέλεσης όλων των σχετικών με την ασφάλεια καθηκόντων στη λιμενική εγκατάσταση.
2. Έλεγχος πρόσβασης στη λιμενική εγκατάσταση.
3. Παρακολούθηση των χώρων αγκυροβολιάς και προσόρμισης καθώς και του συνόλου της λιμενικής εγκατάστασης.
4. Έλεγχος των εισόδων χώρων περιορισμένης πρόσβασης ώστε να διασφαλίζεται η πρόσβαση μόνο εξουσιοδοτημένων ατόμων.
5. Επίβλεψη του χειρισμού φορτίων και εφοδιασμού.
6. Διασφάλιση της άμεσης επικοινωνίας ασφαλείας.

Αξιολόγηση ασφαλείας λιμενικής εγκατάστασης

Η κατ’ ελάχιστον αξιολόγηση λιμενικών εγκαταστάσεων περιλαμβάνει τα ακόλουθα μέτρα:

1. Αξιολόγηση και προσδιορισμός των περιουσιακών στοιχείων και υποδομών των οποίων η προστασία κρίνεται ως σημαντική.
2. Αξιολόγηση και προσδιορισμός των πιθανών απειλών και κινδύνων για τα περιουσιακά στοιχεία και υποδομές και θέσπιση μέτρων ασφαλείας κατά σειρά προτεραιότητας.
3. Αξιολόγηση και προσδιορισμός σε συνδυασμό με την επιλογή και την κατάταξη κατά σειρά προτεραιότητας διαδικαστικών αλλαγών και αντισταθμιστικών μέτρων με σκοπό την μείωση του βαθμού ευπάθειας.

4. Αξιολόγηση και προσδιορισμός των αδυναμιών προστασίας και ασφάλειας της λιμενικής εγκατάστασης συμπεριλαμβανομένου του ανθρώπινου παράγοντα στις υποδομές, στις πολιτικές και στις διαδικασίες.

Σχέδιο ασφάλειας λιμενικής εγκατάστασης

Το σχέδιο ασφάλειας λιμενικής εγκατάστασης περιλαμβάνει μέτρα για την πρόληψη της εισόδου στη λιμενική εγκατάσταση ή σε πλοίο όπλων και επικίνδυνων ουσιών και μηχανισμών. Επίσης περιλαμβάνει μέτρα για τον έλεγχο πρόσβασης στην λιμενική εγκατάσταση, σε πλοία προσδεμένα στη λιμενική εγκατάσταση και σε ζώνες περιορισμένης πρόσβασης για μη εξουσιοδοτημένα άτομα. Το σχέδιο λιμενικής εγκατάστασης καλύπτει και τις διαδικασίες αντιμετώπισης απειλών της ασφάλειας ή συμβάντων παραβίασης της ασφάλειας συμπεριλαμβανομένων των απαραίτητων διαδικασιών για την διατήρηση των κρίσιμων λειτουργιών της λιμενικής εγκατάστασης και της διασύνδεσης πλοίου/λιμένα. Στην περίπτωση που κρατικές αρχές ενεργοποιήσουν τις οδηγίες ασφαλείας επιπέδου 3 όλες οι απαραίτητες διαδικασίες περιλαμβάνονται στο σχέδιο ασφαλείας. Η διαδικασία εκκένωσης περιλαμβάνεται στο σχέδιο όπως και ο καθορισμός των καθηκόντων ασφαλείας του προσωπικού του λιμένα. Οι υπεύθυνοι ασφαλείας οφείλουν να προβούν σε διαδικασίες περιοδικής αναθεώρησης του σχεδίου και όποτε κρίνεται απαραίτητο σε αναθεώρηση του.

Σχέδιο ασφαλείας πλοίου

Σύμφωνα με τον κώδικα *I.S.P.S* πρέπει να δημιουργηθεί ένα σχέδιο ασφαλείας πλοίου *(SSP)*, το οποίο να επικεντρώνεται στην φυσική ασφάλεια του πλοίου. Σύμφωνα με το σχέδιο καθορίζονται οι ευθύνες και υποχρεώσεις του προσωπικού του πλοίου και του λιμένα. Επίσης είναι υποχρέωση του πλοίου η ανάπτυξη σχεδίου εκτίμησης κινδύνου πλοίου *(SSA)*. Ο υπεύθυνος ασφαλείας της εταιρείας διασφαλίζει ότι τα άτομα με τις κατάλληλες δεξιότητες που λαμβάνουν τις κατευθυντήριες γραμμές που παρέχονται στο Β μέρος του κώδικα *I.S.P.S* εκπονούν την Εκτίμηση Κινδύνου του πλοίου. Η εκτίμηση κινδύνου του πλοίου εγκρίνεται από τον υπεύθυνο ασφαλείας της εταιρείας. Η Εκτίμηση Κινδύνου λαμβάνει υπόψιν τα ακόλουθα στοιχεία:

- Τον προσδιορισμό των υφιστάμενων μέτρων, διαδικασιών και πράξεων ασφαλείας.
- Τον προσδιορισμό και αξιολόγηση των βασικών λειτουργιών επί του πλοίου που είναι σημαντικό να προστατευθούν.
- Τον εντοπισμό πιθανών απειλών και την πιθανότητα εμφάνισης τους.
- Τον προσδιορισμό της αδυναμίας, συμπεριλαμβανομένου του ανθρώπινου παράγοντα.

3.4 Εγκύκλιος *I.M.O* για την κυβερνοασφάλεια

Το 2017 η επιτροπή για την ασφάλεια ενέκρινε τις κατευθυντήριες οδηγίες για την διαχείριση των θαλάσσιων κινδύνων στον κυβερνοχώρο έχοντας εξετάσει τα τρωτά σημεία του πλοίου. Οι οδηγίες που εξέδωσε η επιτροπή παρέχουν υψηλού επιπέδου ασφάλεια για την διαχείριση μιας κυβερνοεπίθεσης και τις οδηγίες για την ασφάλεια του προσωπικού.

Δόθηκε ο ορισμός του θαλάσσιου κινδύνου στον κυβερνοχώρο ως η απειλή που μπορεί να υποστεί ένα τεχνολογικό περιουσιακό στοιχείο του πλοίου ή της εταιρείας είτε από μια περίσταση ή ένα γεγονός. Επίσης καθορίστηκε η σπουδαιότητα της διαχείρισης κινδύνου για την ασφάλεια και προστασία και η ανάγκη ψηφιοποίησης της καθώς τα συστήματα του πλοίου είναι πλέον αυτοματοποιημένα και συνδέονται σε δίκτυα. Τα ενδιαφερόμενα μέλη καλούνται να λάβουν τα απαιτούμενα μέτρα για την προστασία και ασφάλεια από κυβερνοεπιθέσεις. Με βάση το στόχο της στήριξης της ασφαλούς ναυτιλίας, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους στον κυβερνοχώρο, οι κατευθυντήριες γραμμές παρέχουν προτάσεις οι οποίες μπορούν να ενσωματωθούν στις τρέχουσες διαδικασίες διαχείρισης και αξιολόγησης κινδύνων.

Εν προκειμένω, οι κατευθυντήριες γραμμές είναι συμπληρωματικές προς τις πρακτικές διαχείρισης της ασφάλειας και της προστασίας που έχουν καθοριστεί από τον *IMO*.

Η εξέλιξη της τεχνολογίας τηλεπικοινωνιών καθιστά τις τεχνολογίες του κυβερνοχώρου απαραίτητες για την ασφαλή λειτουργία του πλοίου. Η χρήση όμως αρκετών συστημάτων του πλοίου μπορεί να δημιουργήσει τρωτά σημεία στην ασφαλή λειτουργία του πλοίου, γι' αυτό τον λόγο αρκετά από αυτά καλούνται να συμμορφώνονται σε διεθνή πρότυπα και απαιτήσεις ανάλογα με τη σημαία. Τα συστήματα αυτά αναφέρθηκαν σε προηγούμενο κεφάλαιο σε συνδυασμό με τα τρωτά σημεία του πλοίου.

3.5 Η στρατηγική της Ε.Ε για την ασφάλεια στη θάλασσα

Οι αρχές που καθορίζουν την πολιτική για την κυβερνοασφάλεια στην Ε.Ε καθορίστηκαν το 2013 και είναι οι εξής:

- Επίτευξη άμυνας ενάντια σε απειλές στον κυβερνοχώρο.
- Μείωση του κυβερνοεγκλήματος.
- Ανάπτυξη πολιτικής άμυνας στον κυβερνοχώρο.
- Ανάπτυξη των βιομηχανικών και τεχνολογικών πηγών για την κυβερνοασφάλεια.
- Εγκαθίδρυση και παγίωση μιας συνεκτικής διεθνούς πολιτικής κυβερνοχώρου από την Ε.Ε και προώθηση βασικών αξιών.

Κάποιες από τις ανωτέρω αρχές συνοδεύτηκαν από νομοθετικά εργαλεία και μετατράπηκαν σε κανόνες.

Η αρχή της ανθεκτικότητας στον κυβερνοχώρο μετατράπηκε στον κανονισμό 526/2013 και στην οδηγία 2016/1148 όπου παρουσιάζονται μέτρα για ένα κοινό υψηλό επίπεδο ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών εντός της Ένωσης.

Η αρχή για την μείωση του εγκλήματος στον κυβερνοχώρο μετατράπηκε σε τρεις οδηγίες, για την αντιμετώπιση σεξουαλικής κακοποίησης και παιδικής πορνογραφίας, για αντιμετώπιση επιθέσεων εναντίον συστημάτων πληροφοριών και για την αντιμετώπιση απατών όπως πλαστογραφία μη ταμειακών μέσων πληρωμής.

Η Ευρωπαϊκή Στρατηγική Ασφαλείας για τη Θάλασσα παρέχει το στρατηγικό πλαίσιο σε συνδυασμό με τις πολιτικές αντιμετώπισης των ζητημάτων ασφαλείας που είναι δυνατό να εμφανιστούν. Το αντικείμενο της στρατηγικής είναι η προστασία των συμφερόντων θαλάσσιας ασφαλείας της Ε.Ε , οι συγκεκριμένες στρατηγικές έχουν τα ακόλουθα πεδία εφαρμογής:

1. Εξωτερική δράση.
2. Ανάπτυξη δυνατοτήτων.
3. Ευαισθητοπο.ίηση θεμάτων που αφορούν τη θάλασσα.
4. Παρακολούθηση και διαμοιρασμός της πληροφορίας.
5. Διαχείριση κινδύνου και προστασία θαλάσσιων υποδομών.
6. Εκπαίδευση, κατάρτιση και θαλάσσια έρευνα.

Στην συγκεκριμένη στρατηγική περιλαμβάνονται οι κίνδυνοι και απειλές που έχουν καταγραφεί στη θάλασσα και αναπτύσσεται Σχέδιο Δράσης της Στρατηγικής της Ε.Ε.

Κεφάλαιο 4: Μέτρα αντιμετώπισης κυβερνοεπίθεσης

4.1 Ανάπτυξη μέτρων προστασίας

Τα κρίσιμα συστήματα του πλοίου καθώς και τα δεδομένα είναι σημαντικό να προστατεύονται με πολλαπλά επίπεδα προστατευτικών μέτρων. Τα μέτρα αυτά οφείλουν να εξετάζουν τον ρόλο του προσωπικού, των διαδικασιών και της τεχνολογίας έτσι ώστε να αυξηθεί η πιθανότητα ανίχνευσης περιστατικού στον κυβερνοχώρο σε συνδυασμό με την βέλτιστη αξιοποίηση των πόρων που απαιτούνται για την προστασία του απορρήτου και την ακεραιότητα της διαθεσιμότητας δεδομένων σε συστήματα *IT* και *OT*. Τα συστήματα *OT* που είναι συνδεδεμένα στο διαδίκτυο απαιτούν περισσότερα του ενός τεχνικά και διαδικαστικά μέτρα προστασίας. Οι περιμετρικές άμυνες όπως το τείχος προστασίας *(firewall)* είναι σημαντικές για την πρόληψη ανεπιθύμητης εισόδου στο σύστημα, βέβαια αυτές οι άμυνες δεν μπορούν να αντιμετωπίσουν εσωτερικές απειλές.

4.1.1 Άμυνα σε βάθος

Η συγκεκριμένη προσέγγιση προστασίας περιλαμβάνει έναν συνδυασμό από μέτρα και διαδικασίες τα οποία παρουσιάζονται παρακάτω.

1. Ύπαρξη φυσικής ασφάλειας στο πλοίο η οποία λειτουργεί σύμφωνα με το Σύστημα Ασφαλείας του Πλοίου *(SSP)*
2. Αποτελεσματική κατάτμηση των δικτύων και προστασία τους
3. Ανίχνευση εισβολής
4. Χρήση τείχους προστασίας *(firewall)*
5. Περιοδικός έλεγχος των τρωτών σημείων του πλοίου
6. Λίστα επιτρεπόμενων λογισμικών
7. Έλεγχος πρόσβασης χρήστη
8. Στοιχεία ελέγχου διαχείρισης διαμόρφωσης και πιθανών αλλαγών
9. Κατάλληλες διαδικασίες για την χρήση κωδικών πρόσβασης και οδηγίες για την χρήση αφαιρούμενων μέσων
10. Ενημέρωση και εκπαίδευση του προσωπικού για τους κινδύνους για την προσωπική τους ασφάλεια αλλά και της εταιρείας από ενδεχόμενη κυβερνοεπίθεση
11. Κατανόηση και εξοικείωση με τις κατάλληλες διαδικασίες συμπεριλαμβανομένης της αντιμετώπισης περιστατικών παραβίασης

Οι πολιτικές ασφαλείας σε συνδυασμό με τις δράσεις της εταιρείας θα πρέπει να συμβάλλουν στη μέγιστη επίτευξη ασφάλειας στον κυβερνοχώρο με μια συνολική προσέγγιση στη διαχείριση κινδύνων ασφάλειας και προστασίας. Η πολυπλοκότητα και η πιθανή επιμονή των απειλών στον κυβερνοχώρο σημαίνει ότι πρέπει να εξεταστεί μια προσέγγιση «άμυνας σε βάθος». Ο εξοπλισμός και τα δεδομένα πρέπει να προστατεύονται από διαφορετικά επίπεδα μέτρων προστασίας όποτε να είναι πιο ανθεκτικά σε κυβερνοεπιθέσεις.

4.1.2 Άμυνα σε πλάτος

Κατά την ανάπτυξη και ολοκλήρωση της διασύνδεσης μεταξύ συστημάτων του πλοίου είναι σημαντικό να καθορίζεται ένα όριο εμπιστοσύνης όπου τα συστήματα ομαδοποιούνται μεταξύ εκείνων που η εμπιστοσύνη πρέπει να είναι σιωπηρή (για παράδειγμα χρήστης και σταθμό εργασίας) και εκείνων όπου η εμπιστοσύνη πρέπει να είναι σαφή(για παράδειγμα μεταξύ υπολογιστών γέφυρας και εταιρικά συστήματα εκτός πλοίου). Για πολύπλοκα και μεγάλα

δίκτυα δημιουργείται μια μοντελοποίηση των απειλών όπου εφαρμόζονται τεχνικοί έλεγχοι μεταξύ συστημάτων προκειμένου να υποστηρίζεται άμυνα ευρείας κλίμακας.

Στα πλοία όπου το επίπεδο διασύνδεσης των συστημάτων *IT* και *OT* είναι υψηλό για να εφαρμοστεί η άμυνα σε βάθος είναι απαραίτητη η εφαρμογή διαδικαστικών και τεχνικών μέτρων προστασίας σε διαφορετικά επίπεδα σε όλα τα τρωτά σημεία του πλοίου, αυτή είναι η «άμυνα σε πλάτος» και χρησιμοποιείται για την πρόληψη οποιασδήποτε ευπάθειας σε ένα σύστημα που χρησιμοποιείται για την παράκαμψη μέτρων προστασίας ενός άλλου συστήματος.

Η *άμυνα σε βάθος* και *η άμυνα στο πλάτος* είναι συμπληρωματικές προσεγγίσεις, οι οποίες, όταν εφαρμόζονται μαζί, παρέχουν τη βάση μιας ολιστικής απάντησης στη διαχείριση των κινδύνων στον κυβερνοχώρο. Η προτεραιότητα του τμήματος ασφαλείας οφείλει να είναι η εφαρμογή των ελέγχων στον κυβερνοχώρο, εστιάζοντας κυρίως στην εφαρμογή μέτρων ή συνδυασμούς μέτρων που αποφέρουν το μέγιστο αποτέλεσμα. Φυσικά, όλα τα συστήματα μπορούν να προστατευτούν αλλά σε ορισμένες περιπτώσεις, η δαπάνη σε χρόνο και χρήμα είναι πολύ μεγαλύτερη από τον κίνδυνο μιας επίθεσης.

4.2 Μέτρα τεχνικής προστασίας

Το κέντρο ασφάλειας στο διαδίκτυο *Center of Internet Security*[5] παρέχει κατευθυντήριες οδηγίες για τα μέτρα τεχνικής προστασίας τα οποία μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των τρωτών σημείων της κυβερνοασφάλειας στα πλοία. Τα μέτρα προστασίας έχουν δημοσιευτεί σε λίστα από τον οργανισμό *Center of Internet Security* με τίτλο *Critical Security Controls (CSC)*. Στην συγκεκριμένη λίστα δίνονται οι απαιτούμενες προτεραιότητες και ελέγχονται τα μέτρα ώστε να διασφαλιστεί πως παρέχουν την απαιτούμενη αποτελεσματική προσέγγιση στις εταιρείες ώστε να έχουν τη δυνατότητα αξιολόγησης και βελτίωσης της άμυνας τους. Τα *CSC* περιλαμβάνουν τεχνικές και διαδικαστικές πτυχές που παρουσιάζονται παρακάτω στους 20 ελέγχους που περιλαμβάνει η συγκεκριμένη λίστα. Οι έλεγχοι βασίζονται στις πρόσφατες πληροφορίες σχετικά με τις συνηθέστερες επιθέσεις και αντικατοπτρίζουν την συνδυασμένη γνώση εμπορικών εμπειρογνωμόνων, μεμονωμένων ελεγκτών και συνεργατών από κυβερνητικές υπηρεσίες των Η.Π.Α.

[5] https://www.cisecurity.org/controls/

1. Κατάλογος εξουσιοδοτημένων και μη συσκευών

Οι οργανισμοί πρέπει να διαχειρίζονται ενεργά όλες τις *hardware* συσκευές στο δίκτυο, έτσι ώστε να παρέχεται πρόσβαση μόνο σε εξουσιοδοτημένες συσκευές και οι μη εξουσιοδοτημένες συσκευές να μπορούν να αναγνωριστούν και να αποσυνδεθούν γρήγορα πριν προκαλέσουν οποιαδήποτε βλάβη.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι σαρώνουν συνεχώς τον χώρο διευθύνσεων των οργανισμών, περιμένοντας να συνδεθούν νέα και απροστάτευτα συστήματα στο δίκτυο. Αυτός ο έλεγχος είναι ιδιαίτερα σημαντικός για οργανισμούς που επιτρέπουν το *BYOD*[6], αφού οι *hackers* αναζητούν συγκεκριμένα συσκευές που συνδέονται και αποσυνδέονται από το δίκτυο της επιχείρησης.

2. Κατάλογος εξουσιοδοτημένων και μη λογισμικών συστημάτων

Οι οργανισμοί πρέπει να διαχειρίζονται ενεργά όλο το λογισμικό που χρησιμοποιούν, έτσι ώστε να εγκαθίσταται μόνο εξουσιοδοτημένο λογισμικό. Τα μέτρα ασφαλείας όπως η λίστα επιτρεπόμενων εφαρμογών μπορούν να επιτρέψουν στους οργανισμούς να βρουν γρήγορα μη εξουσιοδοτημένο λογισμικό προτού εγκατασταθεί.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι αναζητούν ευάλωτες εκδόσεις λογισμικού το οποίο μπορεί να χρησιμοποιηθεί από απόσταση. Μία από τις συνηθέστερες εγκληματικές δραστηριότητες τους είναι να διανείμουν εχθρικές ιστοσελίδες, αρχεία πολυμέσων και άλλο περιεχόμενο ή να χρησιμοποιούν εκμεταλλεύσεις *zero-days*[7] που εκμεταλλεύονται άγνωστα μέχρι εκείνη τη στιγμή τρωτά σημεία του πλοίου και του δικτύου. Επομένως, η σωστή γνώση του λογισμικού που χρησιμοποιείται στην εταιρεία και το πλοίο είναι απαραίτητη για την ασφάλεια και το απόρρητο των δεδομένων.

[6] *Bring your own device*

[7] Ορολογία που χρησιμοποιείται για τύπο ευπάθειας ή τρωτού σημείου που είναι άγνωστα μέχρι εκείνη τη στιγμή σφάλματα του λογισμικού

3. Ασφαλείς ρυθμίσεις παραμέτρων για υπολογιστικά συστήματα και λογισμικά

Οι εταιρείες πρέπει να δημιουργήσουν, να εφαρμόσουν και να διαχειριστούν τη διαμόρφωση ασφαλείας φορητών υπολογιστών, διακομιστών και σταθμών εργασίας. Οι εταιρείες πρέπει να ακολουθούν αυστηρή διαχείριση διαμόρφωσης και να εφαρμόζουν διαδικασίες ελέγχου αλλαγών για να αποτρέψουν τους επιτιθέμενους από την εκμετάλλευση ευάλωτων υπηρεσιών και ρυθμίσεων.

Γιατί είναι σημαντικό;

Οι κατασκευαστές και οι μεταπωλητές σχεδιάζουν τις προεπιλεγμένες ρυθμίσεις παραμέτρων λειτουργικών συστημάτων και εφαρμογών για ευκολία στην ανάπτυξη και χρήση, όχι για ισχυρή ασφάλεια. Οι ανοιχτές υπηρεσίες και οι θύρες, καθώς και οι προεπιλεγμένοι λογαριασμοί ή κωδικοί πρόσβασης μπορούν να αξιοποιηθούν στην προεπιλεγμένη τους κατάσταση, οπότε οι εταιρείες πρέπει να αναπτύξουν ρυθμίσεις παραμέτρων με αυξημένες ιδιότητες ασφαλείας.

4. Συνεχής εκτίμηση των τρωτών σημείων και αποκατάσταση αυτών

Οι οργανισμοί πρέπει συνεχώς να αποκτούν, να αξιολογούν και να λαμβάνουν μέτρα για νέες πληροφορίες (π.χ. ενημερώσεις λογισμικού, επιδιορθώσεις, συμβουλές ασφαλείας και δελτία απειλών) για τον εντοπισμό και την αποκατάσταση των τρωτών σημείων που θα μπορούσαν να χρησιμοποιήσουν οι επιτιθέμενοι για να διεισδύσουν στα δίκτυά τους.

Γιατί είναι σημαντικό;

Από την πρώτη στιγμή που οι ερευνητές αναφέρουν νέα τρωτά σημεία, ξεκινά ένας αγώνας μεταξύ όλων των σχετικών μερών: Οι επιτιθέμενοι προσπαθούν να χρησιμοποιήσουν την ευπάθεια για μια επίθεση, οι προμηθευτές αναπτύσσουν επιδιορθώσεις ή ενημερώσεις και οι υπεύθυνοι ασφαλείας αρχίζουν να πραγματοποιούν αξιολογήσεις κινδύνου ή ανάδρομες δοκιμές. Οι επιτιθέμενοι έχουν πρόσβαση στις ίδιες πληροφορίες για όλους τους άλλους και μπορούν να επωφεληθούν από τα κενά μεταξύ της εμφάνισης νέας γνώσης και της αποκατάστασης.

5. Ελεγχόμενη χρήση διοικητικών προνομίων

Αυτός ο έλεγχος απαιτεί από τις εταιρείες να χρησιμοποιούν αυτοματοποιημένα εργαλεία για την παρακολούθηση της συμπεριφοράς των χρηστών και την παρακολούθηση του τρόπου

εκχώρησης και χρήσης των διαχειριστικών δικαιωμάτων, προκειμένου να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα συστήματα.

Γιατί είναι σημαντικό;

Η κατάχρηση διοικητικών προνομίων είναι η κύρια μέθοδος εξάπλωσης της επίθεσης σε μια επιχείρηση. Για να αποκτήσουν τα διαπιστευτήρια του διαχειριστή χρησιμοποιήσουν τεχνικές ηλεκτρονικού "ψαρέματος" ενώ προσπαθούν να σπάσουν ή να μαντέψουν τον κωδικό πρόσβασης για έναν χρήστη που έχει τα προνόμια του διαχειριστή ή να αυξήσουν τα προνόμια ενός κανονικού λογαριασμού χρήστη σε λογαριασμό διαχειριστή. Εάν οι οργανισμοί δεν διαθέτουν πόρους για να παρακολουθούν τι συμβαίνει στο περιβάλλον πληροφορικής τους, είναι ευκολότερο για τους επιτιθέμενους να αποκτήσουν τον πλήρη έλεγχο των συστημάτων τους.

6. Συντήρηση και παρακολούθηση αρχείων καταγραφής ελέγχου

Οι οργανισμοί πρέπει να συλλέγουν, να διαχειρίζονται και να αναλύουν αρχεία καταγραφής συμβάντων για να εντοπίζουν παρεκκλίνουσες δραστηριότητες και να ερευνούν περιστατικά ασφαλείας.

Γιατί είναι σημαντικό;

Η έλλειψη καταγραφής και ανάλυσης ασφαλείας επιτρέπει στους επιτιθέμενους να αποκρύψουν τη θέση και τις δραστηριότητές τους στο δίκτυο. Ακόμα κι αν η οργάνωση -θύμα γνωρίζει ποια συστήματα έχουν υπονομευτεί, χωρίς την πλήρη εγγραφή καταγραφής θα είναι δύσκολο για αυτούς να καταλάβουν το είδος και εύρος της επίθεσης και να ανταποκριθούν αποτελεσματικά στο περιστατικό ασφαλείας.

7. Προστασία ηλεκτρονικού ταχυδρομείου και των προγραμμάτων περιήγησης

Οι οργανισμοί καλούνται να διασφαλίσουν την χρησιμοποίηση μόνο πλήρως υποστηριζόμενων προγραμμάτων περιήγησης ιστού καθώς και προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου προκειμένου να ελαχιστοποιηθεί η πιθανότητα επίθεσης σε αυτά.

Γιατί είναι σημαντικό;

Τα προγράμματα περιήγησης στο διαδίκτυο και τα προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου είναι πολύ συνηθισμένα σημεία εισόδου για τους *hackers* λόγω της υψηλής τεχνικής πολυπλοκότητας και ευελιξίας τους. Οι επιτιθέμενοι μπορούν να δημιουργήσουν

περιεχόμενο και να εξαπατήσουν τους χρήστες ώστε να προβούν σε ενέργειες που μπορούν να εισαγάγουν κακόβουλο κώδικα και να οδηγηθούν σε απώλεια πολύτιμων δεδομένων.

8. Προστασία από κακόβουλο λογισμικό (malware)

Οι οργανισμοί πρέπει να βεβαιωθούν ότι μπορούν να ελέγξουν την εγκατάσταση και την εκτέλεση κακόβουλου κώδικα σε πολλά σημεία της επιχείρησης. Αυτό το στοιχείο ελέγχου συνιστά τη χρήση αυτοματοποιημένων εργαλείων για τη συνεχή παρακολούθηση των σταθμών εργασίας, των διακομιστών και των κινητών συσκευών με *anti-virus, anti-spyware, firewalls* και λειτουργίες *host based IPS (HIPS)* που βασίζονται σε κεντρικούς υπολογιστές.

Γιατί είναι σημαντικό;

Το σύγχρονο κακόβουλο λογισμικό μπορεί να κινείται γρήγορα και ταυτόχρονα ενώ μπορεί να εισέλθει μέσω οποιουδήποτε τρωτού σημείου του συστήματος. Επομένως, οι άμυνες κακόβουλου λογισμικού πρέπει να μπορούν να λειτουργούν σε αυτό το δυναμικό περιβάλλον μέσω αυτοματισμού μεγάλης κλίμακας, ενημέρωσης και ολοκλήρωσης με διαδικασίες όπως η ενεργοποίηση της διαδικασίας απόκρισης περιστατικού ασφαλείας.

9. Περιορισμός και έλεγχος των θυρών του δικτύου , πρωτοκόλλων και υπηρεσιών

Οι οργανισμοί πρέπει να παρακολουθούν και να διαχειρίζονται τη χρήση θυρών, πρωτοκόλλων και υπηρεσιών σε συσκευές δικτύου για να ελαχιστοποιήσουν τα παράθυρα ευπάθειας που διατίθενται στους εισβολείς.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι αναζητούν υπηρεσίες δικτύου από απόσταση που αποτελούν τρωτά σημεία του πλοίου και δίνουν τη δυνατότητα στους επιτιθέμενους να εκμεταλλευτούν τα τρωτά σημεία. Τα συνήθη παραδείγματα περιλαμβάνουν διακομιστές ιστού, διακομιστές αλληλογραφίας και υπηρεσίες αρχείων και εκτύπωσης, καθώς και διακομιστές συστήματος ονομάτων τομέα[8] *(DNS)* που είναι εγκατεστημένοι από προεπιλογή σε διάφορες συσκευές. Επομένως, είναι ζωτικής σημασίας ο υπεύθυνος ασφαλείας να βεβαιωθεί ότι μόνο θύρες, πρωτόκολλα και υπηρεσίες με επικυρωμένα πιστοποιητικά να εκτελούνται σε κάθε σύστημα.

[8] *Domain name system*

10. Δυνατότητα ανάκτησης δεδομένων

Οι εταιρείες πρέπει να διασφαλίσουν ότι για τα κρίσιμα συστήματα και τα σημαντικά δεδομένα να δημιουργούνται τα κατάλληλα αντίγραφα ασφαλείας, τουλάχιστον σε εβδομαδιαία βάση. Επίσης είναι αναγκαία η ύπαρξη αποδεδειγμένης μεθοδολογίας για την έγκαιρη ανάκτηση των δεδομένων.

Γιατί είναι σημαντικό;

Στις περισσότερες επιθέσεις οι επιτιθέμενοι όταν αποκτούν πρόσβαση σε συστήματα της εταιρείας προβαίνουν συχνά σε αλλαγές σε δεδομένα, σε ρυθμίσεις παραμέτρων των συστημάτων και σε αλλαγές σε ρυθμίσεις του λογισμικού. Χωρίς αξιόπιστη δημιουργία αντιγράφων και διαδικασία ανάκτησης καθίσταται αρκετά δύσκολη η διαδικασία ανάκαμψης για τις πληγέντες εταιρείες.

11. Ασφαλείς διαμορφώσεις για τις συσκευές δικτύου

Οι οργανισμοί πρέπει να δημιουργήσουν, να εφαρμόσουν και να διαχειριστούν ενεργά τη διαμόρφωση ασφαλείας των συσκευών υποδομής δικτύου, όπως δρομολογητές *(routers)* , τείχη προστασίας *(firewalls)* και διακόπτες *(switches).*

Γιατί είναι σημαντικό;

Όπως και με τα λειτουργικά συστήματα και τις εφαρμογές (βλ. Μέτρο 3), οι προεπιλεγμένες διαμορφώσεις και ρυθμίσεις παραμέτρων για συσκευές υποδομής δικτύου είναι προσανατολισμένες στην ευκολία της ανάπτυξης και στην ασφάλεια. Επιπλέον, οι συσκευές δικτύου συχνά διαμορφώνονται λιγότερο ασφαλώς, οπότε με την πάροδο του χρόνου οι επιτιθέμενοι εκμεταλλεύονται αυτά τα ελαττώματα διαμόρφωσης για να αποκτήσουν πρόσβαση σε δίκτυα ή να χρησιμοποιήσουν ένα μηχανογραφικό μηχάνημα ώστε να θέσουν ως αξιόπιστο ένα δικό τους σύστημα.

12. *Boundary defense* (οριακή άμυνα)

Οι οργανισμοί πρέπει να εντοπίσουν και να διορθώσουν τη ροή πληροφοριών μεταξύ δικτύων διαφορετικών επιπέδων εμπιστοσύνης, με έμφαση στα δεδομένα που θα μπορούσαν να βλάψουν την ασφάλεια. Η καλύτερη άμυνα είναι οι τεχνολογίες που παρέχουν βαθιά ορατότητα και έλεγχο της ροής δεδομένων σε όλο το περιβάλλον, όπως συστήματα ανίχνευσης εισβολών και πρόληψης εισβολών.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι συχνά χρησιμοποιούν αδυναμίες διαμόρφωσης και αρχιτεκτονικής σε περιμετρικά συστήματα, συσκευές δικτύου και μηχανήματα-πελάτες με πρόσβαση στο διαδίκτυο για να αποκτήσουν αρχική πρόσβαση στο δίκτυο ενός οργανισμού.

13. Προστασία δεδομένων

Οι οργανισμοί πρέπει να χρησιμοποιούν κατάλληλες διαδικασίες και εργαλεία για τον μετριασμό του κινδύνου διαφυγής- απώλειας δεδομένων και τη διασφάλιση της ακεραιότητας των ευαίσθητων πληροφοριών. Η προστασία των δεδομένων επιτυγχάνεται καλύτερα μέσω του συνδυασμού τεχνικών κρυπτογράφησης, προστασίας της ακεραιότητας και πρόληψης απώλειας δεδομένων.

Γιατί είναι σημαντικό;

Ενώ πολλές διαρροές δεδομένων είναι σκόπιμη κλοπή, άλλες περιπτώσεις απώλειας ή ζημιάς δεδομένων είναι αποτέλεσμα κακών πρακτικών ασφαλείας ή ανθρώπινων λαθών. Για να ελαχιστοποιηθούν αυτοί οι κίνδυνοι, οι οργανισμοί πρέπει να εφαρμόσουν λύσεις που μπορούν να βοηθήσουν στην ανίχνευση της διείσδυσης δεδομένων και να μετριάσουν τις επιπτώσεις του συμβιβασμού δεδομένων.

14. Ελεγχόμενη πρόσβαση

Οι οργανισμοί πρέπει να είναι σε θέση να παρακολουθούν, να ελέγχουν και να εξασφαλίζουν πρόσβαση στα κρίσιμα περιουσιακά τους στοιχεία και να καθορίζουν εύκολα ποια άτομα, υπολογιστές ή εφαρμογές έχουν δικαίωμα πρόσβασης σε αυτά τα στοιχεία.

Γιατί είναι σημαντικό;

Ορισμένοι οργανισμοί δεν εντοπίζουν και διαχωρίζουν τα πιο κρίσιμα περιουσιακά τους στοιχεία από τα λιγότερο ευαίσθητα δεδομένα γεγονός που έχει ως επακόλουθο να υπάρχουν χρήστες που έχουν πρόσβαση σε πιο ευαίσθητα δεδομένα από αυτά που χρειάζονται για να κάνουν τη δουλειά τους. Ως αποτέλεσμα, είναι ευκολότερο για έναν κακόβουλο μυημένο - ή έναν εισβολέα ή κακόβουλο λογισμικό που αναλαμβάνει τον λογαριασμό του - να κλέψει σημαντικές πληροφορίες ή να διακόψει τις λειτουργίες σημαντικών υπολογιστικών συστημάτων.

15. Έλεγχος ασύρματης πρόσβασης

Οι οργανισμοί πρέπει να διαθέτουν διαδικασίες και εργαλεία για την παρακολούθηση και τον έλεγχο της χρήσης ασύρματων τοπικών δικτύων *(LAN),* σημείων πρόσβασης και ασύρματων συστημάτων πελατών. Πρέπει να διενεργούν ελέγχους σάρωσης ευπάθειας δικτύου με τα κατάλληλα εργαλεία και να διασφαλίζουν ότι όλες οι ασύρματες συσκευές που είναι συνδεδεμένες στο δίκτυο πληρούν τις προϋποθέσεις που θέτει ένα εξουσιοδοτημένο προφίλ διαμόρφωσης και ασφάλειας.

Γιατί είναι σημαντικό;

Οι ασύρματες συσκευές είναι ένας από τους φορείς που επιδιώκουν πρωτίστως οι επιτιθέμενοι ώστε να διατηρούν μακροπρόθεσμη πρόσβαση στο περιβάλλον *IT*, καθώς δεν απαιτούν άμεση φυσική σύνδεση. Για παράδειγμα, οι συσκευές *wireless clients* που χρησιμοποιούνται από τους εργαζόμενους κατά τη μετακίνησή τους μολύνονται σε τακτική βάση και αργότερα χρησιμοποιούνται ως πίσω πόρτες όταν επανασυνδέονται στο δίκτυο του οργανισμού.

16. Παρακολούθηση και έλεγχος λογαριασμού

Είναι ζωτικής σημασίας για τους οργανισμούς να διαχειρίζονται ενεργά τον κύκλο ζωής των λογαριασμών χρηστών (δημιουργία, χρήση και διαγραφή) για να ελαχιστοποιήσουν τις ευκαιρίες στους επιτιθέμενους να τους αξιοποιήσουν. Όλοι οι λογαριασμοί του συστήματος πρέπει να επανεξετάζονται τακτικά ενώ οι λογαριασμοί πρώην εργολάβων και υπαλλήλων πρέπει να απενεργοποιούνται μόλις το άτομο αποχωρήσει από την εταιρεία.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι συχνά εκμεταλλεύονται ανενεργούς λογαριασμούς χρηστών για να αποκτήσουν νόμιμη πρόσβαση στα υπολογιστικά συστήματα του οργανισμού, γεγονός που καθιστά τον εντοπισμό της επίθεσης πιο δύσκολη.

17. Αξιολόγηση δεξιοτήτων ασφαλείας και κατάλληλη εκπαίδευση για την κάλυψη των κενών

Οι οργανισμοί πρέπει να προσδιορίσουν τις συγκεκριμένες γνώσεις και δεξιότητες που χρειάζεται το προσωπικό τους για να ενισχύσουν την ασφάλεια. Αυτό απαιτεί την ανάπτυξη και εκτέλεση ενός σχεδίου για τον εντοπισμό των κενών και τη διόρθωσή τους μέσω προγραμμάτων πολιτικής, σχεδιασμού και κατάρτισης.

Γιατί είναι σημαντικό;

Είναι δελεαστικό να σκεφτούμε την κυβερνοάμυνα ως μια κυρίως τεχνική πρόκληση. Ωστόσο, οι ενέργειες των εργαζομένων είναι επίσης κρίσιμες για την επιτυχία ενός προγράμματος ασφαλείας. Οι επιτιθέμενοι χρησιμοποιούν συχνά τον ανθρώπινο παράγοντα για να σχεδιάσουν εκμεταλλεύσεις, για παράδειγμα, δημιουργώντας προσεκτικά μηνύματα ηλεκτρονικού ψαρέματος που μοιάζουν με κανονικά μηνύματα ηλεκτρονικού ταχυδρομείου ή δουλεύοντας εντός του χρονικού διαστήματος της ενημέρωσης κώδικα ή του ελέγχου καταγραφής.

18. Ασφάλεια λογισμικού εφαρμογών

Οι οργανισμοί πρέπει να διαχειρίζονται τον κύκλο ζωής ασφάλειας όλων των λογισμικών που χρησιμοποιούν προκειμένου να εντοπίζουν και να διορθώνουν όποιες αδυναμίες ασφαλείας εμφανίζονται. Συγκεκριμένα, πρέπει να ελέγχουν τακτικά ότι χρησιμοποιούν μόνο τις πιο πρόσφατες εκδόσεις κάθε εφαρμογής και ότι εγκαθίστανται άμεσα όλες οι σχετικές ενημερώσεις κώδικα

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι συχνά εκμεταλλεύονται τα τρωτά σημεία σε εφαρμογές που βασίζονται στον ιστό και άλλο λογισμικό. Μπορούν να εισάγουν συγκεκριμένα *exploits* [9] , συμπεριλαμβανομένων υπερχειλίσεων *buffer,* επιθέσεων έγχυσης *SQL*, δέσμης ενεργειών μεταξύ τοποθεσιών και επιθέσεων τύπου *click-jacking* [10], για να αποκτήσουν έλεγχο σε ευάλωτα μηχανήματα.

19. Αντιμετώπιση και διαχείριση περιστατικών

Οι οργανισμοί πρέπει να αναπτύξουν και να εφαρμόσουν τα κατάλληλα πρωτόκολλα αντιμετώπισης περιστατικών, τα οποία περιλαμβάνουν σχέδια και καθορισμένους ρόλους, εκπαίδευση, εποπτεία διαχείρισης και άλλα μέτρα που θα βοηθήσουν το προσωπικό

[9] Ακολουθία εντολών που εκμεταλλεύεται ένα σφάλμα ή μια ευπάθεια που προκαλεί ακούσια ή απρόβλεπτη συμπεριφορά σε λογισμικό υπολογιστή

[10] Κακόβουλη τεχνική εξαπάτησης ενός χρήστη όπου κάνει κλικ σε κάτι διαφορετικό από αυτό που αντιλαμβάνεται, αποκαλύπτοντας με αυτόν τον τρόπο εμπιστευτικές πληροφορίες

ασφαλείας να ανακαλύψει επιθέσεις και να περιορίσει αποτελεσματικότερα τις ζημιές μιας εγκληματικής ενέργειας.

Γιατί είναι σημαντικό;

Τα περιστατικά ασφαλείας αποτελούν πλέον ένα φυσιολογικό κομμάτι της πραγματικότητας. Ακόμη και μεγάλες και καλά χρηματοδοτούμενες επιχειρήσεις αγωνίζονται να συμβαδίσουν με το εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο. Δυστυχώς, στις περισσότερες περιπτώσεις, η πιθανότητα επιτυχούς κυβερνοεπίθεσης δεν είναι "αν" αλλά "πότε". Χωρίς σχέδιο αντιμετώπισης περιστατικών, ένας οργανισμός μπορεί να μην ανακαλύψει μια επίθεση μέχρι αυτή να προκαλέσει σοβαρή ζημιά ή να είναι σε θέση να εξαλείψει την παρουσία του εισβολέα και να αποκαταστήσει την ακεραιότητα του δικτύου και των συστημάτων.

20. Στρατηγικός σχεδιασμός *(Red team exercise)*

Ο τελικός έλεγχος απαιτεί από τους οργανισμούς να αξιολογήσουν τη συνολική ισχύ των αμυνών τους (την τεχνολογία, τις διαδικασίες και τους ανθρώπους) πραγματοποιώντας τακτικές εξωτερικές και εσωτερικές δοκιμές αντιμετώπισης κυβερνοεπίθεσης. Αυτό θα τους επιτρέψει να εντοπίσουν τα τρωτά σημεία και να αναγνωρίσουν επίθεση που μπορεί να χρησιμοποιηθεί από *exploits* για την εκμετάλλευση υπολογιστικών συστημάτων του οργανισμού.

Γιατί είναι σημαντικό;

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν το χάσμα μεταξύ του σχεδιασμού άμυνας του οργανισμού και υλοποίησής του, όπως το χρονικό διάστημα μεταξύ της ανακοίνωσης ενός τρωτού σημείου, της διαθεσιμότητας μιας αναβάθμισης από τον προμηθευτή *(vendor patch)* και της εγκατάστασης ενημερωμένης έκδοσης κώδικα. Σε ένα πολύπλοκο περιβάλλον όπου η τεχνολογία εξελίσσεται συνεχώς, οι οργανισμοί θα πρέπει να δοκιμάζουν περιοδικά την άμυνά τους για να εντοπίζουν κενά και να τα διορθώνουν πριν από μια ενδεχόμενη κυβερνοεπίθεση.

4.3 Διαδικαστικά μέτρα προστασίας

Οι διαδικαστικοί έλεγχοι επικεντρώνονται στον τρόπο με τον οποίο το προσωπικό χρησιμοποιεί τα ενσωματωμένα συστήματα. Σχέδια και διαδικασίες που περιέχουν ευαίσθητες πληροφορίες που πρέπει να διατηρούνται εμπιστευτικές και να χειρίζονται σύμφωνα με την σαφείς εταιρικές πολιτικές. Παραδείγματα διαδικαστικών ενεργειών μπορεί να είναι τα εξής:

1. Εκπαίδευση και ευαισθητοποίηση

Η εκπαίδευση και ευαισθητοποίηση αποτελούν τα βασικά εργαλεία για την αποτελεσματική διαχείριση και αντιμετώπιση του κινδύνου στον κυβερνοχώρο. Η εσωτερική απειλή στον κυβερνοχώρο πρέπει να λαμβάνεται υπόψη, ότι προσωπικό της εταιρείας διαδραματίζει σημαντικό ρόλο στην προστασία πληροφοριακών συστημάτων καθώς και συστημάτων *OT*. Η εκπαίδευση και ευαισθητοποίηση του προσωπικού είναι σημαντική καθώς είναι σημαντική η αποφυγή λαθών όπως η χρησιμοποίηση αφαιρούμενων μέσων για την μεταφορά δεδομένων μεταξύ συστημάτων χωρίς προφύλαξη έναντι κακόβουλου λογισμικού. Η εκπαίδευση και ευαισθητοποίηση του προσωπικού αφορά και το προσωπικό του πλοίου, συμπεριλαμβανομένου και του πλοίαρχου αλλά και του προσωπικού της εταιρείας που βρίσκεται στα γραφεία της εταιρείας.

Αυτές οι κατευθυντήριες γραμμές υποθέτουν ότι και οι άλλοι κύριοι ενδιαφερόμενοι στην αλυσίδα εφοδιασμού, όπως οι ναυλωτές, οι νηογνώμονες και οι πάροχοι υπηρεσιών θα εφαρμόσουν τη δική τους βέλτιστη πρακτική στον κυβερνοχώρο όσον αφορά την προστασία και εκπαίδευση του προσωπικού τους. Ένα κατάλληλο πρόγραμμα εκπαίδευσης και ευαισθητοποίησης πρέπει να καλύπτει τουλάχιστον τις ακόλουθες προδιαγραφές:

- Κινδύνους που σχετίζονται με μηνύματα ηλεκτρονικού ταχυδρομείου καθώς και τους τρόπους ασφαλούς συμπεριφοράς. Επίσης παρουσίαση πιθανών επιθέσεων όπως phishing emails
- Κινδύνους που σχετίζονται με τη χρήση του διαδικτύου, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης, των *forums* συνομιλιών καθώς και τις διαδικασίες αποθήκευσης αρχείων στο *cloud* όπου η μεταφορά δεδομένων ελέγχεται λιγότερο ενώ δύναται να παρακολουθηθεί από τρίτους
- Κινδύνους που σχετίζονται με τη χρήση δικών τους συσκευών στις οποίες είναι πιθανόν να υπάρχουν κενά ασφαλείας, όπως μη ενημερωμένο λογισμικό ή έλλειψη επιδιορθώσεων ασφαλείας ή έλλειψη ενημερωμένου λογισμικού προστασίας από ιούς και κακόβουλο

λογισμικό. Το αποτέλεσμα είναι η μεταφορά του κινδύνου στα συστήματα του πλοίου όταν αυτές οι συσκευές συνδεθούν στο δίκτυο του πλοίου.

- Κινδύνους που σχετίζονται με την εγκατάσταση και συντήρηση λογισμικού στα υπολογιστικά συστήματα της εταιρείας, χρησιμοποιώντας αφαιρούμενα μέσα με μολυσμένο υλικό ή λογισμικό.
- Διασφάλιση των πληροφοριών χρήστη, κωδικών πρόσβασης και ψηφιακών πιστοποιητικών
- Κινδύνους διαδικτύου που σχετίζονται με την φυσική παρουσία μη εταιρικού προσωπικού, για παράδειγμα όταν τρίτα μέρη όπως τεχνικοί αφήνονται να εργαστούν σε εξοπλισμό του πλοίου χωρίς επίβλεψη
- Ανίχνευση ύποπτης δραστηριότητας ή ύποπτων συσκευών και διαδικασία αναφοράς ενός πιθανού περιστατικού στον κυβερνοχώρο
- Ευαισθητοποίηση σχετικά με τις συνέπειες και τον αντίκτυπο ενός περιστατικού κυβερνοεπίθεσης στην ασφάλεια και τις λειτουργίες του πλοίου
- Κατανόηση του τρόπου εφαρμογής της ρουτίνας των προληπτικών μέτρων και διαδικασιών συντήρησης, όπως η ρουτίνα διαδικασίας αντιγράφων ασφαλείας, ο σχεδιασμός δοκιμών αντιμετώπισης περιστατικών και η ρουτίνα ελέγχου σάρωσης λογισμικού για την ανίχνευση κακόβουλου λογισμικού και ιών
- Διαδικασίες προστασίας από κινδύνους που προκαλούνται από αφαιρούμενα μέσα παροχής υπηρεσιών πριν από τη σύνδεση τους στα υπολογιστικά συστήματα του πλοίου

Επιπλέον, το προσωπικό πρέπει να ενημερωθεί ότι η ύπαρξη λογισμικού προστασίας από κακόβουλο λογισμικό δεν καταργεί την απαίτηση για ισχυρές διαδικασίες ασφαλείας, για παράδειγμα τον έλεγχο της χρήσης όλων αφαιρούμενα μέσα. Επιπλέον, το κατάλληλο προσωπικό του πλοίου θα πρέπει να γνωρίζει τα σημάδια όταν ένας υπολογιστής έχει παραβιαστεί. Αυτό μπορεί να περιλαμβάνει τα ακόλουθα:

- Όταν ένα σύστημα αργεί να ανταποκριθεί στις εντολές του χρήστη ή δεν ανταποκρίνεται καθόλου
- Απρόσμενες αλλαγές κωδικού χρήστη ή αποκλεισμός πρόσβασης εξουσιοδοτημένων χρηστών

- Απροσδόκητα σφάλματα στα προγράμματα, συμπεριλαμβανομένης της αποτυχίας σωστής εκτέλεσης ή απροσδόκητη εκτέλεση προγραμμάτων
- Απροσδόκητες ή ξαφνικές αλλαγές στον διαθέσιμο αποθηκευτικό χώρο του συστήματος ή στην διαθέσιμη μνήμη
- Απροσδόκητη επιστροφή μηνυμάτων ηλεκτρονικού ταχυδρομείου
- Απροσδόκητες δυσκολίες σύνδεσης στο τοπικό δίκτυο ή στο διαδίκτυο
- Συχνές καταρρεύσεις του συστήματος
- Μη φυσιολογική δραστηριότητα του επεξεργαστή του συστήματος ή του σκληρού δίσκου αποθήκευσης
- Απροσδόκητες αλλαγές στον διακομιστή περιήγησης ή στις ρυθμίσεις χρήστη συμπεριλαμβανομένου τις άδειες πρόσβασης

Είναι ζωτικής σημασίας το υπεύθυνο προσωπικό ασφαλείας να είναι σε θέση να κατανοήσει τις αναφορές από τα συστήματα *IDS*[11] όταν αυτό χρησιμοποιείται. Ακολουθεί μια λίστα με πιθανά σημεία που είναι πιθανό να αντιμετωπιστούν σαν πιθανά περιστατικά κυβερνοεπίθεσης.

Πρόσβαση για τους επισκέπτες

Επισκέπτες όπως ελεγκτικές αρχές, τεχνικοί, πράκτορες, υπάλληλοι λιμένων και τερματικών και εκπρόσωποι ιδιοκτητών θα πρέπει να περιορίζονται όσον αφορά την πρόσβαση στον υπολογιστή όσο είναι εν πλω. Η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές δικτύου, ευαίσθητα συστήματα *OT* θα πρέπει να απαγορεύεται. Εάν απαιτείται πρόσβαση σε ένα δίκτυο από έναν επισκέπτη και επιτρέπεται, τότε θα πρέπει να περιοριστούν όσον αφορά τα δικαιώματα χρήστη. Πρόσβαση σε ορισμένα δίκτυα για λόγους συντήρησης θα πρέπει να εγκρίνεται πρώτα και έπειτα να συντονίζεται ακολουθώντας τις κατάλληλες διαδικασίες όπως περιγράφονται από την εταιρεία/διαχειριστή πλοίου. Στην περίπτωση που ένας επισκέπτης χρειάζεται πρόσβαση σε υπολογιστή ή εκτυπωτή αυτή πρέπει να γίνει σε σύστημα που δεν θα είναι συνδεδεμένο στο δίκτυο του πλοίου.

[11] Σύστημα ανίχνευσης εισβολής *(Intrusion Detection System)*

Ακολουθεί ένα παράδειγμα από τις οδηγίες *The Guidelines on Cyber Security Onboard Ships (IMO 2021)*

Ένα πλοίο ξηρού φορτίου στο λιμάνι είχε μόλις ολοκληρώσει τις εργασίες αποθήκευσης. Ο επιθεωρητής αποθήκης επιβιβάστηκε στο πλοίο και ζήτησε άδεια πρόσβασης σε υπολογιστή στο δωμάτιο ελέγχου κινητήρα για εκτύπωση εγγράφων για υπογραφή. Ο επιθεωρητής εισήγαγε μια μονάδα *USB* στον υπολογιστή και ταυτόχρονα εισήγαγε ακούσια κακόβουλο λογισμικό στο δίκτυο διαχείρισης του πλοίου. Το κακόβουλο λογισμικό παρέμεινε απαρατήρητο έως ότου πραγματοποιήθηκε προγραμματισμένη κυβερνοεκτίμηση στο πλοίο, ενώ το πλήρωμα είχε αναφέρει ένα "πρόβλημα υπολογιστή" που επηρεάζει το δίκτυο διαχείρισης του πλοίου. Αυτό το περιστατικό τονίζει την ανάγκη για διαδικασίες πρόληψης ή τον περιορισμό της χρήσης συσκευών *USB* επί του πλοίου, συμπεριλαμβανομένων αυτών

που ανήκουν σε επισκέπτες.

Αναβάθμιση και συντήρηση λογισμικού

Υπολογιστικά συστήματα καθώς και είδη λογισμικού τα οποία μετά την πάροδο χρονικού διαστήματος που δεν υποστηρίζονται από τον κατασκευαστή ή τον προγραμματιστή δεν λαμβάνουν πλέον τις απαραίτητες ενημερώσεις και αναβαθμίσεις για την αντιμετώπιση πιθανών τρωτών σημείων. Ως εκ τούτου η χρήση τέτοιων συστημάτων και υλικού για το οποίο έχει παρέλθει η τεχνική υποστήριξη οφείλει το τμήμα του πλοίου ή της εταιρείας που είναι υπεύθυνο για την ασφάλεια να αξιολογήσει προσεκτικά και να εκτιμήσει το μέγεθος του κινδύνου από την χρήση του. Οι σχετικές εγκαταστάσεις υπολογιστικών συστημάτων επί του πλοίου θα πρέπει να είναι πάντα ενημερωμένες ώστε να διατηρείται το επίπεδο ασφαλείας του πλοίου υψηλό. Πρέπει να θεσπιστούν διαδικασίες για την έγκαιρη ενημέρωση λογισμικού, λαμβάνοντας πάντα υπόψη τον τύπο του πλοίου, την ταχύτητα σύνδεσης στο διαδίκτυο, τον χρόνο ταξιδιού στη θάλασσα κ.α. Επίσης πρέπει να θεσπιστούν χρονοδιαγράμματα για τις ενημερώσεις λογισμικού.

Επιπλέον ένας αριθμός δρομολογητών *(routers)*, διακόπτες *(switches)*, τείχη προστασίας *(firewalls)* καθώς και διάφορες συσκευές *OT* εκτελούν δικό τους λογισμικό, το οποίο μπορεί να απαιτεί τακτική ενημέρωση και έτσι θα πρέπει να θεσπίζεται η κατάλληλη διαδικασία ανάλογα με τις απαιτήσεις του λογισμικού.

Η αποτελεσματική συντήρηση του λογισμικού εξαρτάται από τον προσδιορισμό, τον προγραμματισμό και την εκτέλεση των απαραίτητων μέτρων για την υποστήριξη δραστηριοτήτων συντήρησης καθ’ όλη τη διάρκεια του κύκλου ζωής του λογισμικού. Για να

διασφαλιστεί ότι έχει αναπτυχθεί η συντήρηση ασφάλειας και προστασίας του λογισμικού, καθορίζονται από τους υπεύθυνους ασφαλείας οι απαιτήσεις για όλους τους εμπλεκόμενους φορείς που εμπλέκονται στη συντήρηση λογισμικού εξοπλισμού πλοίων καθώς και των συνδεδεμένων ολοκληρωμένων συστημάτων. Το πρότυπο ασφαλείας που καθορίζεται καλύπτει την συντήρηση επί του σκάφους και του απομακρυσμένου λογισμικού από τα γραφεία της εταιρείας στην στεριά.

Η αναβάθμιση και ενημέρωση είναι πολύ σημαντική και για τα εργαλεία ανίχνευσης κακόβουλου λογισμικού και ιών, ως εκ τούτου είναι αναγκαία η θέσπιση πρότυπου χρονοδιαγράμματος αναβάθμισης τους και τακτικός έλεγχος σάρωσης.

Απομακρυσμένη πρόσβαση

Θα πρέπει να θεσπιστούν πολιτικές και διαδικασίες για τον έλεγχο της απομακρυσμένης πρόσβασης σε ενσωματωμένα *IT* και *OT* συστήματα. Οι σαφείς οδηγίες θα πρέπει να καθορίζουν ποιος έχει άδεια πρόσβασης, πότε μπορεί να έχει πρόσβαση και σε ποια συστήματα μπορεί να έχει πρόσβαση. Οποιεσδήποτε διαδικασίες που αφορούν την απομακρυσμένη πρόσβαση θα πρέπει να περιλαμβάνουν στενό συντονισμό με τον πλοίαρχο και τα ανώτερα στελέχη του πλοίου. Όλες οι εμφανίσεις απομακρυσμένης πρόσβασης θα πρέπει να καταγράφονται για έλεγχο σε περίπτωση διακοπής ενός *IT* ή του *OT* συστήματος. Τα συστήματα που απαιτούν απομακρυσμένη πρόσβαση θα πρέπει να καθορίζονται με σαφήνεια, να παρακολουθούνται και να αναθεωρούνται περιοδικά.

Χρήση δικαιωμάτων διαχειριστή

Η πρόσβαση στις πληροφορίες του πλοίου ή της εταιρείας πρέπει να επιτρέπεται μόνο στο αντίστοιχο εξουσιοδοτημένο προσωπικό. Τα δικαιώματα διαχειριστή επιτρέπουν την πλήρη πρόσβαση στις ρυθμίσεις διαμόρφωσης συστήματος και σε όλα τα δεδομένα και πληροφορίες. Όταν κάποιος χρήστης συνδεθεί σε κάποιο υπολογιστικό σύστημα του πλοίου με δικαιώματα διαχειριστή ενδέχεται να επιτρέψει την εκμετάλλευση κάποιου τρωτού σημείου. Τα προνόμια διαχειριστή πρέπει να δίνονται μόνο σε κατάλληλα εκπαιδευμένο προσωπικό, το οποίο ως μέρος του ρόλου τους στην εταιρεία ή στο πλοίο πρέπει να συνδεθεί σε συστήματα που χρησιμοποιούν αυτά τα προνόμια. Σε κάθε περίπτωση, η χρήση δικαιωμάτων διαχειριστή πρέπει πάντα να περιορίζεται σε λειτουργίες που απαιτούν τέτοια πρόσβαση. Τα δικαιώματα χρήστη διαχειριστή πρέπει να αναιρούνται όταν το προσωπικό δεν βρίσκεται στο πλοίο. Επίσης στην περίπτωση μεταβίβασης λογαριασμών μεταξύ χρηστών δεν πρέπει σε καμία

περίπτωση να χρησιμοποιούνται ‘*generic*’ ονόματα χρήστη (*username*). Οι ίδιοι ή παρόμοιοι κανόνες πρέπει να εφαρμόζονται και από το προσωπικό στη στεριά το οποίο έχει απομακρυσμένη πρόσβαση σε υπολογιστικά συστήματα του πλοίου όταν αλλάξουν ρόλο και δεν χρειάζεται πλέον να έχουν πρόσβαση.

Σε ένα επιχειρηματικό περιβάλλον, όπως η ναυτιλία η πρόσβαση στα ενσωματωμένα συστήματα παρέχεται σε διάφορα ενδιαφερόμενα μέρη. Οι προμηθευτές και οι εργολάβοι αποτελούν κίνδυνο επειδή συχνά έχουν τις γνώσεις για τις λειτουργίες ενός πλοίου σε συνδυασμό με την πλήρη πρόσβαση σε συστήματα του. Για την προστασία της πρόσβασης σε εμπιστευτικά δεδομένα και συστήματα κρίσιμης ασφάλειας, θα πρέπει να υπάρχει μια ισχυρή πολιτική κωδικού πρόσβασης και να διαμορφωθεί ένα πρότυπο ασφαλείας. Οι κωδικοί πρόσβασης πρέπει να είναι ισχυροί και να αλλάζονται περιοδικά. Η πολιτική της εταιρείας πρέπει να αντιμετωπίζει το γεγονός ότι οι υπερβολικά περίπλοκοι κωδικοί πρόσβασης, οι οποίοι πρέπει να αλλάζουν πολύ συχνά, κινδυνεύουν καθώς είναι συχνό φαινόμενο να είναι γραμμένοι σε κάποιο κομμάτι χαρτιού το οποίο μπορεί να βρίσκεται κοντά στον υπολογιστή.

Ακολουθεί η περιγραφή ενός περιστατικού από τις οδηγίες *The Guidelines on Cyber Security Onboard Ships (IMO 2021).*

Μια επίθεση με χρήση *ransomware* λογισμικού στον κύριο διακομιστή εφαρμογών του πλοίου προκάλεσε πλήρη διακοπή λειτουργίας των πληροφοριακών συστημάτων *IT* του πλοίου. Το *ransomware* κρυπτογραφούσε κάθε κρίσιμο αρχείο στον διακομιστή με αποτέλεσμα την απώλεια ευαίσθητων δεδομένων και τη αχρήστευση των εφαρμογών που είναι απαραίτητες για την διοικητική λειτουργία του πλοίου. Ακόμα και μετά την αποκατάσταση του διακομιστή εφαρμογής το περιστατικό επαναλήφθηκε. Η βασική αιτία της μόλυνσης ήταν η λανθασμένη πολιτική κωδικού πρόσβασης, που ως αποτέλεσμα είχε την απομακρυσμένη πρόσβαση του επιτιθέμενου στα υπολογιστικά συστήματα του πλοίου.

Αφαιρούμενα οπτικά μέσα

Κατά την μεταφορά δεδομένων από μη ελεγχόμενα συστήματα σε ελεγχόμενα συστήματα υπάρχει κίνδυνος εισχώρησης κακόβουλου λογισμικού. Τα αφαιρούμενα μέσα μπορούν να χρησιμοποιηθούν για να παρακάμψουν επίπεδα άμυνας και να επιτεθούν σε συστήματα που δεν είναι συνδεδεμένα στο διαδίκτυο. Είναι πολύ σημαντικό για την ασφάλεια να καθοριστεί μια σαφής πολιτική χρήσης τέτοιων συσκευών. Πρέπει να διασφαλιστεί πως συσκευές πολυμέσων δεν χρησιμοποιούνται για την μεταφορά δεδομένων μεταξύ μη ελεγχόμενων συστημάτων. Στις καταστάσεις όπου είναι αναπόφευκτη η χρήση τέτοιων συσκευών

πολυμέσων πρέπει να είναι καθορισμένη η διαδικασία ελέγχου των αφαιρούμενων μέσων για κακόβουλο λογισμικό και η επικύρωση του νόμιμου λογισμικού είτε με υδατογράφημα είτε με ψηφιακή υπογραφή.

Οι πολιτικές και οι διαδικασίες που σχετίζονται με τη χρήση αφαιρούμενων μέσων πρέπει να περιλαμβάνουν απαίτηση σάρωσης οποιασδήποτε αφαιρούμενης συσκευής πολυμέσων σε υπολογιστή που δεν είναι συνδεδεμένη με τα ελεγχόμενα δίκτυα του πλοίου. Αν δεν είναι δυνατή η σάρωση των αφαιρούμενων μέσων επί του σκάφους, π.χ. στην περίπτωση του φορητού υπολογιστή ενός τεχνικού συντήρησης τότε η σάρωση πρέπει να γίνει πριν από την επιβίβαση του τεχνικού. Οι εταιρείες θα πρέπει να εξετάσουν το ενδεχόμενο ειδοποίησης λιμένων και τερματικών σχετικά με την απαίτηση σάρωσης αφαιρούμενων μέσων προτού επιτραπεί η μεταφόρτωση αρχείων στα υπολογιστικά συστήματα ενός πλοίου. Αυτή η σάρωση πρέπει να πραγματοποιείται κατά την μεταφορά των ακόλουθων τύπου αρχείων:

1. Αρχεία φορτίου και σχέδια φόρτωσης
2. Έντυπα εθνικών, τελωνειακών και λιμενικών αρχών
3. Έντυπα ανεφοδιασμού
4. Καταστήματα πλοίου και λίστες προμηθειών
5. Τεχνικά έντυπα και αρχεία συντήρησης

Όπου είναι δυνατόν, τα αρχεία και τα έντυπα θα πρέπει να μεταφέρονται ηλεκτρονικά ή να μεταφορτώνονται απευθείας από αξιόπιστη πηγή χωρίς την χρήση αφαιρούμενων μέσων.

Απόρριψη εξοπλισμού και καταστροφή δεδομένων

Κατά τη διαδικασία αναβάθμισης απαρχαιωμένου εξοπλισμού, πρέπει να ελεγχθεί ο εξοπλισμός που οδηγείται στην απόρριψη για την ύπαρξη ευαίσθητων ή εμπιστευτικών δεδομένων. Πριν από τη διάθεση του εξοπλισμού η εταιρεία θα πρέπει να εφαρμόσει μια διαδικασία που διασφαλίζει πως τα δεδομένα που βρίσκονται στον παρωχημένο εξοπλισμό καταστρέφονται σωστά και δεν υπάρχει δυνατότητα ανάκτησης τους.

Τεχνική υποστήριξη από τη στεριά και σχέδια έκτακτης ανάγκης

Τα πλοία θα πρέπει να έχουν πρόσβαση σε τεχνική υποστήριξη σε περίπτωση κυβερνοεπίθεσης. Λεπτομέρειες αυτής της υποστήριξης και οι σχετικές διαδικασίες θα πρέπει να είναι διαθέσιμες επί του σκάφους.

Κεφάλαιο 5: Αντιμετώπιση περιστατικών κυβερνοεπίθεσης

5.1 Καθιέρωση σχεδίων έκτακτης ανάγκης

Κατά την ανάπτυξη σχεδίων έκτακτης ανάγκης για την υλοποίηση εν πλω, είναι σημαντικό να έχει γίνει κατανοητή η σημασία οποιουδήποτε περιστατικού στον κυβερνοχώρο και να δοθεί η αντίστοιχη προτεραιότητα στις ενέργειες αντίδρασης.

Οποιοδήποτε περιστατικό στον κυβερνοχώρο θα πρέπει να αξιολογείται ώστε να εκτιμηθεί ο αντίκτυπος στις λειτουργίες του πλοίου και τα περιουσιακά στοιχεία του. Στην πλειοψηφία των περιστατικών κυβερνοεπίθεσης δεν απειλείται άμεσα η ασφαλή λειτουργία του πλοίου, εξαίρεση αποτελούν οι κυβερνοεπιθέσεις στα συστήματα σχεδιασμού διαχείρισης φορτίου. Η απώλεια ελέγχου των συστημάτων πληροφορικής επί του πλοίου, συμπεριλαμβανομένης της παραβίασης εμπιστευτικών πληροφοριών και δεδομένων είναι εξαιρετικά επικίνδυνο ζήτημα για την ασφαλή λειτουργία του πλοίου. Σε περίπτωση ενός συμβάντος στον κυβερνοχώρο που να επηρεάζει μόνο τα συστήματα πληροφορικής, πρέπει κατά προτεραιότητα να τίθεται η άμεση εφαρμογή ενός σχεδίου έρευνας και ανάκτησης.

Η απώλεια συστημάτων *OT* μπορεί να έχει σημαντικό και άμεσο αντίκτυπο στην ασφαλή λειτουργία του πλοίου. Εάν ένα περιστατικό στον κυβερνοχώρο καταλήξει σε απώλεια ή δυσλειτουργία των συστημάτων *OT*, είναι απαραίτητο να λαμβάνονται αποτελεσματικά μέτρα ώστε να διασφαλιστεί η άμεση ασφάλεια του πληρώματος, του πλοίου, του φορτίου και της προστασίας του θαλάσσιου περιβάλλοντος. Σε γενικές γραμμές είναι αναγκαία η σχεδίαση κατάλληλων σχεδίων έκτακτης ανάγκης για κυβερνοεπιθέσεις, συμπεριλαμβανομένων την αντιμετώπιση απώλειας κρίσιμων συστημάτων καθώς και η ανάγκη χρήσης εναλλακτικών

τρόπων λειτουργίας των συστημάτων *OT*. Οι σχετικές διαδικασίες λειτουργίας έκτακτης ανάγκης που περιλαμβάνονται στο σύστημα διαχείρισης της ασφάλειας σε συνδυασμό με τα ανωτέρω πρέπει να εφαρμόζονται άμεσα.

Ορισμένες από τις υπάρχουσες διαδικασίες στο σύστημα διαχείρισης της ασφάλειας του πλοίου καλύπτουν ήδη αρκετά από τα πιθανά περιστατικά κυβερνοεπιθέσεων. Ωστόσο τα περιστατικά στον κυβερνοχώρο μπορεί να οδηγήσουν σε πολλαπλές αποτυχίες υπολογιστικών συστημάτων με αποτέλεσμα την διακοπή λειτουργίας πολλών συστημάτων ταυτόχρονα. Ο προγραμματισμός έκτακτης ανάγκης θα πρέπει να λαμβάνει υπόψη τέτοια περιστατικά όπως τα ακόλουθα:

- **Αποσύνδεση του δικτύου *OT* από το δίκτυο στην στεριά**

Οι συνδέσεις μεταξύ συστημάτων ακτής και *OT* μπορεί να είναι σχετίζονται με ένα ευρύ φάσμα εφαρμογών, όπως παρακολούθηση της απόδοσης, η προγνωστική συντήρηση και η απομακρυσμένη υποστήριξη. Συνήθως κάποια από τα *OT* συστήματα του πλοίου που συνδέονται με συστήματα στην ακτή δεν είναι απολύτως απαραίτητα για την ασφαλή λειτουργία του πλοίου, ωστόσο αντιπροσωπεύουν έναν πιθανό φορέα επίθεσης στα συστήματα που είναι απαραίτητα για την ασφαλή λειτουργία του πλοίου καθώς συνδέονται με αυτά. Επομένως, είναι σημαντικό να εκτιμηθεί πότε επιτρέπονται αυτές οι συνδέσεις και υπό ποιες συνθήκες. Είναι αναγκαίο να καταρτιστούν σχέδια που θα καθορίζουν πότε θα είναι ασφαλή τέτοια συστήματα *OT* και θα γίνεται ο διαχωρισμός από τη σύνδεση του χερσαίου δικτύου για την προστασία της ασφαλούς λειτουργίας του πλοίου. Η αποσύνδεση τους από το δίκτυο της στεριάς αποτρέπει τον εισβολέα από το να είναι σε θέση να χειριστεί κρίσιμα συστήματα ασφαλείας ή να πάρει τον άμεσο έλεγχο του συστήματος. Με την αποσύνδεση θα μπορούσε ακόμη να αποφευχθεί η διάδοση κακόβουλου λογισμικού μεταξύ των τμημάτων του δικτύου.

Για τον αποτελεσματικό τερματισμό της σύνδεσης με τη στεριά είναι αναγκαία η σύνδεση στο διαδίκτυο και η συνδεσιμότητα με υπηρεσίες που είναι σχεδιασμένες με κατάλληλο τρόπο ώστε τα δίκτυα να μπορούν να διαχωριστούν γρήγορα (πχ με αποσύνδεση καλωδίου το οποίο συνήθως έχει διαφορετικό χρώμα ώστε να είναι η λειτουργία του).

- **Σύστημα διαχείρισης ασφάλειας (*Safety management systems*)**

Το σύστημα διαχείρισης της ασφάλειας περιλαμβάνει διαδικασίες για την αναφορά ατυχημάτων ή καταστάσεις κινδύνου που καθορίζουν τα επίπεδα επικοινωνίας και ελέγχου για τη λήψη αποφάσεων. Όπου ενδείκνυται, τέτοιες διαδικασίες θα πρέπει να τροποποιηθούν ώστε να γίνει η ανάκτηση επικοινωνίας και ελέγχου σε περίπτωση περιστατικού κυβερνοεπίθεσης.

Ακολουθεί ένας μη εξαντλητικός κατάλογος περιστατικών στον κυβερνοχώρο, τα οποία πρέπει να αντιμετωπιστούν σε περίπτωση υλοποίησης σχεδίου έκτακτης ανάγκης επί του πλοίου:

1. Αδυναμία χρήσης ηλεκτρονικού εξοπλισμού πλοήγησης
2. Απώλεια απαραίτητων δεδομένων για την πλοήγηση του πλοίου
3. Απώλεια της απαραίτητης συνδεσιμότητας με την στεριά για την πλοήγηση του πλοίου
4. Απώλεια ελέγχου των συστημάτων πρόωσης και ευστάθειας του πλοίου

Επιπλέον, είναι σημαντικό να διασφαλιστεί πως η απώλεια εξοπλισμού ή αξιόπιστων πληροφοριών εξαιτίας κάποιου περιστατικού στον κυβερνοχώρο να μην καθιστά τα υπάρχοντα σχέδια και διαδικασίες έκτακτης ανάγκης αναποτελεσματικά. Τα σχέδια έκτακτης ανάγκης καθώς και οι σχετικές πληροφορίες θα πρέπει να είναι διαθέσιμες και σε μη ηλεκτρονική μορφή, διότι ορισμένα είδη περιστατικών στον κυβερνοχώρο μπορεί να περιλαμβάνουν την διαγραφή δεδομένων σε συνδυασμό με τον τερματισμό των συνδέσμων επικοινωνίας.

Ενδέχεται να υπάρχουν περιπτώσεις όπου η ανταπόκριση σε κυβερνοεπίθεση να ξεπερνά τις αρμοδιότητες του τμήματος ασφαλείας του πλοίου λόγω της πολυπλοκότητας ή της σοβαρότητας του περιστατικού. Σε τέτοιες περιπτώσεις το συμβούλιο ασφαλείας της εταιρείας ζητά εξωτερική βοήθεια από ειδικούς εμπειρογνώμονες.

5.2 Αντιμετώπιση και ανάκτηση

Η γνώση σχετικά με τα προηγούμενα αναγνωρισμένα περιστατικά επίθεσης στον κυβερνοχώρο θα πρέπει να χρησιμοποιηθεί για τη βελτίωση των σχεδίων αντιμετώπισης σε όλα τα πλοία του στόλου της εταιρείας και πρέπει να ληφθεί υπόψη η κατάλληλη στρατηγική πληροφόρησης για τέτοια περιστατικά.

5.2.1 Αποτελεσματική απόκριση

Για την αποτελεσματική ανταπόκριση σε ενδεχόμενο περιστατικό κυβερνοεπίθεσης είναι αναγκαία η δημιουργία ειδικής ομάδας η οποία μπορεί να περιλαμβάνει προσωπικό επί του σκάφους και της ξηράς, όπου θα συμμετέχουν ειδικοί εμπειρογνώμονες για να λαμβάνουν τα κατάλληλα μέτρα για την αποκατάσταση συστημάτων *IT* και *OT*.

Η αποτελεσματική απόκριση θα πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα βήματα:

- **Αρχική εκτίμηση**

Για να διασφαλιστεί η αποτελεσματική απάντηση η ειδική ομάδα θα πρέπει να ανακαλύψει: 1) πως συνέβη το περιστατικό, 2) ποια συστήματα επηρεάστηκαν και πως, 3) τον βαθμό που επηρεάζονται τα εμπορικά και λειτουργικά δεδομένα, 4) σε ποιο βαθμό παραμένει οποιαδήποτε απειλή για τα συστήματα *IT* και *OT*

- **Ανάκτηση συστημάτων και δεδομένων**

Μετά την αρχική αξιολόγηση του περιστατικού θα πρέπει να γίνεται ο καθαρισμός των συστημάτων *IT* και *OT* που μολύνθηκαν και θα πρέπει να γίνει ανάκτηση δεδομένων στο μέτρο του δυνατού. Η αποκατάσταση των συστημάτων θα πρέπει να γίνεται σε πρότερη λειτουργική κατάσταση απαλείφοντας κάθε απειλή και επαναφέροντας το λογισμικό του συστήματος. Το περιεχόμενο του σχεδίου ανάκτησης θα περιγραφεί στην επόμενη ενότητα.

- **Διερεύνηση του περιστατικού**

Για την κατανόηση σε βάθος των αιτιών καθώς και των συνεπειών του περιστατικού κυβερνοεπίθεσης η εταιρεία θα πρέπει να διεξάγει έρευνα η οποία θα υποστηριχθεί και από εξωτερικούς εμπειρογνώμονες στην περίπτωση που δεν υπάρχει το κατάλληλο προσωπικό. Τα δεδομένα και οι πληροφορίες που συλλέγονται κατά την έρευνα θα έχουν σημαντικό ρόλο στην πρόληψη αλλά και στην αντιμετώπιση πιθανής παρόμοιας επίθεσης.

Στην περίπτωση περίπλοκου περιστατικού, για παράδειγμα όταν μετά από μια κυβερνοεπίθεση τα συστήματα *IT* και *OT* δεν μπορούν να επανέλθουν στην κανονική τους λειτουργία μπορεί να χρειαστεί να ξεκινήσει το σχέδιο ανάκαμψης παράλληλα με το σχέδια έκτακτης ανάγκης. Σε τέτοιες περιπτώσεις η υπεύθυνη ομάδα ασφαλείας θα πρέπει να είναι σε θέση να παρέχει συμβουλές στο πλοίο για τα παρακάτω θέματα:

1. Εάν τα συστήματα *IT* ή *OT* πρέπει να τερματίσουν τη λειτουργία τους ή όχι για την προστασία των ευαίσθητων δεδομένων
2. Εάν συγκεκριμένοι δίαυλοι επικοινωνίας του πλοίου με τη στεριά πρέπει να διακοπούν ή όχι
3. Την κατάλληλη χρήση τυχόν προηγμένων εργαλείων που παρέχονται σε προ εγκατεστημένο λογισμικό ασφαλείας

4. Τον βαθμό στον οποίο το περιστατικό έχει θέσει σε κίνδυνο τα συστήματα *IT* και *OT* πέρα από τις δυνατότητες του υφισταμένου σχεδίου ανάκαμψης

Είναι σημαντικό για το αρμόδιο προσωπικό ασφαλείας να εκτελεί τακτικά ασκήσεις ασφαλείας στον κυβερνοχώρο ώστε να διατηρείται σε υψηλό και αποτελεσματικό επίπεδο η ικανότητα άμεσης απόκρισης. Οι ασκήσεις κυβερνοασφάλειας θα μπορούσαν, όπου ενδείκνυται να εμπνευστούν από πραγματικά γεγονότα επιθέσεων και μπορεί να είναι προσομοιώσεις περιστατικών μεγάλης κλίμακας που κλιμακώνονται και γίνονται κρίσεις στον κυβερνοχώρο. Αυτό προσφέρει μια ευκαιρία για ανάλυση προηγμένων τεχνικών αντιμετώπισης περιστατικών ασφάλειας στον κυβερνοχώρο, αλλά βοηθά και στην αντιμετώπιση της συνέχειας των επιχειρήσεων και της διαχείρισης κρίσεων.

5.2.2 Σχέδιο ανάκτησης

Αρχικά τα σχέδια αποκατάστασης θα πρέπει να είναι διαθέσιμα σε έντυπη μορφή τόσο στο πλοίο όσο και στην ξηρά. Ο σκοπός του σχεδίου είναι η υποστήριξη της ανάκτησης συστημάτων και δεδομένων που είναι απαραίτητα για την επαναφορά των συστημάτων πληροφορικής, καθώς και της τεχνολογίας πληροφοριών σε λειτουργική κατάσταση. Για να διασφαλιστεί η ασφάλεια του προσωπικού του πλοίου, άμεση προτεραιότητα έχει η επαναφορά λειτουργίας των απαραίτητων συστημάτων για την πλοήγηση του πλοίου. Το σχέδιο αποκατάστασης πρέπει να είναι κατανοητό από το προσωπικό που είναι υπεύθυνο για την ασφάλεια στον κυβερνοχώρο. Η λεπτομέρεια και η πολυπλοκότητα ενός σχεδίου αποκατάστασης εξαρτάται από τον τύπο του πλοίου καθώς την τεχνολογία των συστημάτων *IT* και *OT* αλλά και άλλων συστημάτων που είναι εγκατεστημένα στο σκάφος.

Η ομάδα αντιμετώπισης περιστατικών θα πρέπει να εξετάσει προσεκτικά τις επιπτώσεις των ενεργειών ανάκτησης, όπως την σάρωση και καθαρισμό οπτικών μέσων και μέσων αποθήκευσης. Υπάρχει πάντα ο κίνδυνος κάποια από τις ενέργειες ανάκτησης να οδηγήσει στην καταστροφή στοιχείων που θα μπορούσαν να προσφέρουν πολύτιμες πληροφορίες σχετικά με τα αίτια ενός συμβάντος. Επομένως όπου είναι δυνατόν, η επαγγελματική αντιμετώπιση περιστατικών στον κυβερνοχώρο θα πρέπει να παρέχεται ώστε να συνδράμει στη διατήρηση των αποδεικτικών στοιχείων κατά την αποκατάσταση της ικανότητας λειτουργίας.

Η ικανότητα ανάκτησης δεδομένων είναι ένα πολύτιμο μέτρο τεχνικής προστασίας όπως αναφέρθηκε παραπάνω. Οι δυνατότητες ανάκτησης δεδομένων είναι συνήθως με τη μορφή αντιγράφων ασφαλείας λογισμικού για δεδομένα πληροφορικής. Η διαθεσιμότητα ενός

αντιγράφου ασφαλείας λογισμικού, είτε επί του σκάφους είτε στην ξηρά, θα πρέπει να επιτρέπει την ανάκτηση των πληροφοριακών συστημάτων σε λειτουργική κατάσταση μετά από κυβερνοεπίθεση. Η ανάκτηση των συστημάτων *OT* μπορεί να είναι πιο περίπλοκη, ειδικά εάν δεν υπάρχουν διαθέσιμα εφεδρικά συστήματα και μπορεί να απαιτείται συνδρομή από την ξηρά. Οι λεπτομέρειες για το πού είναι διαθέσιμη αυτή η βοήθεια και από ποιον, θα πρέπει να είναι μέρος του σχεδίου ανάκτησης, για παράδειγμα προχωρώντας σε λιμάνι για να λάβει βοήθεια από μια υπηρεσία.

Εάν υπάρχει διαθέσιμο εξειδικευμένο προσωπικό επί του σκάφους, ενδέχεται να πραγματοποιηθούν και να εκτελεστούν εκτενέστερες διαγνωστικές ενέργειες σε συνδυασμό με ενέργειες αποκατάστασης.

5.2.3 Διερεύνηση του περιστατικού

Η διερεύνηση ενός περιστατικού στον κυβερνοχώρο μπορεί να παράσχει πολύτιμες πληροφορίες σχετικά με τον τρόπο με τον οποίο ο επιτιθέμενος εκμεταλλεύτηκε κάποιο από τα τρωτά σημεία του πλοίου. Οι εταιρείες θα πρέπει, όπου είναι δυνατόν, να διερευνούν τα περιστατικά στον κυβερνοχώρο που επηρεάζουν τα συστήματα πληροφορικής καθώς και τα επιχειρησιακά συστήματα επί του σκάφους σύμφωνα με τις καθορισμένες διαδικασίες της εταιρείας. Μια λεπτομερής έρευνα μπορεί να απαιτεί εξωτερική υποστήριξη εμπειρογνωμόνων. Οι πληροφορίες από μια έρευνα μπορούν να χρησιμοποιηθούν για τη βελτίωση των τεχνικών και διαδικαστικών μέτρων προστασίας στο πλοίο και στην ξηρά. Μπορεί επίσης να βοηθήσει την ευρύτερη ναυτιλιακή βιομηχανία με μια καλύτερη κατανόηση των επιθέσεων στον κυβερνοχώρο. Τα πλεονεκτήματα της αποτελεσματικής διερεύνησης περιστατικού είναι τα ακόλουθα:

- Η καλύτερη κατανόηση των πιθανών κινδύνων στον κυβερνοχώρο που αντιμετωπίζει η ναυτιλιακή βιομηχανία, τόσο εν πλω όσο και στην στεριά
- Προσδιορισμός των πληροφοριών που συλλέχθηκαν ώστε να αυξηθεί η ευαισθητοποίηση του προσωπικού για τους κινδύνους μιας κυβερνοεπίθεσης
- Προγραμματισμός βελτιωτικών διαδικασιών του σχεδίου ασφαλείας του πλοίου
- Αναβάθμιση και ενημέρωση των τεχνικών και διαδικαστικών μέτρων προστασίας για την αποφυγή υποτροπής

5.3 Απώλειες που προκύπτουν από μια κυβερνοεπίθεση

Για τις ασφαλιστικές εταιρείες, ο όρος «κυβερνοχώρος» περιλαμβάνει πολλές διαφορετικές πτυχές, οπότε είναι σημαντικό να γίνει διάκριση μεταξύ τους και τις επιπτώσεις τους στην ασφαλιστική κάλυψη. Ορισμένοι ασφαλιστές πιστεύουν ότι δεν υπάρχει συστημικός κίνδυνος για τα πλοία που να προκύπτει από κυβερνοεπίθεση και ο αντίκτυπος ενός συμβάντος θα περιοριστεί πιθανότατα σε ένα μόνο πλοίο. Οι εταιρείες όμως επιλέγουν κάποια από τις διαθέσιμες ασφαλιστικές καλύψεις που είναι σχεδιασμένη για τις θαλάσσιες μεταφορές για την κάλυψη πιθανών οικονομικών κυρώσεων εξαιτίας κάποιας απώλειας δεδομένων.

Οι εταιρείες θα πρέπει να είναι σε θέση να αποδείξουν ότι ενεργούν σύμφωνα με τα καθορισμένα πρότυπα ασφαλείας στην προσέγγισή τους για τη διαχείριση του κινδύνου στον κυβερνοχώρο και την προστασία του πλοίου από τυχόν ζημιές που μπορεί να προκύψουν από ένα περιστατικό κυβερνοεπίθεσης.

5.3.1 Καλύψεις για υλικές ζημιές

Οι περισσότερες ασφαλιστικές εταιρείες που δραστηριοποιούνται στον κλάδο της ναυτιλίας προσφέρουν συμβόλαια που καλύπτουν απώλειες ή ζημιές στο πλοίο και στον εξοπλισμό του που προκαλείται από κάποιο συμβάν που προκαλείται εν πλω, όπως προσάραξη, σύγκρουση, πυρκαγιά ή πλημμύρα ακόμη και όταν η υποκείμενη αιτία του συμβάντος είναι ένα κυβερνοπεριστατικό. Πρέπει να σημειωθεί ότι προς το παρόν σε ορισμένες αγορές, υπάρχουν ρήτρες αποκλεισμού για κυβερνοεπιθέσεις. Εάν η θαλάσσια πολιτική περιέχει ρήτρα αποκλεισμού για κυβερνοεπιθέσεις, η απώλεια ή η ζημιά που μπορεί να προκληθεί ενδέχεται να μην καλυφθεί. Συνιστάται στις εταιρείες να ελέγχουν εκ των προτέρων με τους ασφαλιστές/μεσίτες τους εάν η πολιτική τους καλύπτει αξιώσεις που προκαλούνται από κυβερνοεπιθέσεις ή περιστατικών που συμβαίνουν στον κυβερνοχώρο.

Έχουν δημοσιευθεί κατευθυντήριες γραμμές για την αγορά, στις οποίες συνιστάται να ζητούν οι ασφαλιστές στον κλάδο της ναυτιλίας να κάνουν ερωτήσεις σχετικά με την ευαισθητοποίηση στον κυβερνοχώρο και τις μη τεχνικές διαδικασίες μιας εταιρείας. Οι εταιρείες πρέπει ως εκ τούτου, να αναμένουν ένα αίτημα για μη τεχνικές πληροφορίες σχετικά με την προσέγγισή τους στον κυβερνοχώρο και τη διαχείριση ενός περιστατικού από τους ασφαλιστές. Τα περιορισμένα δεδομένα σχετικά με τη συχνότητα, τη σοβαρότητα της απώλειας ή την πιθανότητα σωματικής βλάβης που προκύπτει από περιστατικά στον κυβερνοχώρο, αποτελούν πρόκληση με αποτέλεσμα να μην υπάρχει διαθέσιμη τυπική τιμολόγηση.

5.3.2 Κάλυψη για την ευθύνη

Ένα περιστατικό που προκλήθηκε, για παράδειγμα από δυσλειτουργία της πλοήγησης ενός πλοίου ή των μηχανικών συστημάτων, εξαιτίας κυβερνοεπίθεσης δεν προκαλεί από μόνη της τυχόν αποκλεισμό από τις καλύψεις. Σε περίπτωση αξίωσης που αφορά περιστατικό στον κυβερνοχώρο, οι ενάγοντες μπορούν κάλλιστα να επιδιώξουν και να υποστηρίξουν τον ισχυρισμό ότι το περιστατικό προέκυψε ως αποτέλεσμα ανεπαρκούς επιπέδου ετοιμότητας στον κυβερνοχώρο. Πρέπει λοιπόν οι εταιρείες να αποδείξουν ότι ενεργούν σύμφωνα με τα διεθνή πρότυπα ασφαλείας στη διαχείριση του κινδύνου στον κυβερνοχώρο και στην προστασία του πλοίου. Θα πρέπει να σημειωθεί ότι πολλές πιθανές απώλειες εξαιτίας κυβερνοεπίθεσης, δεν είναι μέρος των υποχρεώσεων τρίτων, με αποτέλεσμα να μην καλύπτονται από τα τυπικά ασφαλιστικά συμβόλαια. Για παράδειγμα η οικονομική απώλεια που προκαλείται από επίθεση με *ransomware* ή το κόστος ανάκτησης των δεδομένων δεν προσδιορίζεται σε ασφαλιστικό συμβόλαιο με αποτέλεσμα να μην καλύπτονται από την ασφαλιστική εταιρεία.

Κεφάλαιο 6: Συμπεράσματα και μελλοντικές προτάσεις

Η εξέλιξη της τεχνολογίας και διασύνδεση συστημάτων *IT* του πλοίου με συστήματα στα γραφεία της εταιρείας στην στεριά έχουν αυξήσει σημαντικά τον κίνδυνο κυβερνοεπίθεσης. Η τεχνολογία συνεχώς εξελίσσεται και αλλάζει οπότε πολλά συστήματα πρέπει να αναβαθμίζονται και να αναθεωρούνται σε τακτά χρονικά διαστήματα. Οι εγκληματίες συνεχώς αναζητούν νέους τρόπους επίθεσης ανακαλύπτοντας τα τρωτά σημεία είτε αυτά βρίσκονται στο πλοίο είτε στη στεριά και δοκιμάζουν νέες κυβερνοεπιθέσεις. Το κυριότερο συμπέρασμα από τη μελέτη των κυβερνοεπιθέσεων που έχουν συμβεί είναι πως η επίθεση ξεκινά από κάποιο λάθος ή αμέλεια προσωπικού είτε του πλοίου είτε τρίτων είτε από την στεριά. Είναι

υψίστης σημασίας η συνεχής εκπαίδευση και ευαισθητοποίηση του προσωπικού για τα θέματα κυβερνοασφάλειας. Οι ναυτιλιακές εταιρείες σε συνεργασία με εταιρείες πληροφορικής και δημιουργίας λογισμικού καθώς και με μέλη της ακαδημαϊκής κοινότητας αλλά πιθανώς με πανεπιστημιακά ιδρύματα θα μπορούσαν να διοργανώσουν εκπαιδευτικά σεμινάρια για το προσωπικό τους. Μέσα από αυτά τα σεμινάρια οι ειδήμονες των θεμάτων κυβερνοασφάλειας θα εκπαιδεύσουν τους υπεύθυνους ασφαλείας της εταιρείας και θα τους ενημερώνουν έγκαιρα για οποιαδήποτε τεχνολογική εξέλιξη. Το τμήμα ασφαλείας της εταιρείας εν πλω θα πρέπει να έχει τουλάχιστον ένα άτομο αποκλειστικά υπεύθυνο για τα θέματα ασφαλείας στον κυβερνοχώρο. Το τμήμα ασφαλείας οφείλει να έχει το σχέδιο ασφαλείας και σε έντυπη μορφή και να το αναβαθμίζει σε τακτά χρονικά διαστήματα, είναι αναγκαίο να γίνονται ενημερώσεις του προσωπικού για θέματα ασφάλειας στον κυβερνοχώρο ώστε να αποφεύγονται τα ανθρώπινα λάθη. Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο οι εγκληματίες εξελίσσουν την τεχνική του *phishing* η οποία πετυχαίνει τον στόχο της όταν ο παραπλανημένος χρήστης επισκέπτεται έναν ύποπτο σύνδεσμο. Είναι αναγκαίο να ευαισθητοποιηθεί το προσωπικό για τους κινδύνους που υπάρχουν για την ασφάλεια του πλοίου κατά την χρήση αφαιρούμενων μέσων και κατά την χρήση των προσωπικών τους *smartphones* όταν συνδέονται στο δίκτυο του πλοίου.

Η εξέλιξη της **τεχνητής νοημοσύνης** μπορεί να αποτελέσει σημαντικό εργαλείο για ασφάλεια στον κυβερνοχώρο αλλά ταυτόχρονα ενδέχεται να χρησιμοποιηθεί και από τους επιτιθέμενους. Η χρήση τεχνητής νοημοσύνης είναι ένα πολύ σημαντικό εργαλείο για την επιστήμη της ανάλυσης μεγάλων δεδομένων (*big data*). Μέσω αλγορίθμων μπορεί να γίνει ταχύτατα ανάλυση μεγάλων δεδομένων για τον προσδιορισμό μοτίβων. Οι επιτιθέμενοι χρησιμοποιούν τέτοια εργαλεία για την κλοπή κωδικών χρήστη ή διαπιστευτηρίων καθώς και για την διερεύνηση των τρωτών σημείων του πλοίου. Είναι πολύ σημαντικό για την ασφάλεια του πλοίου να υπάρχει έλεγχος των συστημάτων της στεριάς που συνδέονται απομακρυσμένα με το πλοίο και συλλέγουν δεδομένα για την ομαλή λειτουργία του. Οι επιτιθέμενοι θα προσπαθήσουν να υποκλέψουν τα δεδομένα και έπειτα να τα αναλύσουν για την υλοποίηση μιας κυβερνοεπίθεσης. Είναι σημαντική η αναζήτηση κάποιου μοτίβου των κυβερνοεπιθέσεων ώστε να είναι έγκαιρη η προειδοποίηση. Από την άλλη το τμήμα ασφαλείας του πλοίου μπορεί να χρησιμοποιήσει σχετικά εργαλεία για να αναλύσει, αφενός τα δεδομένα από προηγούμενες κυβερνοεπιθέσεις και αφετέρου τα αποτελέσματα ασκήσεων προσομοίωσης. Στην περίπτωση κυβερνοεπίθεσης με χρήση *trojan* (δούρειου ίππου) όπου κάποια φαινομενικά ακίνδυνη εφαρμογή έχει εγκατασταθεί στα υπολογιστικά συστήματα του πλοίου και υποκλέπτει

δεδομένα, η χρήση εργαλείων τεχνητής νοημοσύνης θα μπορούσε να χρησιμοποιηθεί για την έγκαιρη ανακάλυψη του κακόβουλου λογισμικού. Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο μπορεί να έχει μολυνθεί κάποιο από τα συστήματα *IT* του πλοίου ή της εταιρείας και να μην γίνει άμεσα αντιληπτό από το προσωπικό της.

Οι εγκληματίες στον κυβερνοχώρο έχουν αρχίσει και συνεργάζονται και οργανώνονται ώστε να συντονίζονται από διάφορα μέρη του κόσμου για να εκτοξεύσουν συντονισμένη επίθεση με χρήση κακόβουλου λογισμικού όπως συνέβη το 2017 με την επίθεση *Wannacry Ransomware Attack* όπου πάνω από 250.000 υπολογιστές σε 150 χώρες μολύνθηκαν από το συγκεκριμένο κακόβουλο λογισμικό. Οι επιτιθέμενοι ζητούσαν λύτρα σε *bitcoin* για να αποκτήσει ξανά ο χρήστης πρόσβαση στον σύστημα του. Είναι πιθανό λοιπόν στο μέλλον να υπάρξουν ανάλογες επιθέσεις με στόχο κάποιο περιουσιακό στοιχείο ναυτιλιακής εταιρείας, οπότε πρέπει να συνεργαστούν και οι ναυτιλιακές εταιρείες για την αντιμετώπιση μιας ενδεχόμενης τέτοιας επίθεσης.

Η εξέλιξη του *IoT (Internet of Things)* δημιουργεί νέες ευκαιρίες για κυβερνοεπιθέσεις στους εγκληματίες. Ο όρος *IoT* αναφέρεται σε συσκευές εκτός ηλεκτρονικών υπολογιστών, τηλεφώνων και διακομιστών που συνδέονται στο διαδίκτυο και μοιράζονται δεδομένα. Υπολογίζεται πως έως το 2026 θα υπάρχουν περίπου 64 δισεκατομμύρια *IoT* συσκευές συνδεδεμένες στο διαδίκτυο (Πηγή*:* *www.kaspersky.com)* γεγονός που αυξάνει το δυνατό εύρος κυβερνοεπίθεσης για τους εγκληματίες. Οι εταιρείες καλούνται να προετοιμαστούν για επιθέσεις σε τέτοιες συσκευές, οι οποίες συνήθως είναι μέρος του συστήματος *welfare* του πληρώματος και των επιβατών. Το τμήμα ασφαλείας οφείλει να ενημερώνει το προσωπικό και να έχει μονίμως ενημερωμένα τα *firewalls* και τα συστήματα *anti-virus* των διακομιστών όπου συνδέονται αυτές οι συσκευές, ενώ πρέπει να το δίκτυο που συνδέονται να είναι απομονωμένο από τα συστήματα *OT* του πλοίου.

Ο αυξημένος όγκος δεδομένων αποθηκεύεται πλέον σε υπηρεσίες *cloud* όπου με τον όρο αυτό αναφέρονται οι υπηρεσίες όπου διατίθενται υπολογιστικοί πόροι μέσω διαδικτύου από κεντρικά συστήματα που βρίσκονται απομακρυσμένα από τον τελικό χρήστη. Αυτές οι υπηρεσίες προσφέρουν σημαντικά οφέλη στις εταιρείες καθώς μειώνεται το κόστος και αυξάνεται η αποτελεσματικότητα, αλλά αυξάνουν τον κίνδυνο κυβερνοεπιθέσεων καθώς αυξάνονται τα πιθανά σημεία εισόδου των κυβερνοεπιθέσεων.

Συνοψίζοντας η κυβερνοασφάλεια στον χώρο της ναυτιλίας πρέπει να αποτελεί προτεραιότητα για τις εταιρείες. Η δημιουργία εκπαιδευμένου και εξειδικευμένου τμήματος

κυβερνοασφάλειας σε αυτές κρίνεται απαραίτητη. Το τμήμα αυτό θα είναι υπεύθυνο να ευαισθητοποιεί και να ενημερώνει το πλήρωμα για όλα τα τρωτά σημεία και τους πιθανούς κινδύνους μιας κυβερνοεπίθεσης. Η εξέλιξη της τεχνολογίας εκτός από τις θετικές αλλαγές στον κλάδο της ναυτιλίας θα ανοίξει δρόμους σε νέες πιθανές επιθέσεις οπότε είναι αναγκαία η ενημέρωση και προετοιμασία του προσωπικού. Οι κυβερνοεπιθέσεις αναπόφευκτα θα αυξηθούν, γι' αυτό το λόγο οι ναυτιλιακές εταιρείες οφείλουν να είναι έτοιμες ώστε να ανταποκριθούν όσο το δυνατόν ταχύτερα και αποτελεσματικότερα. Είναι αναγκαία η ύπαρξη σχεδίου άμυνας και απόκρισης, το οποίο θα έχει εκτελεστεί αρκετές φορές σε ασκήσεις άμυνας.

Βιβλιογραφία

Έντυπη βιβλιογραφία

1. *Aven, T. & Renn, O. & Rosa, E. (2015), 'On the ontological status of the concept of risk', Safetty Science 49*

2. *Kaleem Awan, M. & Al Ghamdi, M. (2019), 'Understanding the vulnerabilities in digital components of an integrated bridge system', Journal of Marine Science and Engineering, October, 2019*

3. *DNVGL-RP-0496 (2016), 'Cyber security resilience management for ships and mobile offshore units in operation', Edition September 2016*

4. *IMO (2021), 'The Guidelines of Cyber Security Onboard Ships'*

5. *Enisa (2011), 'Analysis of cyber security aspects in the maritime sector'*

6. *Clark, J. (2019), 'Cybercrime in the shipping industry'. Hill Dickinson*

7. *Coquil, T. (2021), 'Best practices for cybersecurity on board ships', Ministere de l 'environment*

8. *ISPS CODE GUIDELINES FOR SHIP SUPPLIERS (2016), 'International ship and port facility security code', ISSA*

9. *Pajunen, N. (2017), 'Overview of Maritime Cybersecurity', South-Eastern Finland University of Applied Sciences*

10. Νικητάκος, Ν. (2019), ' *Κυβερνοασφάλεια και εμπορικό πλοίο',* Κέντρο Μελετών Ασφαλείας

11. *IMO, (2017), ‘ GUIDELINES ON MARITIME CYBER RISK MANAGEMENT’, MSC-FAL.1 /Circ.3*

Ηλεκτρονική βιβλιογραφία

1. https://safety4sea.com (ημερομηνία προβολής 14/9/2021)

2. https://marine-digital.com/cybersecurity_in_shipping_and_ports (ημερομηνία προβολής 28/9/2021)

3. https://marine-digital.com/article_importance_of_cybersecurity (ημερομηνία προβολής 11/10/2021)

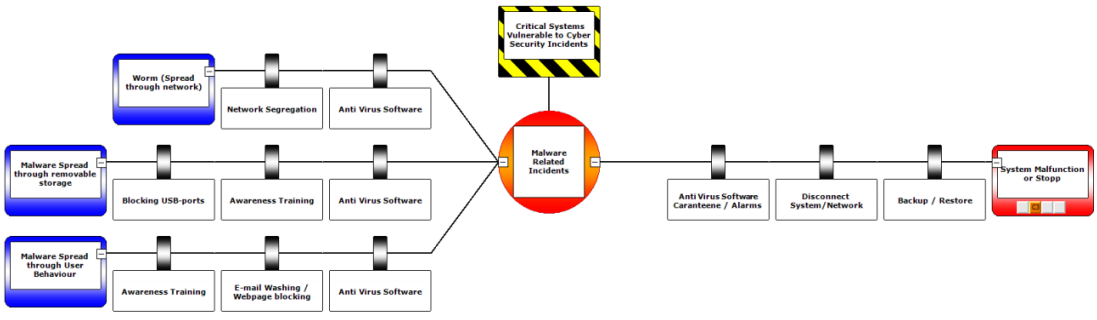
4. https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0 (ημερομηνία προβολής 24/10/2021)

Παράρτημα 1. Διαχείριση στρατηγικής άμυνας

1.1 Α. *Cyber security barrier management* (Διαχείριση στρατηγικής άμυνας στον κυβερνοχώρο)

Στρατηγική εμποδίων ενάντια σε επίθεση *malware (Barriers against malware)*

Παραδείγματα αντιμέτρων σε κυβερνοεπίθεση



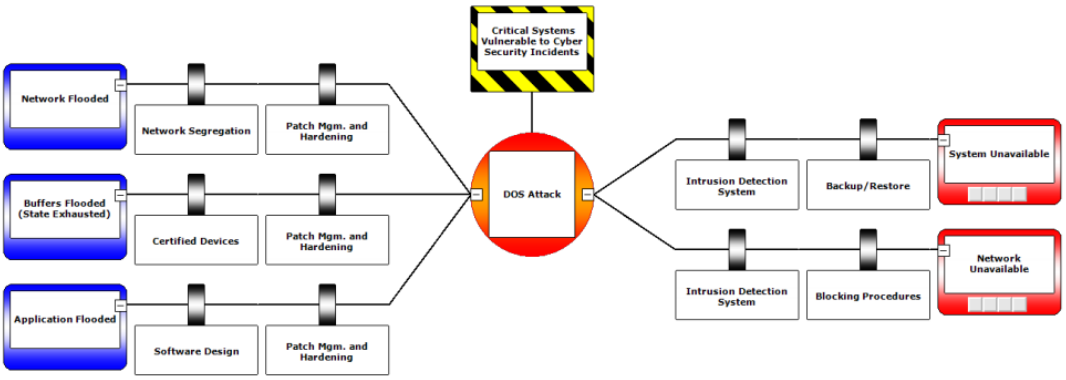
Εικόνα 1: Διάγραμμα της άμυνας κατά επίθεσης με χρήση malware (Πηγή: DNV-GL Recommended Practice, 2016)

Στην εικόνα 1 ταξινομούνται οι απειλές ανάλογα με τον τρόπου που μπορεί το κακόβουλο λογισμικό να εισέλθει στα υπολογιστικά συστήματα του πλοίου ή της εταιρείας. Όπως παρουσιάστηκε σε προηγούμενο κεφάλαιο αυτό συμβαίνει μέσω αφαιρούμενων μέσων αποθήκευσης , μέσω *worms* και μέσω δραστηριότητας του χρήστη. Η κοινωνική μηχανική (*social engineering*) χρησιμοποιείται όλο και περισσότερο για την εκμετάλλευση των αδυναμιών στη συμπεριφορά και δραστηριότητα του χρήστη. Στο παράδειγμα της εικόνας 1 τα εμπόδια για την αποφυγή εισόδου ενός *worm* είναι ο διαχωρισμός του δικτύου και ο περιορισμός της ροής δεδομένων μεταξύ τμημάτων του δικτύου, ώστε να επιτρέπεται μόνο καθορισμένη μεταφορά πρωτοκόλλων και διευθύνσεων. Τα συστήματα *IPS*[12] αναγνωρίζουν και αποκλείουν γνωστά κακόβουλα μοτίβα αλλά αυτά απευθύνονται σε πληροφοριακά συστήματα και ενδέχεται να μην είναι κατάλληλα για βιομηχανικά συστήματα ελέγχου. Το λογισμικό προστασίας από ιούς και λογισμικό κατασκοπείας (*spyware*) είναι υποχρεωτικό για όλες τις απειλές κακόβουλου λογισμικού, συμπεριλαμβανομένου του καθεστώτος για την ενημέρωση των ψηφιακών υπογραφών. Η ενημέρωση λογισμικού προστασίας από ιούς και λογισμικό υποκλοπής *spyware* για πλοία μπορεί να απαιτεί χειροκίνητες διαδικασίες, καθώς η ροή δεδομένων στα πλοία μπορεί να είναι περιορισμένη λόγω τμηματοποίησης και περιορισμένου εύρους ζώνης. Η ενίσχυση του συστήματος και η διαχείριση επιδιορθώσεων αποτελούν εμπόδια για κακόβουλο λογισμικό, δεδομένου ότι οι αλλαγές δοκιμάζονται, ιδιαίτερα για κρίσιμα συστήματα. Τέλος, ένα σύστημα απογραφής ενημερωμένης έκδοσης κώδικα λογισμικού είναι απαραίτητο για να γνωρίζει ο υπεύθυνος ασφαλείας τι επιδιορθώσεις έχουν εγκατασταθεί σε όλα τα συστήματα του πλοίου.

1.2 Β. *Barriers against denial of service attacks* (Διαχείριση στρατηγικής άμυνας ενάντια σε επιθέσεις άρνησης εισόδου)

Παράδειγμα αντιμέτρων ενάντια σε επιθέσεις άρνησης εισόδου

[12] *Intrusion Prevention System*: Σύγχρονη μορφή διαδικτυακής ασφάλειας



Εικόνα 2: Διάγραμμα της άμυνας κατά επίθεσης άρνησης εισόδου (Πηγή: DNV-GL Recommended Practice, 2016)

Στο σενάριο που απεικονίζεται στο παραπάνω σχήμα, ο εισβολέας υπερφορτώνει το δίκτυο, υπερφορτώνει το *buffer* διαφόρων συσκευών (π.χ. *buffers* κατάστασης στο τείχος προστασίας) ή υπερφορτώνει την εφαρμογή (π.χ. αναγκάζοντας την σε συχνές λειτουργίες που καταναλώνουν πόρους του συστήματος). Τα εμπόδια για την αποφυγή της απειλής πλημμύρας δικτύου είναι ο διαχωρισμός του δικτύου και ο περιορισμός της κυκλοφορίας που επιτρέπει την ροή δεδομένων μεταξύ των τμημάτων. Θα πρέπει να επιτρέπεται μόνο μια ελάχιστη καθορισμένη επισκεψιμότητα (πρωτόκολλα) και κόμβοι (διευθύνσεις). Διατίθενται ειδικές συσκευές για τον αποκλεισμό επιθέσεων άρνηση υπηρεσιών *DoS* (κέντρα καθαρισμού), αλλά απευθύνονται κυρίως σε μεγαλύτερα συστήματα πληροφοριών και ενδέχεται να μην είναι κατάλληλες για βιομηχανικά συστήματα ελέγχου επί πλοίου, υπεράκτιας εγκατάστασης ή τερματικού.

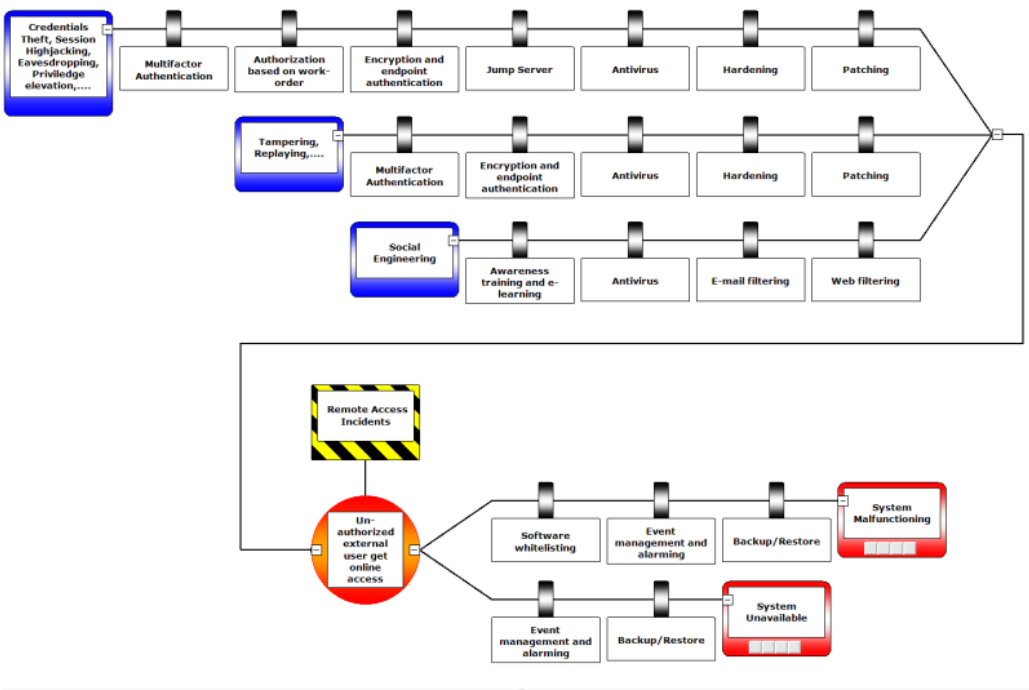
Όπως και με την στρατηγική διαχείρισης άμυνας κατά κακόβουλου λογισμικού, οι ενημερώσεις λογισμικού και η διαχείριση ενημερωμένων εκδόσεων είναι σημαντικές διαδικασίες άμυνας, καθώς και η ενίσχυση των συστημάτων για όλους τους τύπους επιθέσεων. Τυπικά εμπόδια για την αποφυγή υπερφόρτωσης *buffer* είναι η χρήση συσκευών με πιστοποίηση ασφαλείας και η διαμόρφωση των συσκευών σύμφωνα με τις απαιτήσεις του πιστοποιητικού. Η υπερφόρτωση εφαρμογών αντιμετωπίζεται κυρίως στο σχεδιασμό της εφαρμογής. Στη συνέχεια, σε συνδυασμό με ισχυρό ηλεκτρονικό έλεγχο ταυτότητας και έλεγχο εξουσιοδότησης του χρήστη, μπορεί να δημιουργηθεί ένα αποτελεσματικό εμπόδιο στην πλημμύρα εφαρμογών. Προκειμένου να μειωθούν οι συνέπειες μιας επίθεσης *DoS*, πρέπει να εντοπιστεί η ανεπιθύμητη κίνηση και να υπάρχουν ειδικά συστήματα ανίχνευσης εισβολών (*IDS*) ή συστήματα ανίχνευσης *DoS*, αλλά αυτά ενδέχεται να μην είναι κατάλληλα για τα

μικρότερα πλοία και τα υπεράκτια βιομηχανικά συστήματα ελέγχου. Έτσι, μια άλλη προσέγγιση για τον αποκλεισμό μιας επίθεση *DoS* είναι η χρήση απλούστερων συσκευών για την παρακολούθηση της κίνησης του δικτύου και η καθιέρωση διαδικασιών για την παρακολούθηση αυτών των αρχείων καταγραφής. Στη συνέχεια, εάν εντοπιστούν ανωμαλίες, το δίκτυο προέλευσης θα πρέπει να αποκλειστεί και τα συστήματα να αποκατασταθούν.

1.3 Γ. *Barriers for the handling of remote connections* (Στρατηγική άμυνας για την αντιμετώπιση απομακρυσμένης σύνδεσης)

Οι νέες δορυφορικές συνδέσεις καθιστούν δυνατή την απομακρυσμένη συντήρηση εξαρτημάτων ακόμη και όταν το πλοίο βρίσκεται σε λειτουργία. Δημόσια και ιδιωτικά δίκτυα (τηλεφωνία, ασύρματο, κινητό τηλέφωνο και διαδίκτυο) χρησιμοποιούνται ως μέσα μετάδοσης δεδομένων. Εάν αυτά τα σημεία πρόσβασης έχουν σχεδιαστεί ανεπαρκώς, δεν έχουν διαμορφωθεί σωστά ή δεν παρακολουθούνται, εγκληματίες που παρακολουθούν τα τρωτά σημεία του πλοίου ενδέχεται να έχουν πρόσβαση σε μεμονωμένα στοιχεία *ICS*[13] ή στην υποδομή *ICS* με μη εξουσιοδοτημένο τρόπο ώστε να παρακάμπτουν τους μηχανισμούς ασφαλείας. Όταν επιτρέπονταιι τέτοιες συνδέσεις, ενεργοποιείται μια μεγάλη επιφάνεια επίθεσης για κακόβουλους επιτιθέμενους και οι κατάλληλες διαδικασίες άμυνας είναι υποχρεωτικές.

[13] *Industrial Control Systems*: χρησιμοποιούνται στις βιομηχανίες για τον αυτοματοποιημένο και απομακρυσμένο έλεγχο της παραγωγής



Εικόνα 3: Διάγραμμα της άμυνας κατά επίθεσης απομακρυσμένης σύνδεσης (Πηγή: DNV-GL Recommended Practice, 2016)

Στο σενάριο που απεικονίζεται στο παραπάνω σχήμα, ένας κακόβουλος εισβολέας μπορεί να χρησιμοποιήσει παραδοσιακές τεχνικές *hacking* για να αποκτήσει πρόσβαση σε ένα κρίσιμο σύστημα επί του σκάφους. Οι τυπικές διαδικασίες για την πρόληψη τέτοιων περιστατικών είναι πρώτα να διασφαλιστεί η ταυτοποίηση του χειριστή και αυτό γίνεται με την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων *MFA* [14] . Τότε η πρόσβαση παρέχεται μόνο σε περιορισμένο χρονικό διάστημα με βάση την εντολή εργασίας. Η σύνδεση στο διαδίκτυο πρέπει να είναι κρυπτογραφημένη και τα τελικά σημεία επικοινωνίας πρέπει να πιστοποιούνται με ψηφιακά πιστοποιητικά. Στη συνέχεια πρέπει να τοποθετηθεί διακομιστής άλματος (*jump server*) σε ξεχωριστό τμήμα του δικτύου. Η εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας είναι ζωτικής σημασίας καθώς ένας κακόβουλος εισβολέας μπορεί να αποκτήσει διαπιστευτήρια από ανυποψίαστους χρήστες με χρήση κοινωνικής μηχανικής.

[14] Ο έλεγχος ταυτότητας πολλών παραγόντων (*MFA*) προσθέτει ένα επίπεδο προστασίας στη διαδικασία εισόδου. Κατά την πρόσβαση σε λογαριασμούς ή εφαρμογές, οι χρήστες υποβάλλονται σε πρόσθετες ενέργειες επαλήθευσης ταυτότητας, όπως σάρωση δακτυλικού αποτυπώματος ή εισαγωγή κωδικού που λαμβάνεται μέσω τηλεφώνου.

Παράρτημα 2. Χαρτογράφηση συστημάτων *IT & OT*

Α. Χαρτογράφηση συστημάτων *IT*

Στις εικόνες που ακολουθούν παρουσιάζονται παραδείγματα πινάκων που υποστηρίζουν τη χαρτογράφηση συστημάτων *IT* σε διαδικασίες που υποστηρίζονται από τα συστήματα *IT*.

Identifier	*Description of IT supported process*	*Responsible person*	*Users*
P1	Processing of ship administrative information	Master	Officers
P2	IT-System management (admin system, intrusion prevention, etc.)		
P3	Surveillance (physical access control, closed circuit television (CCTV) and personnel on board system)		
P4	Ship communication (e.g. Email, fax, intercom, sat-telephones, mobile phones)		
P5	Information provision via data storage devices (e.g. USB,DVD/CD, portable HDD)		
P6	Maintenance		
P7	Crew entertainment (crew facing networks (entertainment, communication, internet)		
P8	Passenger entertainment (passenger facing networks (entertainment, communication, internet).		
P9	Passenger servicing and management system		
P10	Remote support and access/connectivity (secure connections to onshore) for performing IT support from land based IT department		
P11	...		
...			

Εικόνα 4: Παραδείγματα διαδικασιών που υποστηρίζονται από συστήματα IT(Πηγή: DNV-GL Recommended Practice, 2016)

Identifier	*Description*	*Platform*	*No. of components*	*Installation site*	*Users*	*Admin rights*	*Remote access*	*USB/DVD access*	*Restricted physkcal access*
S1	Group of clients for vessel administration	Windows 7	6	Bridge, cargo control room, etc.	Officers only	Master	Yes or No	Yes or No	Yes or No
S2	Group of servers								

Identifier	*Description*	*Platform*	*No. of components*	*Installation site*	*Users*	*Admin rights*	*Remote access*	*USB/DVD access*	*Restricted physkcal access*
S3	Group of printers								
S4	Group of external HDD								
S5	Group of wireless access points								
S6	Group of firewalls								
S7	Group of IP telephones								
...									

Εικόνα 5: Παράδειγμα απογραφής συστημάτων IT(Πηγή: DNV-GL Recommended Practice, 2016)

Identifier	*Description of IT process*	*IT system*			
		S1	*S2*	*S3*	*S...*
P1	Processing of ship administrative information	x	x	x	
P2	IT-System management (admin system, intrusion prevention, etc.)	x	x	x	
P3	Security control (physical access control, surveillance system, closed circuit television (CCTV) and personnel on board system)	x	x		
P4	Ship communication (e.g. Email, fax, intercom, sat-telephones, mobile phones)	x	x	x	
P5	Information provision via data storage devices (e.g. USB,DVD/CD, portable HDD)	x	x		x
P6	Maintenance	x	x	x	
P7	Crew entertainment (crew facing networks (entertainment, communication, internet)	x	x		
P8	Passenger entertainment (passenger facing networks (entertainment, communication, internet).	x	x	x	
P9	Passenger servicing and management system	x	x		
...					

Εικόνα 6: Παράδειγμα χαρτογράφησης συστημάτων IT(Πηγή: DNV-GL Recommended Practice, 2016)

Β. Χαρτογράφηση συστημάτων ΟΤ

Στις εικόνες 7-9 που ακολουθούν παρουσιάζονται οι λειτουργίες του σκάφους που συνδέονται με τα επιχειρησιακά συστήματα

Vessel function/service	*OT system*
Water tight integrity	— Local and remote control, monitoring and alarm systems for: — water tight doors — shell doors — hatches
Power generation and distribution	— Local and remote control, monitoring and alarm systems for: — engine, turbine, generator, battery and other power sources — auxiliary machinery — Power management system — Power source safety system — Electrical circuit protection system
Propulsion	— Local and remote control, monitoring and alarm system for: — propulsion system (driver, shaft, gear, propeller, etc) — propulsion auxiliary machinery — Propulsion safety system
Steering	— Local and remote control, monitoring and alarm systems for: — steering (rudder, thruster, waterjet, etc.) — steering auxiliaries
Navigation	— Radar — Electronic chart display and information system (ECDIS) — Heading/gyro system — Autopilot — Automatic identification system (AIS) — Position reference system (GPS, etc.) — Voyage data recorder (VDR) — Bridge navigation watch alarm system (BNWAS) — CCTV — Navigation light system — Weather routing assistance system
Communication	— External communication system (GMDSS, satellite, radio etc.) — Internal communication system (PA, GA, telephone, radio etc.)
Drainage and bilge pumping	— Local and remote control, monitoring and alarm systems for bilge pumps, valve, sensors — Water ingress monitoring and alarm system

Εικόνα 7: Παραδείγματα λειτουργιών του σκάφους που συνδέονται με συστήματα ΟΤ (Πηγή: DNV-GL Recommended Practice, 2016)

Vessel function/service	*OT system*
Ballasting	– Local and remote control, monitoring and alarm systems for ballast pumps, valve, sensors – Load calculation system
Anchoring	– Anchor and winch control and monitoring system – Position mooring control system
Cargo operation	– Local and remote control, monitoring and alarm systems for cargo pumps, valve – Cargo level, pressure and temperature monitoring and alarm system – Cargo tank and other cargo-related safety systems – Inert gas control and monitoring system – Loading and offloading control and monitoring system – Crane control and monitoring system – Cargo conditioning, temperature, ventilation system
Fire and gas	– Fire detection system – Gas detection system (gas fuel) – Fire door control and monitoring system – Fire pump control and monitoring – Fire extinguishing systems
Ignition source control	– Gas detection system – Emergency shutdown system
Accommodation and passenger	– Ventilation and climate control system – Emergency safety/response system – Flooding detection system

Dynamic positioning	– Local and remote control, monitoring and alarm system for:
	  – DP-thrusters and other driven units for positioning
	  – auxiliary machinery
	– DP control system
	– Independent joystick system
	– DP sensors and reference systems

Drilling	– Hoisting control and monitoring system – Rotation control and monitoring system – Vertical pipe handling control and monitoring system – Horizontal pipe handling control and monitoring system – Well control and monitoring system – Mud and shaker control and monitoring system – Well intervention control and monitoring system – Manage pressure drilling control and monitoring system – Heave compensation control and monitoring system

Εικόνα 8: Παραδείγματα λειτουργιών του σκάφους που συνδέονται με συστήματα ΟΤ (Πηγή: DNV-GL Recommended Practice, 2016)

Vessel function/service	*OT system*
Oil and gas production	– Process control and monitoring system – Production safety system – Production skid local control and monitoring system – Production skid safety system – Subsea control and monitoring system – High integrity pressure protection system (HIPPS)
Other	– Auxiliary boiler control and monitoring system – Auxiliary safety system – Incinerator control and monitoring system – Main alarm system – Integrated control, monitoring, alarm and safety system – CCTV – Jacking control and monitoring system – Pollution prevention system

Εικόνα 9: Παραδείγματα λειτουργιών του σκάφους που συνδέονται με συστήματα ΟΤ (Πηγή: DNV-GL Recommended Practice, 2016)

Παράρτημα 3. Απαιτήσεις σύμφωνα με το *BSI* για συστήματα *IT*

Το *BSI* είναι το Γερμανικό Ομοσπονδιακό Γραφείο για την ασφάλεια πληροφοριών, οι λίστες *IT-GS* αφορούν τις εξελίξεις στον τομέα των πληροφοριακών συστημάτων για τις οποίες οι κυβερνητικές υπηρεσίες και εταιρείες καλούνται να βρουν λύσεις, λαμβάνοντας υπόψη το κόστος και την ασφάλεια των χρηστών. Στις εικόνες που ακολουθούν παρουσιάζονται οι απαιτήσεις για τα συστήματα *IT*.

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.101 General server	S 2.22	Escrow of passwords			×
S 3.101 General server	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 3.101 General server	S 4.24	Ensuring consistent system management	×	×	×
S 3.101 General server	S 4.93	Regular integrity checking			×
S 3.101 General server	S 4.238	Use of local packet filters	×	×	×
S 3.101 General server	S 4.239	Secure operation of a server	×	×	×
S 3.101 General server	S 4.240	Setting up a testing environment for servers			×
S 3.101 General server	S 5.8	Regular security checks of the network		×	×
S 3.101 General server	S 5.9	Logging on the server		×	×
S 3.102 Servers under Unix	S 4.25	Use of logging in Unix systems	×	×	×
S 3.102 Servers under Unix	S 4.26	Regular security checks of Unix systems			×
S 3.107 S/390 and zSeries mainframes	S 2.291	Security reporting and security audits under z/OS			×
S 3.107 S/390 and zSeries mainframes	S 2.292	Monitoring of z/OS systems		×	×
S 3.107 S/390 and zSeries mainframes	S 2.293	Maintenance of zSeries systems			×
S 3.107 S/390 and zSeries mainframes	S 2.294	Synchronisation of z/OS passwords and RACF commands			×
S 3.107 S/390 and zSeries mainframes	S 4.210	Secure operation of the z/OS operating system		×	×
S 3.107 S/390 and zSeries mainframes	S 4.214	Administration of data media under z/OS systems		×	×

Εικόνα 10: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Εικόνα 11: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.107 S/390 and zSeries mainframes	S 4.215	Protection of z/OS utilities that are critical to security		×	×
S 3.107 S/390 and zSeries mainframes	S 4.218	Information on character set conversion in z/OS systems			×
S 3.108 Windows Server 2003	S 2.368	Handling of administrative templates under Windows Server 2003 and higher			×
S 3.108 Windows Server 2003	S 2.369	Regular security-relevant maintenance of a Windows Server 2003	×	×	×
S 3.108 Windows Server 2003	S 2.370	Administration of access rights under Windows Server 2003 and higher	×	×	×
S 3.108 Windows Server 2003	S 4.56	Secure deletion under Windows operating systems			×
S 3.109 Windows Server 2008	S 2.368	Handling of administrative templates under Windows Server 2003 and higher			×
S 3.109 Windows Server 2008	S 2.369	Regular security-relevant maintenance of a Windows Server 2003	×	×	×
S 3.109 Windows Server 2008	S 2.370	Administration of access rights under Windows Server 2003 and higher	×	×	×
S 3.109 Windows Server 2008	S 4.56	Secure deletion under Windows operating systems			×
S 3.109 Windows Server 2008	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server 2008 and higher versions			×

Εικόνα 12: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.109 Windows Server 2008	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×
S 3.109 Windows Server 2008	S 4.411	Secure use of DirectAccess under Windows			×
S 3.109 Windows Server 2008	S 4.415	Secure operation of biometric authentication under Windows			×
S 3.109 Windows Server 2008	S 4.416	Use of Windows Server Core			×
S 3.109 Windows Server 2008	S 4.417	Patch Management with WSUS under Windows Server 2008 and higher		×	×
S 3.201 General client	S 3.18	Log-out obligation for PC users	×	×	×
S 3.201 General client	S 4.2	Screen lock	×	×	×
S 3.201 General client	S 4.3	Use of virus protection programs	×	×	×
S 3.201 General client	S 4.4	Correct handling of drives for removable media and external data storage			×
S 3.201 General client	S 4.200	Handling of USB storage media			×
S 3.201 General client	S 4.238	Use of local packet filters	×	×	×
S 3.201 General client	S 4.241	Secure operation of clients	×	×	×
S 3.201 General client	S 4.242	Setting up a reference installation for clients			×

Εικόνα 13: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.201 General client	S 5.45	Secure use of browsers		×	×
S 3.202 General stand-alone IT systems	S 2.22	Escrow of passwords			×
S 3.202 General stand-alone IT systems	S 3.18	Log-out obligation for PC users	×	×	×
S 3.202 General stand-alone IT systems	S 4.2	Screen lock	×	×	×
S 3.202 General stand-alone IT systems	S 4.4	Correct handling of drives for removable media and external data storage			×
S 3.202 General stand-alone IT systems	S 4.30	Utilisation of the security functions offered in application programs	×	×	×
S 3.203 Laptop	S 1.33	Safe keeping of laptop PCs during mobile use	×	×	×
S 3.203 Laptop	S 1.34	Safe keeping of laptop PCs during stationary use	×	×	×
S 3.203 Laptop	S 1.35	Pooled storage of portable IT systems			×
S 3.203 Laptop	S 1.46	Use of anti-theft devices			×
S 3.203 Laptop	S 4.3	Use of virus protection programs	×	×	×
S 3.203 Laptop	S 4.27	Laptop access protection	×	×	×
S 3.203 Laptop	S 4.28	Software reinstallation in the case of change of laptop users			×

Εικόνα 14: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.203 Laptop	S 4.31	Ensuring power supply during mobile use	×	×	×
S 3.203 Laptop	S 4.235	Comparison of stored data on laptops		×	×
S 3.203 Laptop	S 4.236	Central administration of laptops			×
S 3.203 Laptop	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.204 Unix client	S 4.25	Use of logging in Unix systems	×	×	×
S 3.204 Unix client	S 4.26	Regular security checks of Unix systems			×
S 3.208 Internet PCs	S 2.313	Secure registration with Internet services	×	×	×
S 3.208 Internet PCs	S 4.3	Use of virus protection programs	×	×	×
S 3.208 Internet PCs	S 4.152	Secure operation of Internet PCs		×	×
S 3.208 Internet PCs	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 3.208 Internet PCs	S 5.93	Security issues relating to the use of web browsers by Internet PCs	×	×	×
S 3.208 Internet PCs	S 5.94	Security issues relating to the use of e-mail clients by Internet PCs	×	×	×
S 3.208 Internet PCs	S 5.95	Secure e-commerce using Internet PCs		×	×
S 3.208 Internet PCs	S 5.96	The secure use of webmail	×	×	×

Εικόνα 15: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.209 Windows XP client	S 2.329	Introduction of Windows XP SP2	×	×	×
S 3.209 Windows XP client	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.209 Windows XP client	S 4.56	Secure deletion under Windows operating systems			×
S 3.209 Windows XP client	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.209 Windows XP client	S 4.148	Monitoring a Windows 2000/XP system		×	×
S 3.209 Windows XP client	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.210 Windows Vista client	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.210 Windows Vista client	S 2.443	Implementation of Windows Vista SP1	×	×	×
S 3.210 Windows Vista client	S 4.56	Secure deletion under Windows operating systems			×
S 3.210 Windows Vista client	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.210 Windows Vista client	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.210 Windows Vista client	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server 2008 and higher versions			×
S 3.210 Windows Vista client	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×

Εικόνα 16: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.211 Client under Mac OS X	S 2.359	Monitoring and administration of storage systems		×	×
S 3.211 Client under Mac OS X	S 2.360	Security audits and reporting for storage systems		×	×
S 3.211 Client under Mac OS X	S 4.275	Secure operation of storage systems	×	×	×
S 3.212 Clients under Windows 7 or higher	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.212 Clients under Windows 7 or higher	S 4.56	Secure deletion under Windows operating systems			×
S 3.212 Clients under Windows 7 or higher	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server			×
S 3.212 Clients under Windows 7 or higher	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×
S 3.212 Clients under Windows 7 or higher	S 4.420	Secure use of the Maintenance Center under Windows 7	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.422	Use of BitLocker To Go in Windows 7 and higher			×

Εικόνα 17: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.301 Security gateway (firewall)	S 2.78	Secure operation of a firewall	×	×	×
S 3.301 Security gateway (firewall)	S 2.302	Security gateways and high availability			×
S 3.301 Security gateway (firewall)	S 4.47	Logging of security gateway activities	×	×	×
S 3.301 Security gateway (firewall)	S 4.100	Security gateways and active content			×
S 3.301 Security gateway (firewall)	S 4.101	Firewalls and encryption			×
S 3.301 Security gateway (firewall)	S 4.222	Correct configuration of security proxies		×	×
S 3.301 Security gateway (firewall)	S 4.223	Integration of proxy servers into the security gateway		×	×
S 3.301 Security gateway (firewall)	S 4.225	Use of a logging server on a security gateway			×
S 3.301 Security gateway (firewall)	S 4.226	Integration of virus scanners into a security gateway			×
S 3.301 Security gateway (firewall)	S 4.227	Use of a local NTP server for time synchronisation			×

Εικόνα 18: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.301 Security gateway (firewall)	S 5.39	Secure use of protocols and services	×	×	×
S 3.301 Security gateway (firewall)	S 5.46	Installing stand-alone-systems for Internet use	×	×	×
S 3.301 Security gateway (firewall)	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 3.301 Security gateway (firewall)	S 5.70	Network address translation (NAT)	×	×	×
S 3.301 Security gateway (firewall)	S 5.71	Intrusion detection and intrusion response system			×
S 3.301 Security gateway (firewall)	S 5.115	Integration of a web server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.116	Integration of an email server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.117	Integration of a database server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.118	Integration of a DNS server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.119	Integration of a web application with web, application, and database servers into a security gateway			×

Εικόνα 19: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.301 Security gateway (firewall)	S 5.120	Handling of ICMP on the security gateway	×	×	×
S 3.303 Storage systems and storage networks	S 2.359	Monitoring and administration of storage systems		×	×
S 3.303 Storage systems and storage networks	S 2.360	Security audits and reporting for storage systems		×	×
S 3.303 Storage systems and storage networks	S 4.275	Secure operation of storage systems	×	×	×
S 3.304 Virtualisation	S 2.448	Monitoring the function and configuration of virtual infrastructures		×	×
S 3.304 Virtualisation	S 2.449	Minimum use of console accesses to virtual IT systems			×
S 3.304 Virtualisation	S 4.348	Time synchronisation in virtual IT systems			×
S 3.304 Virtualisation	S 4.349	Secure operation of virtual infrastructures	×	×	×
S 3.305 Terminal servers	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 3.305 Terminal servers	S 4.3	Use of virus protection programs	×	×	×
S 3.305 Terminal servers	S 4.367	Secure use of client applications for terminal servers		×	×

Εικόνα 20: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.305 Terminal servers	S 4.367	Secure use of client applications for terminal servers		×	×
S 3.305 Terminal servers	S 4.368	Regular audits of the terminal server environment		×	×
S 3.305 Terminal servers	S 5.164	Secure use of a terminal server from a remote network		×	×
S 3.401 Telecommunications system	S 3.82	Training on the secure use of PBX systems		×	×
S 3.401 Telecommunications system	S 4.5	Logging for PBX systems		×	×
S 3.401 Telecommunications system	S 4.6	Audit of the PBX configuration			×
S 3.402 Fax machine	S 2.48	Designating authorised fax operators			×
S 3.402 Fax machine	S 2.51	Producing copies of incoming fax messages			×
S 3.402 Fax machine	S 2.52	Supply and monitoring of consumables			×
S 3.402 Fax machine	S 2.53	Deactivation of fax machines after office hours			×
S 3.402 Fax machine	S 4.43	Fax machine with automatic envelopment sealing system			×
S 3.402 Fax machine	S 5.24	Use of a suitable fax cover sheet			×
S 3.402 Fax machine	S 5.25	Using transmission and reception logs	×	×	×
S 3.402 Fax machine	S 5.26	Announcing fax messages via telephone			×

Εικόνα 21: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.402 Fax machine	S 5.29	Periodic checks of destination addresses and logs			×
S 3.404 Mobile telephones	S 2.189	Blocking of the mobile phone in the event of its loss	×	×	×
S 3.404 Mobile telephones	S 4.115	Safeguarding the power supply of mobile phones		×	×
S 3.404 Mobile telephones	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.404 Mobile telephones	S 5.78	Protection against mobile phone usage data being used to create movement profiles			×
S 3.404 Mobile telephones	S 5.79	Protection against call number identification during use of mobile phones			×
S 3.404 Mobile telephones	S 5.80	Protection against bugging of indoor conversations using mobile phones			×
S 3.404 Mobile telephones	S 5.81	Secure transmission of data over mobile phones		×	×
S 3.405 PDA	S 1.33	Safe keeping of laptop PCs during mobile use	×	×	×
S 3.405 PDA	S 4.3	Use of virus protection programs	×	×	×
S 3.405 PDA	S 4.31	Ensuring power supply during mobile use	×	×	×
S 3.405 PDA	S 4.228	Using the built-in security mechanisms on PDAs	×	×	×
S 3.405 PDA	S 4.229	Secure operation of PDAs			×
S 3.405 PDA	S 4.230	Central administration of PDAs			×

Εικόνα 22: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 3.405 PDA	S 4.232	Secure use of extended memory cards			×
S 3.405 PDA	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.406 Printers, copiers, and all-in-one devices	S 2.52	Supply and monitoring of consumables			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.302	Logging on printers, copiers, and all-in-one devices			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.303	Use of network-enabled document scanners			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.304	Administration of printers			×
S 3.406 Printers, copiers, and all-in-one devices	S 5.146	Network separation when using all-in-one devices			×

Εικόνα 23: Απαιτήσεις για συστήματα IT σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Ακολουθούν οι απαιτήσεις για συστήματα *IT* επιπέδου 4.

Module 4 - Networks	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 4.1 Heterogeneous networks	S 4.81	Auditing and logging of activities in a network		×	×
S 4.1 Heterogeneous networks	S 4.83	Updating/upgrading of software and hardware in network components			×
S 4.2 Network- and System management	S 2.146	Secure operation of a network management system	×	×	×

Εικόνα 24: Απαιτήσεις για συστήματα IT module 4 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 4 - Networks	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 4.2 Network- and System management	S 4.92	Secure operation of a system management system	×	×	×
S 4.3 Modem	S 2.60	Secure administration of a modem	×	×	×
S 4.3 Modem	S 3.17	Briefing personnel on modem usage	×	×	×
S 4.3 Modem	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 4.3 Modem	S 5.44	One-way connection setup			×
S 4.4 VPN	S 4.321	Secure operation of a VPN	×	×	×
S 4.5 LAN connection of an IT system via ISDN	S 5.29	Periodic checks of destination addresses and logs			×
S 4.6 WLAN	S 2.388	Appropriate key management for WLAN		×	×
S 4.6 WLAN	S 2.389	Secure use of hotspots			×
S 4.6 WLAN	S 4.293	Secure operation of hotspots			×
S 4.6 WLAN	S 4.296	Use of a suitable management solution for WLAN			×
S 4.6 WLAN	S 4.297	Secure operation of WLAN components	×	×	×
S 4.6 WLAN	S 4.298	Regular audits of WLAN components		×	×
S 4.6 WLAN	S 5.141	Regular security checks of WLANs		×	×

Εικόνα 25: Απαιτήσεις για συστήματα IT module 4 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 4.7 VoIP	S 3.12	Informing all staff members about possible PBX warning notices, warning symbols, and acoustic alarm signals		×	×
S 4.7 VoIP	S 3.13	Increasing staff awareness of potential threats to the PBX		×	×
S 4.7 VoIP	S 4.5	Logging for PBX systems		×	×
S 4.7 VoIP	S 4.6	Audit of the PBX configuration			×
S 4.7 VoIP	S 4.291	Secure configuration of VoIP middleware	×	×	×
S 4.7 VoIP	S 4.292	Logging of VoIP events	×	×	×
S 4.8 Bluetooth	S 2.463	Use of a central pool of Bluetooth peripheral devices			×
S 4.8 Bluetooth	S 4.363	Secure operation of Bluetooth devices	×	×	×

Εικόνα 26: Απαιτήσεις για συστήματα IT module 4 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Ακολουθούν οι απαιτήσεις για συστήματα *IT* επιπέδου 5.

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.2 Exchange of data media	S 1.36	Safekeeping of data media before and after dispatch	×	×	×
S 5.2 Exchange of data media	S 2.43	Adequate labelling of data media for dispatch	×	×	×
S 5.2 Exchange of data media	S 2.44	Secure packaging of data media	×	×	×

Εικόνα 27: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.2 Exchange of data media	S 3.14	Briefing personnel on correct procedures of exchanging data media		×	×
S 5.2 Exchange of data media	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.2 Exchange of data media	S 4.35	Pre-dispatch verification of the data to be transferred			×
S 5.3 Groupware	S 3.76	Basic user training on how to use groupware and e-mail			×
S 5.3 Groupware	S 4.199	Avoiding problematic file formats		×	×
S 5.3 Groupware	S 4.357	Secure operation of groupware systems	×	×	×
S 5.3 Groupware	S 4.358	Logging groupware systems		×	×
S 5.3 Groupware	S 5.54	Dealing with unwanted e-mails		×	×
S 5.3 Groupware	S 5.56	Secure operation of a mail server	×	×	×
S 5.3 Groupware	S 5.108	Cryptographic protection of groupware and/or e-mail			×
S 5.3 Groupware	S 5.109	Use of an e-mail scanner on the mail server			×
S 5.4 Web servers	S 2.174	Secure operation of a web server	×	×	×
S 5.4 Web servers	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×

Εικόνα 28: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 5.4 Web servers	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.4 Web servers	S 4.78	Careful modifications of configurations	×	×	×
S 5.4 Web servers	S 4.177	Assuring the integrity and authenticity of software packages		×	×
S 5.4 Web servers	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 5.5 Lotus Notes/Domino	S 4.128	Secure operation of the Lotus Notes/Domino environment	×	×	×
S 5.5 Lotus Notes/Domino	S 4.132	Monitoring the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.426	Archiving for the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.427	Security-relevant logging and evaluating for Lotus Notes/Domino			×
S 5.5 Lotus Notes/Domino	S 4.428	Audit of the Lotus Notes/Domino environment			×
S 5.6 Fax servers	S 5.24	Use of a suitable fax cover sheet			×
S 5.6 Fax servers	S 5.25	Using transmission and reception logs	×	×	×
S 5.6 Fax servers	S 5.26	Announcing fax messages via telephone			×
S 5.6 Fax servers	S 5.27	Acknowledging successful fax reception via telephone			×

Εικόνα 29: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.6 Fax servers	S 5.28	Acknowledging correct fax origin via telephone			×
S 5.6 Fax servers	S 5.73	Secure operation of a fax server	×	×	×
S 5.6 Fax servers	S 5.74	Maintenance of fax server address books and distribution lists	×	×	×
S 5.6 Fax servers	S 5.75	Protecting against overloading the fax server			×
S 5.7 Databases	S 2.31	Documentation of authorised users and rights profiles	×	×	×
S 5.7 Databases	S 2.34	Documentation on changes made to an existing IT system	×	×	×
S 5.7 Databases	S 2.65	Checking the efficiency of user separation on an IT system			×
S 5.7 Databases	S 2.127	Inference prevention		×	×
S 5.7 Databases	S 2.128	Controlling access to a database system	×	×	×
S 5.7 Databases	S 2.129	Controlling access to database information	×	×	×
S 5.7 Databases	S 2.130	Ensuring the integrity of a database	×	×	×
S 5.7 Databases	S 2.131	Separation of administrative tasks for database systems			×
S 5.7 Databases	S 2.133	Checking the log files of a database system	×	×	×
S 5.7 Databases	S 3.18	Log-out obligation for PC users	×	×	×

Εικόνα 30: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 5.7 Databases	S 4.67	Locking and deleting database accounts which are no longer required		×	×
S 5.7 Databases	S 4.68	Ensuring consistent database management	×	×	×
S 5.7 Databases	S 4.69	Regular checks of database security		×	×
S 5.7 Databases	S 4.70	Monitoring a database			×
S 5.7 Databases	S 4.72	Database encryption			×
S 5.7 Databases	S 5.117	Integration of a database server into a security gateway			×
S 5.8 Telecommuting	S 3.21	Training of telecommuters as regards security-related issues	×	×	×
S 5.9 Novell eDirectory	S 4.159	Secure operation of Novell eDirectory	×	×	×
S 5.9 Novell eDirectory	S 4.160	Monitoring of Novell eDirectory		×	×
S 5.9 Novell eDirectory	S 5.97	Protection of communications with Novell eDirectory		×	×
S 5.12 Microsoft Exchange/ Outlook	S 2.482	Regular security checks of Exchange systems		×	×
S 5.12 Microsoft Exchange/ Outlook	S 4.166	Secure operation of Exchange systems	×	×	×

Εικόνα 31: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.13 SAP System	S 2.347	Regular security checks of SAP systems		×	×
S 5.13 SAP System	S 2.348	Security aspects relating to the customisation of SAP systems			×
S 5.13 SAP System	S 2.349	Secure software development for SAP systems			×
S 5.13 SAP System	S 4.270	Logging of SAP events	×	×	×
S 5.13 SAP System	S 4.271	Computer virus protection for SAP systems			×
S 5.13 SAP System	S 4.272	Secure use of the SAP transport system	×	×	×
S 5.13 SAP System	S 4.273	Secure use of the SAP Java Stack software deployment	×	×	×
S 5.14 Mobile data media	S 3.60	Sensitising staff to secure handling of mobile data media and devices			×
S 5.14 Mobile data media	S 4.4	Correct handling of drives for removable media and external data storage			×
S 5.14 Mobile data media	S 4.200	Handling of USB storage media			×
S 5.14 Mobile data media	S 4.232	Secure use of extended memory cards			×
S 5.15 General directory service	S 4.78	Careful modifications of configurations	×	×	×
S 5.15 General directory service	S 4.311	Secure operation of directory services	×	×	×
S 5.15 General directory service	S 4.312	Monitoring directory services		×	×

Εικόνα 32: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 5.15 General directory service	S 5.147	Protection of communications with directory services			×
S 5.16 Active Directory	S 4.138	Configuration of Windows Server as a domain controller	×	×	×
S 5.16 Active Directory	S 4.315	Maintenance of the operational reliability of an Active Directory	×	×	×
S 5.16 Active Directory	S 4.316	Monitoring the Active Directory infrastructure		×	×
S 5.17 Samba	S 4.335	Secure operation of a Samba server		×	×
S 5.18 DNS-Server	S 2.8	Assignment of access rights	×	×	×
S 5.18 DNS-Server	S 2.35	Obtaining information on security weaknesses of the system		×	×
S 5.18 DNS-Server	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 5.18 DNS-Server	S 4.78	Careful modifications of configurations	×	×	×
S 5.18 DNS-Server	S 4.354	Monitoring of a DNS server		×	×
S 5.18 DNS-Server	S 5.118	Integration of a DNS server into a security gateway			×
S 5.19 Internet use	S 2.313	Secure registration with Internet services	×	×	×
S 5.19 Internet use	S 5.45	Secure use of browsers		×	×

Image 33: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.19 Internet use	S 5.155	Data protection aspects when using the Internet			×
S 5.19 Internet use	S 5.156	Secure use of Twitter			×
S 5.19 Internet use	S 5.157	Secure use of social networks			×
S 5.19 Internet use	S 5.158	Use of web disk space			×
S 5.19 Internet use	S 5.173	Use of short URLs and QR codes			×
S 5.20 OpenLDAP	S 4.390	Secure updating of OpenLDAP			×
S 5.20 OpenLDAP	S 4.391	Secure operation of OpenLDAP		×	×
S 5.20 OpenLDAP	S 4.407	Logging when using OpenLDAP		×	×
S 5.20 OpenLDAP	S 5.170	Secure communication connections when using OpenLDAP			×
S 5.21 Web applications	S 2.8	Assignment of access rights	×	×	×
S 5.21 Web applications	S 2.31	Documentation of authorised users and rights profiles	×	×	×
S 5.21 Web applications	S 2.34	Documentation on changes made to an existing IT system	×	×	×
S 5.21 Web applications	S 2.35	Obtaining information on security weaknesses of the system		×	×
S 5.21 Web applications	S 2.64	Checking the log files	×	×	×

Εικόνα 34: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)

S 5.22 Logging	S 2.110	Data protection guidelines for logging procedures	×	×	×
S 5.22 Logging	S 4.225	Use of a logging server on a security gateway			×
S 5.22 Logging	S 4.227	Use of a local NTP server for time synchronisation			×
S 5.22 Logging	S 4.430	Analysing the logged data	×	×	×
S 5.22 Logging	S 4.431	Selecting and processing relevant information for logging	×	×	×
S 5.22 Logging	S 5.9	Logging on the server		×	×

Εικόνα 35: Απαιτήσεις για συστήματα IT module 5 σύμφωνα με το γραφείο BSI (Πηγή: DNV-GL Recommended Practice, 2016)