ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«Ασφάλεια Ψηφιακών Συστημάτων»

Ονοματεπώνυμο Σπουδαστή:

ΣΟΦΙΑ ΜΑΛΤΕΖΟΥ

Ονοματεπώνυμο Υπεύθυνου Καθηγητή:

ΧΡΙΣΤΟΦΟΡΟΣ ΝΤΑΝΤΟΓΙΑΝ

Τίτλος Διπλωματικής Εργασίας:

ΕΠΙΓΝΩΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΗ ΝΑΥΤΙΛΙΑ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Σε αυτή την εργασία θα αναλυθούν τα τελευταία πιστοποιητικά που προορίζονται για τον τομέα της Ναυτιλίας και αφορούν στην ενημέρωση για θέματα ασφάλειας καθώς και την πιστοποίηση για την προστασία πληροφοριακών συστημάτων και δικτύων.

Πίνακας Περιεχομένων

Ακρωνύμια

ICS - Industrial Control Systems
IT – Information Technology
OT - Operational Technology
CDI – Chemical Distribution Institute
IMO – International Maritime Organization
TMSA – Tanker Management Self-Assessment
ABS – American Bureau of Shipping
DNV – Det Norsk Veritas
BIMCO – Baltic and International Maritime Council
ISPS – International Ship and Port Security
ISM - International Security Management
ICT – Information and Communication Technology
SIRE – Ship Inspection Reporting Program
SMS – Safety Management System
PDCA – Plan, Do, Check, Act
ISMS – Information Security Management System
VISHING – Voice Phishing
DMAIC – Define, Measure, Analyze, Increase, Control
IoT – Internet of Things
AIS – Automatic Identification System
GMDSS – Global Maritime Distress and Safety System
ECDIS – Electronic Chart Display and Information System
GNSS – Global Navigation Satellite System
GPS – Global Positioning System
OCIMF – Oil Companies International Marine Forum
DoS – Denial of Service
CIA – Confidentiality, Integrity, Availability
NIST – National Institute of Standards and Technology

1. Εισαγωγή

Ο Διεθνής Οργανισμός Ναυτιλίας - IMO έχει αναγνωρίσει την επείγουσα ανάγκη να αυξηθεί η ευαισθητοποίηση σχετικά με απειλές και επιθέσεις του κυβερνοχώρου στις δραστηριότητες της ναυτιλίας, καθώς αυτές ολοένα και περισσότερο εκτίθενται στο διαδίκτυο. Αυτό συμβαίνει λόγω της ανάγκης διασύνδεσης πέρα των πληροφοριακών συστημάτων και των λειτουργικών συστημάτων του πλοίου στη στεριά.

Επίσης, έχει αναγνωρίσει την ανάγκη να εργαστούν μαζί όλοι οι εμπλεκόμενοι στις διαδικασίες της ναυτιλίας, όπως αυτοί είναι οι ναυτιλιακές, οι λιμενικές αρχές, οι κατασκευαστές κ.α., για να εξασφαλίσουν την ασφάλεια του πλοίου από πιθανούς κινδύνους κυβερνοεπίθεσης, καθώς αυτή θα μπορούσε να είναι καταστροφική για την ανθρώπινη ζωή των πληρωμάτων, την περιουσία του πλοιοκτήτη και του φορτίου αλλά και τις λειτουργικές διαδικασίες της διαχειριστικής αλυσίδας.

Για αυτό το λόγο, ο IMO εξέδωσε νομοθεσία μέσω της επιτροπής του για την ασφάλεια της ναυτιλίας, η οποία εφαρμόστηκε στις 16 Ιουνίου 2017 και είναι η **Resolution MSC.428(98)**. Σύμφωνα με τον κανονισμό αυτό, οι ναυτιλιακές εταιρείες θα πρέπει να έχουν σχέδιο διαχείρισης ρίσκου για τους κινδύνους στον κυβερνοχώρο, ώστε αυτοί να αντιμετωπίζονται κατάλληλα. Το πλάνο της εταιρείας θα πρέπει να βρίσκεται στα συστήματα διαχείρισης της ασφάλειας (Safety Management System – SMS) του πλοίου και να έχει εγκριθεί όχι το αργότερο από την 1η Ιανουαρίου του 2021. Ήδη πολλές ναυτιλιακές εταιρείες έχουν προετοιμαστεί κατάλληλα και οργανώνονται σχετικά, καθώς υπάρχουν απαιτήσεις από τους φορτωτές σχετικά με τις δραστηριότητες των ναυτιλιακών εταιρειών όσον αφορά την κυβερνοασφάλεια.

Επιπλέον, η **OCIMF -** Oil Companies International Marine Forum έχει προχωρήσει στην 3η έκδοση του Tanker Management and Self- Assessment (**TMSAv3**) [9], όπου στο κεφάλαιο 13 συμπεριλαμβάνει ελέγχους ασφαλείας για θέματα κυβερνοασφάλειας τα οποία είναι σύμφωνα με πρότυπα διεθνών οργανισμών όπως αυτά του NIST, της BIMCO, InterTanko, ISMS ISO 27001 κ.α.

Οι ναυτιλιακές εταιρείες μεταφοράς προϊόντων πετρελαίου υποχρεούνται να ακολουθήσουν τις οδηγίες του TMSA και να αυτοπροσδιοριστούν σε κάποιο από τα 4 επίπεδά του, με το 4 να είναι το υψηλότερο από αυτά, έτσι ώστε να μπορούν να ανεβαίνουν σε κατατάξεις του OCIMF και να επιλέγονται με μεγαλύτερη ευκολία από τους φορτωτές.

Το εγχειρίδιο κυβερνοασφάλειας βρίσκεται στο SMS Manual (Safety Management System) της εταιρείας και είναι αποτέλεσμα συμβούλων ή οργανωμένου τμήματος πληροφορικής.

Επίσης, τα τμήματα πληροφορικής έχουν ένα αγώνα να οργανώσουν το περιβάλλον πληροφορικής του πλοίου αλλά και να το συντηρούν ώστε να είναι ασφαλές, ενώ ταυτόχρονα όλες οι εργασίες πρέπει να γίνονται με απομακρυσμένο τρόπο καθιστώντας το έργο τους πολύ δύσκολο.

Αυτή τη στιγμή οι επιθεωρητές πλοίων δίνουν μεγάλο βάρος στις θύρες USB των Information Technology (IT) και των Operational Technology (OT) συστημάτων αλλά και στην γνώση των πληρωμάτων σχετικά με θέματα κυβερνοασφάλειας, γράφοντας πολλές φορές παρατηρήσεις με συστάσεις σχετικά.
Ως αποτέλεσμα, οι ναυτιλιακές χρησιμοποιούν «τάπες» για τις θύρες USB ή εξειδικευμένες εφαρμογές ασφαλείας και αφίσες (cyber security awareness) για την ενημέρωση του προσωπικού πλοίου. Επιπροσθέτως, υπάρχει συστηματική ενημέρωση τόσο στο περιβάλλον του πλοίου, όσο και του γραφείου μέσω newsletter, αφίσες κλπ. σχετικά με επιθέσεις κυβερνοασφάλειας και διαδικασίες αναγνώρισης phishing/spam emails.

2. Cyber Security στην Ναυτιλία

Η ναυτιλιακή βιομηχανία διαθέτει μια σειρά χαρακτηριστικών που επηρεάζουν την ευπάθειά της σε περιστατικά κυβερνοεπιθέσεων:

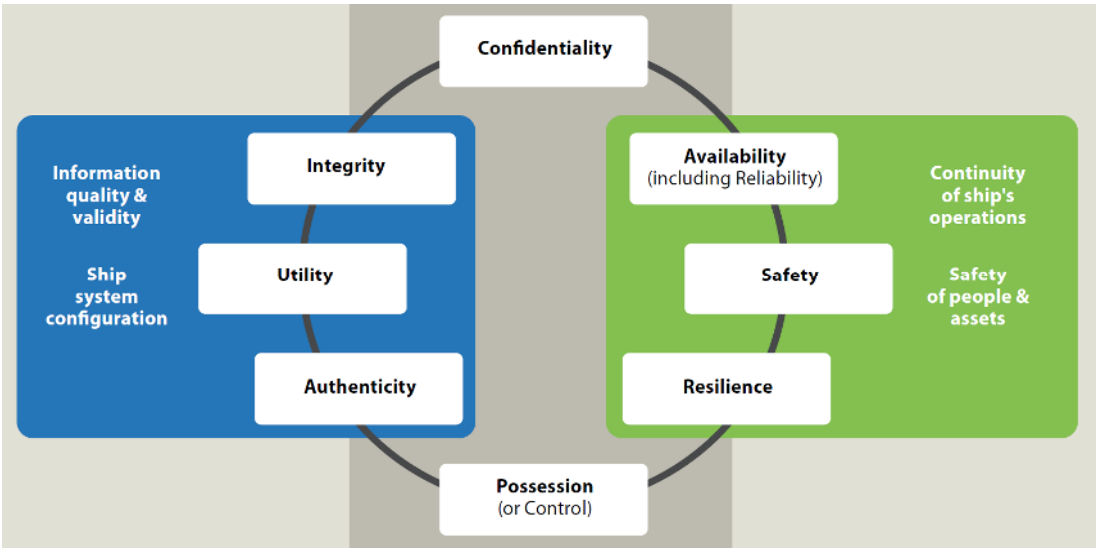
- Τα ενδιαφερόμενα μέρη (stakeholders) εμπλέκονται συχνά στη λειτουργία και τη ναύλωση ενός πλοίου, κάτι το οποίο ενδέχεται να οδηγήσει σε έλλειψη λογοδοσίας/ευθύνης για την υποδομή πληροφορικής

- Το πλοίο είναι πλέον διασυνδεδεμένο και ο τρόπος διασύνδεσης του με άλλα μέρη της παγκόσμιας αλυσίδας εφοδιασμού.

- Κρίσιμες και εμπορικά ευαίσθητες πληροφορίες για την επιχείρηση που διαμοιράζονται με παρόχους υπηρεσιών στην ξηρά.

- Η διαθεσιμότητα και η χρήση κρίσιμων υπολογιστικών συστημάτων για την ασφάλεια του πλοίου και για την προστασία του περιβάλλοντος.

- Η αυξανόμενη χρήση των δεδομένων (big data), των έξυπνων/αυτόνομων πλοίων(smart ships) και των IoT (Internet of Things) αυξάνει τον όγκο των πληροφοριών που διατίθενται στους hackers στον κυβερνοχώρο, καθιστώντας την ανάγκη για ισχυρές προσεγγίσεις για την ασφάλεια στον κυβερνοχώρο.



Δεδομένου ότι η ασφάλεια, οι περιβαλλοντικές και εμπορικές συνέπειες της μη προετοιμασίας για ένα συμβάν στον κυβερνοχώρο μπορεί να είναι τρομερές, είναι επιτακτική ανάγκη για τα παρακάτω:

- Ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια και τους εμπορικούς κινδύνους εάν δεν υπάρχουν μέτρα ασφάλειας στον κυβερνοχώρο
- Προστασία της υποδομής της πληροφορικής (IT Infrastructure) του πλοίου και του συνδεδεμένου εξοπλισμού (OT), καθώς και των δεδομένων που χρησιμοποιούνται στα πλοία ή διακινούνται μεταξύ του πλοίου και του γραφείου
- Διαχείριση των χρηστών, διασφαλίζοντας την κατάλληλη πρόσβαση μόνο σε απαραίτητες πληροφορίες σύμφωνα με τον ρόλο τους
- Εξουσιοδότηση δικαιωμάτων διαχειριστή για συγκεκριμένους χρήστες, κατά τη διάρκεια συντήρησης και υποστήριξης των συστημάτων του πλοίου ή μέσω απομακρυσμένης σύνδεσης

Cyber Security vs Cyber Safety:

Το Cyber safety είναι εξίσου σημαντικό με το Cyber Security.

Και οι δύο έχουν ίσες πιθανότητες να επηρεάσουν την ασφάλεια του προσωπικού, των πλοίων και των φορτίων.
Το Cyber Security ασχολείται με την προστασία της πληροφορικής, του OT και των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χειραγώγηση και διακοπή.
Το Cyber Safety καλύπτει τους κινδύνους από την απώλεια διαθεσιμότητας ή ακεραιότητας κρίσιμων δεδομένων ασφαλείας και OT.

Συμβάντα ασφάλειας στον κυβερνοχώρο μπορεί να προκύψουν ως αποτέλεσμα:

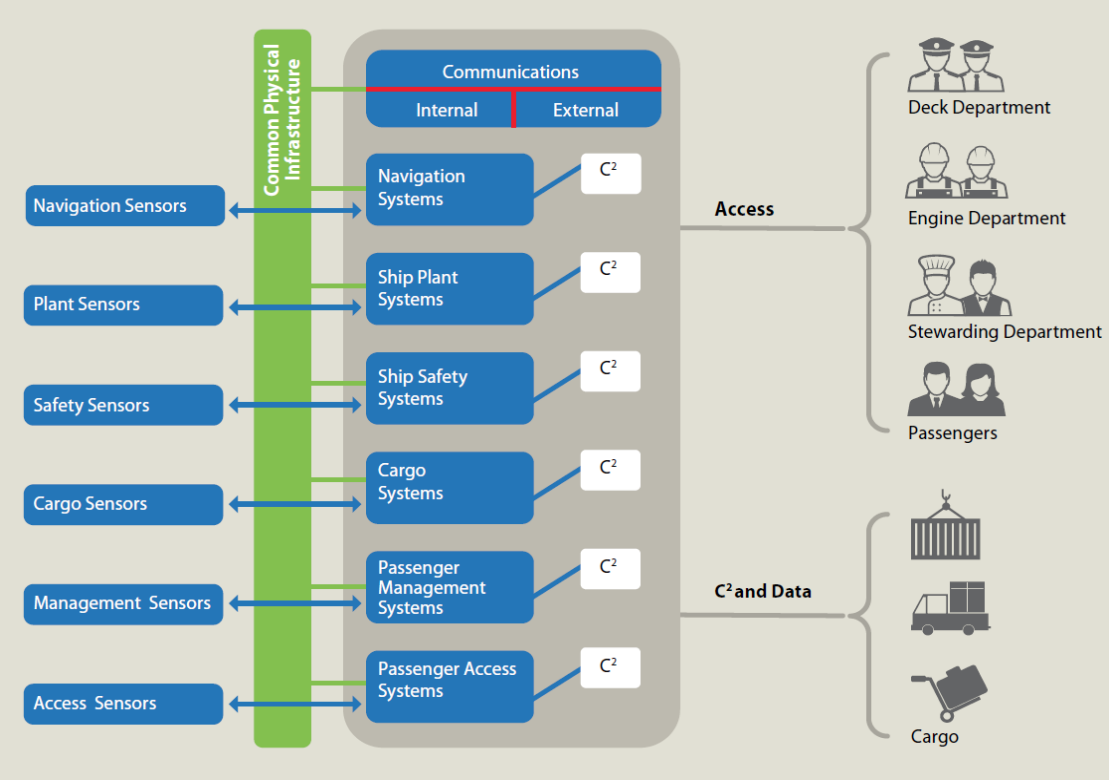
- Ένα συμβάν ασφάλειας στον κυβερνοχώρο, το οποίο επηρεάζει τη διαθεσιμότητα και την ακεραιότητα του OT, για παράδειγμα αλλοίωση των δεδομένων γραφημάτων που παρουσιάζονται σε ένα Ηλεκτρονικό Σύστημα Οθόνης και Πληροφοριών Χάρτη (ECDIS).

- Μια αποτυχία (failure) που προέκυψε κατά τη συντήρηση και την ενημέρωση κώδικα του λογισμικού (patching).

- Απώλεια ή χειραγώγηση δεδομένων των εξωτερικών αισθητήρων, οι οποίοι είναι ζωτικής σημασίας για τη λειτουργία ενός πλοίου. Αυτό περιλαμβάνει επίσης, και τα παγκόσμια δορυφορικά συστήματα πλοήγησης (GNSS).

Ενώ τα αίτια ενός περιστατικού cyber safety μπορεί να διαφέρουν από ένα περιστατικό cyber security, μια αποτελεσματική απάντηση και στα δύο βασίζεται στην εκπαίδευση και την επίγνωση των κατάλληλων πολιτικών και διαδικασιών της εταιρείας. Ως αποτέλεσμα όλων των παραπάνω, η διαχείριση κινδύνων στον κυβερνοχώρο πρέπει να ενσωματωθεί στο SMS της εταιρείας.

2.1 Γιατί το cyber security είναι σημαντικό για τα πλοία;



Ένα πλοίο είναι ένα σύνθετο σύστημα μηχανικής και φυσικής μηχανικής που περιλαμβάνει τόσο πλωτές δραστηριότητες και συστήματα, όσο και απομακρυσμένα συστήματα ελέγχου, όπως σήματα πλοήγησης.
Όπως φαίνεται παραπάνω, ένα πλοίο περιλαμβάνει πέντε βασικούς τύπους περιουσιακών στοιχείων (π.χ. εγκαταστάσεις και μηχανήματα, επιχειρησιακή τεχνολογία, τεχνολογία πληροφοριών, επικοινωνίες ραδιοσυχνοτήτων (RF) και συστήματα πλοήγησης) που χρησιμοποιούνται για την παροχή μιας σειράς επιχειρησιακών υπηρεσιών, στις οποίες η τεχνολογία παίζει ολοένα και περισσότερο σημαντικός ρόλος.

Η απώλεια ή συμβιβασμός ενός ή περισσοτέρων από αυτά τα περιουσιακά στοιχεία έχει τη δυνατότητα να επηρεάσει:

α) την υγεία και την ασφάλεια του προσωπικού και άλλων ατόμων, τα οποία επηρεάζονται από τις δραστηριότητες εργασίας και σε ποιους έχουν ανατεθεί
β) την ικανότητα του πλοίου να λειτουργεί με ασφάλεια και να μην θέτει σε κίνδυνο άλλα πλοία, θαλάσσιες δομές ή το περιβάλλον, και
γ) την ταχύτητα και την αποτελεσματικότητα στην οποία μπορεί να λειτουργεί το πλοίο.

Οποιαδήποτε αποτυχία των συστημάτων που περιγράφονται παραπάνω έχει σημαντικές συνέπειες τόσο στην οικονομία, όσο και στην φήμη των ναυτιλιακών εταιρειών.

2.2 IT/OT συστήματα πλοίου

Κατά την εξέταση της κυβερνοασφάλειας ενός πλοίου, είναι απαραίτητο να γίνει η διάκριση μεταξύ των IT συστημάτων και των συστημάτων (OT – Operational Technology) που συμμετέχουν σε επιχειρησιακές λειτουργίες του πλοίου (Μονάδα διαχείρισης θαλασσίου έρματος, σύστημα διαχείρισης φορτίου, ελέγχου ευστάθειας πλοίου κλπ).

Σύμφωνα με τις κατευθυντήριες οδηγίες του Διεθνή Ναυτιλιακού Οργανισμού (IMO) για τη διαχείριση του κινδύνου της κυβερνοασφάλειας, τα IT συστήματα επικεντρώνονται στη χρήση δεδομένων ως πληροφορία, ενώ τα συστήματα επιχειρησιακών λειτουργιών (OT) επικεντρώνονται στη χρήση δεδομένων για τον έλεγχο ή την παρακολούθηση των φυσικών διεργασιών του πλοίου.

Η προστασία της πληροφορίας και της ανταλλαγής δεδομένων μεταξύ των συστημάτων αποτελεί επίσης σημαντικό παράγοντα που πρέπει να εξεταστεί. Η συνεχής ανάπτυξη νέων τεχνολογιών έχει ως αποτέλεσμα την ολοένα και μεγαλύτερη διασύνδεση των συστημάτων πληροφορικής και τηλεπικοινωνιών των πλοίων τόσο μεταξύ τους και όσο και με το Διαδίκτυο.

Το Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο (BIMCO) επισημαίνει ότι η διασύνδεση μαζί με την ψηφιοποίηση, την ενσωμάτωση και την αυτοματοποίηση των συστημάτων αυξάνει τους κινδύνους στον κυβερνοχώρο - για παράδειγμα με τη μορφή μη εξουσιοδοτημένης πρόσβασης ή κακόβουλων επιθέσεων στα συστήματα και τα δίκτυα του πλοίου.

Αντίστοιχα, ο νηογνώμονας Lloyd’s Register (LR) στις σχετικές οδηγίες αναφέρει ότι τα δια- συνδεδεμένα συστήματα του πλοίου, μετατρέπουν το πλοίο σε ένα σύνολο διασυνδεδεμένων συστημάτων – «Ένα σύστημα από συστήματα». Τέτοια πλοία μπορούν να περιγραφούν με έναν νέο όρο, "cyber-enabled". Σύμφωνα με τον Lloyd’s Register (LR), τα συστήματα αυτά δεν υποκαθιστούν ακριβώς τα παραδοσιακά ηλεκτρομηχανικά συστήματα και τους χειριστές αλλά επιτρέπουν το συνδυασμό παραδοσιακών στοιχείων με πιο περίπλοκες συμπεριφορές. Σύμφωνα με τον LR, οι κίνδυνοι αυτοί πρέπει να αναγνωριστούν, να μελετηθούν και να περιορισθούν για να διασφαλιστεί η ασφαλής ενσωμάτωση των τεχνολογιών στο σχεδιασμό και τη λειτουργία των πλοίων.

Σύμφωνα με τους BIMCO και LR, τα επιχειρησιακά συστήματα των πλοίων περιλαμβάνουν, χωρίς να περιορίζονται σε:

- **Συστήματα Πλοήγησης:** Τα συστήματα πλοήγησης γίνονται όλο και περισσότερο ψηφιακά και δικτυωμένα με τα συστήματα στη στεριά. Η χρήση αφαιρούμενων μέσων (USB removable media) για την ενημέρωση των συστημάτων αυτών μπορεί να κάνει τα συστήματα γέφυρας, ακόμη και όσα δεν είναι συνδεδεμένα με το διαδίκτυο εξίσου ευάλωτα στις κυβερνοεπιθέσεις.
  Συστήματα σε αυτήν την κατηγορία είναι για παράδειγμα:
  - το ηλεκτρονικό σύστημα απεικόνισης χαρτών και πληροφοριών (ECDIS)
  - ο παγκόσμιο σύστημα εντοπισμού θέσης (GPS)
  - το δυναμικό σύστημα εντοπισμού θέσης (DPS)
  - το παγκόσμιο δορυφορικό σύστημα πλοήγησης (GNSS)
  - το σύστημα αυτόματης αναγνώρισης (AIS)
  - το σύστημα καταγραφής ταξιδιού (VDR)
  - το ραντάρ / αυτόματο βοήθημα σχεδιασμού ραντάρ (ARPA)

- **Συστήματα Διαχείρισης Φορτίου:** Τα συστήματα διαχείρισης και ελέγχου φορτίου μπορεί να είναι διασυνδεδεμένα με πολλαπλά συστήματα στην ξηρά. Για παράδειγμα, τα εργαλεία παρακολούθησης αποστολής που είναι διαθέσιμα μέσω σύνδεσης στο διαδίκτυο εκθέτουν κρίσιμα δεδομένα σε κίνδυνο.

- **Συστήματα Επικοινωνιών:** Η σύνδεση στο διαδίκτυο μέσω δορυφόρου ή άλλων ασύρματων επικοινωνιών, συμπεριλαμβανομένων των ραδιοεπικοινωνιών (ευρυζωνική σύνδεση, Voice Over IP (VOIP)), αυξάνει πιθανώς τις ευπάθειες στο περιβάλλον ενός πλοίου.

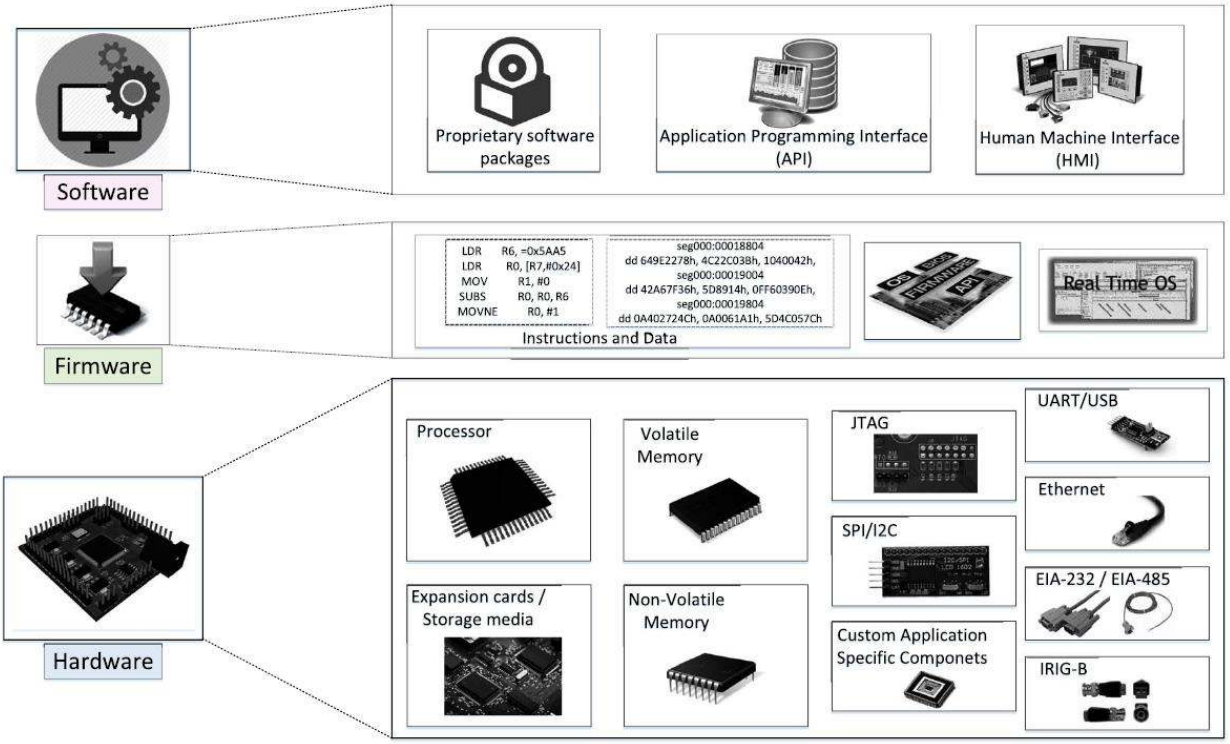
- **Συστήματα ελέγχου:** Τα ψηφιακά συστήματα ελέγχου και παρακολούθησης για ηλεκτρομηχανικά συστήματα, συμπεριλαμβανομένων των κύριων μηχανών, γεννητριών, δεξαμενών έρματος, αντλιών καυσίμου και λαδιού, υδατοστεγών θυρών, συναγερμών πυρκαγιάς και χειριστηρίων, ανεμιστήρων φορτίου, περιβαλλοντικών ελέγχων, είναι ευάλωτα στις επιθέσεις στον κυβερνοχώρο.

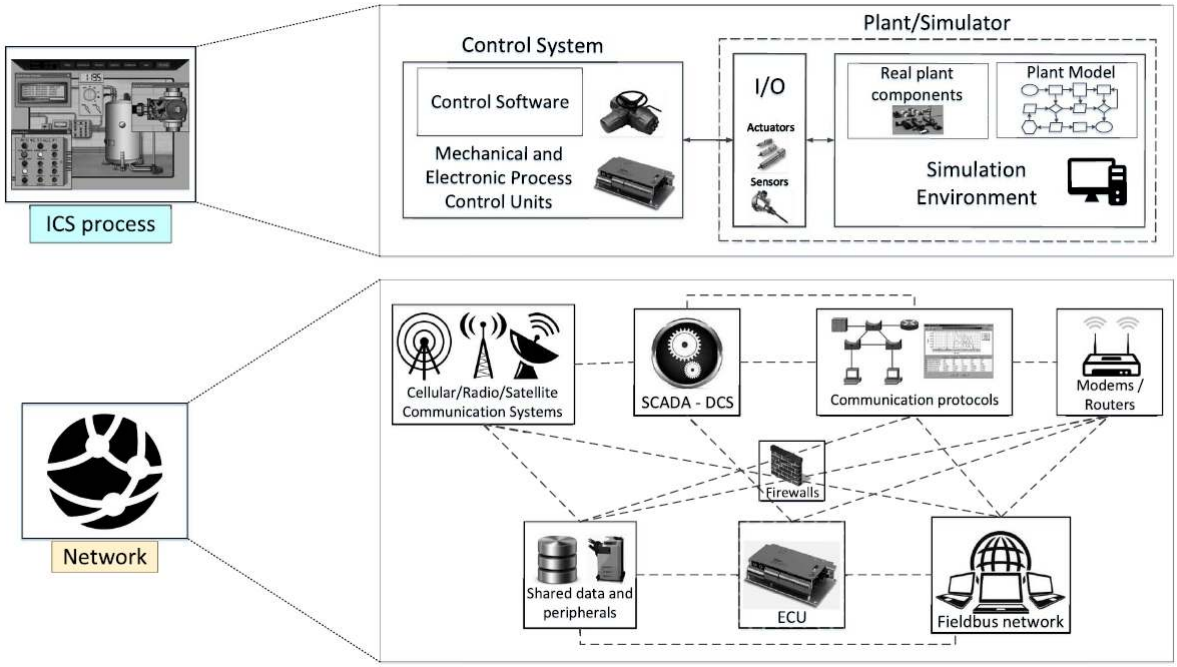
- **Συστήματα ελέγχου πρόσβασης:** Τα συστήματα αυτά χρησιμοποιούνται για τη διασφάλιση της φυσικής ασφάλειας του πλοίου και του φορτίου - συμπεριλαμβανομένης της επιτήρησης, του συναγερμού ασφαλείας του πλοίου και των ηλεκτρονικών συστημάτων «επί του πλοίου».

- **Εξοπλισμός Ναυλωτή:** Οι ναυλωτές μπορούν να χρησιμοποιήσουν εξοπλισμό, για παράδειγμα συστήματα σόναρ και σεισμικών ερευνών, ασύρματα σημεία πρόσβασης, θύρες IP και ασύρματα τηλέφωνα, τα οποία αυξάνουν τις ευπάθειες στον κυβερνοχώρο.

- **Συστήματα εξυπηρέτησης και διαχείρισης επιβατών:** Αξιόλογα δεδομένα που αφορούν τους επιβάτες μπορούν να υπόκεινται σε επεξεργασία από ψηφιακά συστήματα που χρησιμοποιούνται για την επιβίβαση και τον έλεγχο πρόσβασης στα πλοία. Οι ευφυείς συσκευές, όπως τα έξυπνα τηλέφωνα και οι φορητοί σαρωτές, μπορούν να δράσουν ως φορείς επίθεσης όταν τα δεδομένα που συλλέγονται μεταδίδονται σε άλλα συστήματα.

  Τα σταθερά και ασύρματα δίκτυα με σύνδεση στο διαδίκτυο, για παράδειγμα, για χρήση ψυχαγωγίας του επισκέπτη, θα πρέπει να θεωρούνται μη ελεγχόμενα και να διαχωρίζονται από τα συστήματα κρίσιμης σημασίας για το πλοίο. Τα δίκτυα πλοίων που χρησιμοποιούνται για τη διοίκηση του πλοίου ή την καλή διαβίωση του πληρώματος, καθώς και λογισμικό που παρέχεται από εταιρείες διαχείρισης πλοίων ή τους ιδιοκτήτες, ανήκουν στην ίδια κατηγορία.





Εικόνα: ΟΤ Συστήματα

Συνοψίζοντας, στα **συστήματα πληροφορικής IT** επηρεάζονται τα:
Δίκτυα πληροφορικής, emails, Διοίκηση, λογαριασμοί, λίστες πληρωμάτων, προγραμματισμένη συντήρηση, η διαχείριση και η ανακύκλωση ανταλλακτικών, τα ηλεκτρονικά εγχειρίδια, τα ηλεκτρονικά πιστοποιητικά, οι άδειες εργασίας, τα ναυλοσύμφωνα, η ειδοποίηση ετοιμότητας, οι φορτωτικές.
Στα συστήματα IT είναι σε κίνδυνο κυρίως τα οικονομικά μιας εταιρείας και η φήμη (Hugh Boyes, 2014), (BIMCO, 2018), (Kimberly Tam, Kevin Jones, June 2019).

Στα **συστήματα ΟΤ που αφορούν τη λειτουργία του υλικού και του λογισμικού** επηρεάζονται: PLCs, SCADA, Μέτρηση και έλεγχος επί του σκάφους, ECDIS, GPS, απομακρυσμένη υποστήριξη για κινητήρες, καταγραφείς δεδομένων, έλεγχος μηχανής και φορτίου, δυναμική τοποθέτηση.
Στα συστήματα ΟΤ είναι κυρίως σε κίνδυνο η ζωή, η ιδιοκτησία και το περιβάλλον (B.Svilicic – David BrCiC, March 2019), (Kimberly Tam, Kevin Jones, June 2019).

3. Επιθεώρηση πλοίου (Vetting Inspection)

3.1 Εισαγωγή

Η ναυτιλία, ειδικότερα οι μεταφορές αργού πετρελαίου και οι μεταφορείς πετρελαιοειδών που λειτουργούν στο εμπόριο Jones Act, έχουν και θα παραμείνουν σε μεγάλο βαθμό ρυθμισμένες από την ομοσπονδιακή κυβέρνηση, τον IMO και τους νηογνώμονες όπως το Αμερικανικό Γραφείο Ναυτιλίας.

Επιπλέον, οι ανησυχίες για το περιβάλλον και την εικόνα του κόσμου έχουν οδηγήσει τις μεγάλες πετρελαϊκές εταιρείες να αναπτύξουν και να εφαρμόσουν μια αυστηρή διαδικασία δέουσας επιμέλειας κατά την επιλογή των εμπορικών εταίρων ναυτιλίας για να εξασφαλίσουν ότι η διαχείριση του κινδύνου γίνεται με προκαθορισμένα κριτήρια αποδοχής. Επομένως, η διαδικασία εξέτασης έχει εξελιχθεί σε μια εκλεπτυσμένη και ολοκληρωμένη αξιολόγηση τόσο του σκάφους όσο και του χειριστή των σκαφών.

Ενώ πολλοί παράγοντες εξετάζονται και αξιολογούνται πριν από μια εμπορική απόφαση, οι μεγάλες πετρελαϊκές εταιρείες μέσω της ένωσής τους, το Oil Companies International Marine Forum ("OCIMF"), ανέπτυξαν και εφάρμοσαν δύο βασικά εργαλεία:

- **Το πρόγραμμα Έκθεσης Ελέγχου Πλοίων (SIRE):** Η διαδικασία επιθεώρησης πλοίων SIRE βασίζεται σε διεξοδική επιθεώρηση σκαφών που διενεργείται από διαπιστευμένους επιθεωρητές OCIMF, με αποτέλεσμα να δημιουργείται έκθεση και να είναι διαθέσιμη για προβολή από όλα τα μέλη του OCIMF. Η έκθεση είναι ένα σημαντικό στοιχείο της αξιολόγησης πλοίων που αναλαμβάνεται από οποιαδήποτε μεγάλη εταιρεία πετρελαίου όταν υπάρχει εμπορική ανάγκη.
- **Το πρόγραμμα Αυτοαξιολόγησης της Διαχείρισης των Δεξαμενοπλοίων (TMSA) για το περιβάλλον της ναυτιλιακή/διαχειρίστρια εταιρεία:**
  Το πρόγραμμα TMSA προσπαθεί να πετύχει παρέχοντας ξεκάθαρα κριτήρια στους διαχειριστές δεξαμενοπλοίων, οι οποίοι αυτοαξιολογούνται, και παρουσιάζουν τα αποτελέσματά τους στον OCIMF για επιθεώρηση και λεπτομερή εξέταση. Στους διαχειριστές, παρέχεται βοήθεια μέσω των στοιχείων –κλειδιών, των σκοπών των στοιχείων αυτών, των οδηγιών, των βασικών δεικτών απόδοσης (Key Performance Indicators- KPIs) και των πρακτικών της καλύτερης καθοδήγησης (OCIMF).
  Για την αξιολόγηση της προόδου των διαχειριστών των δεξαμενοπλοίων, το πρόγραμμα διαχωρίζεται σε τέσσερα (4) στάδια (stages). Κάθε διαχειριστής πρέπει να εκθέτει στον OCIMF την φόρμα αναφοράς προόδου με το στάδιο όπου φτάνει σε προοδευτική βάση. Οι αναφορές συνεχίζονται και αναβαθμίζονται όταν ο διαχειριστής επιτυγχάνει ένα μεγαλύτερο επίπεδο.

Τα δύο αυτά εργαλεία θα αναλυθούν λεπτομερώς παρακάτω για τον τομέα της κυβερνοασφάλειας, καθώς αποτελούν κρίσιμα κριτήρια για την ναύλωση των πλοίων και κατ' επέκταση την βιωσιμότητα μιας ναυτιλιακής εταιρείας.

Επιθεώρηση πλοίου/γραφείου στον τομέα του Cyber Security

Το Cyber Security στη ναυτιλία αποτελεί πλέον μέρος του κώδικα ISM και θα εφαρμόζεται υποχρεωτικά από τον Ιανουάριο του 2021. Οι εταιρείες ήδη προετοιμάζονται για αυτό, δίνοντας μεγάλη προσοχή σε διαδικασίες, κανονισμούς, εκπαιδεύοντας το προσωπικό τους και πραγματοποιώντας δοκιμές διείσδυσης στα συστήματά τους είτε με τη βοήθεια συμβουλευτικών εταιρειών είτε με δικό τους εξειδικευμένο προσωπικό.

Οι κανονισμοί που υποχρεωτικά ακολουθούν είναι:

- GDPR
- IMO-MSC
- TMSA 3
- VIQ 7 (SIRE)
- IACS
- ISO 27000 (προαιρετικά)

Οι παραπάνω κανονισμοί θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο, καθώς αποτελούν την κατευθυντήρια γραμμή για την ένταξη του Cyber Security στην ναυτιλιακή βιομηχανία.

Επιπρόσθετα, οι νηογνώμονες, εκτός από την πλευρά των επιθεωρήσεων παίζουν πλέον συμβουλευτικό ρόλο για τις εταιρείες. Αυτό πραγματοποιείται, παρέχοντας υπηρεσίες από εξειδικευμένο προσωπικό ώστε να στήσουν τα συστήματά τους, να εκπαιδεύσουν το προσωπικό τους, να εφαρμόσουν δοκιμές διείσδυσης των συστημάτων τους και τέλος τις αξιολογούν. Από την άλλη, οι εταιρείες εφαρμόζουν κάποιες «άτυπες» διαδικασίες οι οποίες βασίζονται στους κανονισμούς και κοινοποιούνται σε όλους τους εργαζομένους της εταιρείας, σε γραφείο και πλοίο.

4. Κανονιστικό Πλαίσιο για την Ασφάλεια Πληροφοριών στην Ναυτιλιακή Βιομηχανία

4.1 Εισαγωγή

Η είσοδος στην ψηφιακή εποχή είναι γεγονός και η ανάγκη για ασφάλεια στον κυβερνοχώρο μεγαλώνει με την πάροδο του χρόνου. Καθημερινά περιστατικά παραβίασης προσωπικών δεδομένων και πληροφοριών οδηγούν στην ανεύρεση λύσεων και πρακτικών μεθόδων που σχετίζονται με αυτό το θέμα. Υπηρεσίες, οργανισμοί καθώς και ο καθένας προσωπικά, είναι πλέον πιο καχύποπτοι σε σχέση με τις επιθέσεις στο διαδίκτυο και την ασφάλεια των προσωπικών δεδομένων. Αυτή η παγκόσμια τάση που τείνει να γίνει συνήθεια στην καθημερινότητα των ανθρώπων στον κλάδο τη; ναυτιλίας.

Η ναυτιλία αποτελεί παγκόσμια υπερδύναμη και δεν είναι καθόλου τυχαίο που το Cyber Security έχει μπει για τα καλά στο χώρο αυτόν. Εκτός από κοινούς κανονισμούς οι οποίοι εφαρμόζονται σε άλλους οργανισμούς, στη ναυτιλία εφαρμόζονται επιπλέον κανονισμοί οι οποίοι έχουν θεσπιστεί για τη διασφάλιση των πληροφοριών κατά την επικοινωνία των πλοίων με το γραφείο.

Ένας λόγος που εφαρμόζονται πλέον υποχρεωτικά κανονισμοί και διαδικασίες σχετικά με την κυβερνοασφάλεια στη ναυτιλία είναι το σκάνδαλο με τη Maersk, η οποία αποτελεί την μεγαλύτερη εταιρεία μεταφοράς εμπορευματοκιβωτίων παγκοσμίως.

Η Maersk είχε δηλώσει ότι περίμενε απώλειες μεταξύ 200- 300 εκατομμύρια δολάρια και αυτό οφειλόταν σε μια σημαντική διακοπή λειτουργίας του συστήματος, η οποία ήταν απλά αποτέλεσμα ενός ιού που κατάφερε να εισχωρήσει στο σύστημα, με αποτέλεσμα η εταιρεία να κλείσει προσωρινά όλα τα κρίσιμα συστήματα τα οποία είχαν μολυνθεί.

Ενδεικτικά, οι κατευθυντήριες γραμμές σχετικά με την ασφάλεια στον κυβερνοχώρο στον τομέα της ναυτιλίας βασίζονται κυρίως σε:

- IMO
- BIMCO
- ISO/IEC 27001 & ISO/IEC 62443 (OT)
- Classification Bodies and IACSDNV GL, ABS κ.ο.κ.

4.2 IMO

Ο IMO – International Maritime Organization, δηλαδή Διεθνής Ναυτιλιακός Οργανισμός είναι η εξειδικευμένη υπηρεσία των Ηνωμένων Εθνών που κατέχει την ευθύνη για την ασφάλεια και τη διασφάλιση της ορθής ναυσιπλοΐας αλλά και την πρόληψη της θαλάσσιας ρύπανσης από τα πλοία.

Πρωταρχικό καθήκον του IMO, όταν τέθηκε σε λειτουργία το 1959, ήταν να υιοθετήσει μια νέα έκδοση της Διεθνούς Σύμβασης για την Ασφάλεια της Ανθρώπινης Ζωής στη Θάλασσα (SOLAS11), η σημαντικότερη από όλες τις συνθήκες που διαπραγματεύονται την ασφάλεια στη θάλασσα.

Ο IMO έχει επίσης αναπτύξει και υιοθετήσει διεθνείς κανονισμούς και παγκόσμια πρότυπα περί σύγκρουσης για τους ναυτικούς, καθώς και διεθνείς συμβάσεις και κωδικούς που αφορούν την έρευνα και διάσωση, τη διευκόλυνση της διεθνούς ναυτιλιακής κίνησης, τις γραμμές φορτίου, τη μεταφορά επικίνδυνων εμπορευμάτων και τη μέτρηση της χωρητικότητας.

Όσον αφορά την κυβερνοασφάλεια, ο IMO έχει εκδώσει σχετικές κατευθυντήριες γραμμές, οι οποίες εμπεριέχονται στην MSC-FAL.1/Circ.3 για τη διαχείριση και την ασφάλεια του θαλάσσιου κυβερνοχώρου.

Οι κατευθυντήριες γραμμές παρέχουν συστάσεις υψηλού επιπέδου σχετικά με τη διαχείριση του κυβερνοχώρου στη ναυτιλία έτσι ώστε να επιτυγχάνεται η διασφάλιση της ναυτιλίας από τις τρέχουσες και αναδυόμενες απειλές και ευπάθειες του κυβερνοχώρου. Αυτές οι κατευθυντήριες γραμμές περιλαμβάνουν λειτουργικά στοιχεία που υποστηρίζουν την αποτελεσματική διαχείριση του κυβερνοχώρου. Οι συστάσεις μπορούν να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης κινδύνων και να συμπληρώσουν τις πρακτικές διαχείρισης της ασφάλειας που έχουν ήδη θεσπιστεί από τον IMO.
(http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx)

Η επιτροπή Ναυτιλιακής Ασφάλειας ενέκρινε στις 16 Ιουνίου 2017 το Παράρτημα 10 (Annex10) το ψήφισμα MSC.428_(98). Το ψήφισμα αναφέρει ότι ένα εγκεκριμένο σύστημα διαχείρισης της ασφάλειας (SMS) πρέπει να λαμβάνει υπόψη τη διαχείριση του κυβερνοχώρου σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις του κώδικα ISM. Έτσι, ενθαρρύνει τις διοικήσεις να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται κατάλληλα στα συστήματα διαχείρισης της ασφάλειας το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης (DOC)της εταιρείας μετά την 1η Ιανουαρίου 2021. Αν και δεν είναι ακόμη υποχρεωτικό, οι εταιρείες θα έπρεπε να έχουν αρχίσει να αναπτύσσουν πολιτικές στον κώδικα ISM τους ώστε να είναι έτοιμες να διασφαλίσουν ασφάλεια (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

Πιο συγκεκριμένα το ψήφισμα MSC.428_(98) το οποίο αφορά τη διαχείριση κινδύνου της ασφάλειας στα συστήματα στη ναυτιλία, αναγνωρίζοντας την ανάγκη να αυξηθεί η ευαισθητοποίηση σχετικά με τις απειλές και τα τρωτά σημεία του κυβερνοχώρου για την υποστήριξη ασφάλειας και προστασίας στη ναυτιλία, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους του κυβερνοχώρου, αναγνωρίζοντας επίσης ότι οι διοικήσεις, οι νηογνώμονες, οι πλοιοκτήτες και τα πλοία, οι παραγωγοί εξοπλισμού, οι πάροχοι υπηρεσιών, οι λιμένες και οι λιμενικές εγκαταστάσεις και όλοι οι άλλοι ενδιαφερόμενοι ναυτιλιακοί κλάδοι θα πρέπει να επιταχύνουν τις εργασίες για τη διασφάλιση της ναυτιλίας από τις τρέχουσες και αναδυόμενες απειλές και ευπάθειες του κυβερνοχώρου, λαμβάνοντας υπόψη την MSC-FAL.1 / Circ.3 σχετικά με τις κατευθυντήριες γραμμές για τη διαχείριση του θαλάσσιου κυβερνοχώρου που εγκρίθηκαν από την επιτροπή διευκόλυνσης κατά την 41ησυνεδρίασή της (4-7 Απριλίου 2017) και από την Επιτροπή Ναυτικής Ασφάλειας, την 98η σύνοδο (7 έως 16 Ιουνίου 2017), η οποία παρέχει συστάσεις υψηλού επιπέδου για τον θαλάσσιο κυβερνοχώρο οι οποίες μπορούν να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης κινδύνων και να συμπληρώσουν τις πρακτικές διαχείρισης της ασφάλειας και της ασφάλειας που έχει θεσπίσει ο εν λόγω Οργανισμός (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

Υπενθυμίζοντας την απόφαση Α.741 (18) με την οποία η Συνέλευση ενέκρινε τον Διεθνή Κώδικα Διαχείρισης για την Ασφαλή Λειτουργία των Πλοίων και την Πρόληψη της Ρύπανσης (Κώδικας Διεθνούς Διαχείρισης Ασφάλειας (ISM)) και αναγνωρίζει, μεταξύ άλλων, την ανάγκη κατάλληλης οργάνωσης της διαχείρισης επιτρέπουν την ανταπόκριση στην ανάγκη των επιβατών να επιτύχουν και να διατηρούν υψηλά πρότυπα ασφάλειας και προστασίας του περιβάλλοντος, Σημειώνοντας τους στόχους του κώδικα ISM που περιλαμβάνουν, μεταξύ άλλων, την παροχή ασφαλών πρακτικών στη λειτουργία των πλοίων και την ασφαλή εργασία στην εκτίμηση όλων των διαπιστωθέντων κινδύνων για τα πλοία, το προσωπικό και το περιβάλλον, τη θέσπιση κατάλληλων διασφαλίσεων και τη συνεχή βελτίωση των δεξιοτήτων διαχείρισης του προσωπικού και των πλοίων (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

1. ΕΠΙΒΕΒΑΙΩΝΕΙ ότι ένα εγκεκριμένο σύστημα διαχείρισης της ασφάλειας πρέπει να λαμβάνει υπόψη τη διαχείριση του κυβερνοχώρου σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις του κώδικα ISM.
2. ΕΝΘΑΡΡΥΝΕΙ τις αρχές να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται κατάλληλα στα συστήματα διαχείρισης της ασφάλειας το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης της εταιρείας μετά την 1η Ιανουαρίου 2021
3. ΑΝΑΓΝΩΡΙΖΕΙ τις απαραίτητες προφυλάξεις που θα μπορούσαν να χρειαστούν για τη διατήρηση της εμπιστευτικότητας ορισμένων πτυχών της διαχείρισης του κυβερνοχώρου.
4. ΖΗΤΑ από τα κράτη μέλη να θέσουν το παρόν ψήφισμα υπόψη όλων των ενδιαφερομένων
(http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx).

4.2.1 ISM Code

Ο κώδικας ISM (International Safety Management Code), ο διεθνής δηλαδή κώδικας για την Διαχείριση της Ασφάλειας (ISM) είναι να παράσχει ένα διεθνές πρότυπο για την ασφαλή διαχείριση και λειτουργία των πλοίων και για την πρόληψη της ρύπανσης
(http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Η προέλευση του Κώδικα επανέρχεται στα τέλη της δεκαετίας του 1980, όταν υπήρχε
αυξανόμενη ανησυχία για τα κακά πρότυπα διαχείρισης στη ναυτιλία. Οι έρευνες για τα ατυχήματα αποκάλυψαν σημαντικά σφάλματα εκ μέρους της διοίκησης και τελικά το 1987 η Συνέλευση του IMO ενέκρινε το ψήφισμα A.596 (15), το οποίο κάλεσε την Επιτροπή Ναυτικής Ασφάλειας να αναπτύξει τις κατευθυντήριες γραμμές σχετικά με
τη διαχείριση της ξηράς
(http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ο Κώδικας καθορίζει τους στόχους διαχείρισης της ασφάλειας μιας εταιρείας και απαιτεί να δημιουργηθεί από την ίδια την εταιρεία η διαχείριση της ασφάλειας (SMS), η οποία ορίζεται ως ο ιδιοκτήτης ή οποιοσδήποτε άλλος οργανισμός ή πρόσωπο, όπως ο διαχειριστής ή ο ναυλωτής του σκάφους που έχει αναλάβει την ευθύνη για την εκμετάλλευση του πλοίου και ο οποίος, αναλαμβάνοντας την ευθύνη αυτή, συμφώνησε να αναλάβει όλα τα καθήκοντα και την ευθύνη που επιβάλλει ο Κώδικας αυτός.

Στη συνέχεια, η Εταιρεία πρέπει να θεσπίσει και να εφαρμόσει μια πολιτική για την επίτευξη αυτών των στόχων. Αυτό περιλαμβάνει την παροχή των απαραίτητων πόρων και την υποστήριξη στη ξηρά.

Κάθε εταιρεία αναμένεται να ορίσει ένα πρόσωπο ή κάποια πρόσωπα στην ξηρά που έχουν άμεση πρόσβαση στο υψηλότερο επίπεδο διοίκησης, προκειμένου να υπάρξει σύνδεση μεταξύ της εταιρείας και εκείνων που βρίσκονται στο πλοίο.

Οι διαδικασίες που απαιτούνται από τον κώδικα πρέπει να τεκμηριώνονται και να καταρτίζονται σε ένα εγχειρίδιο διαχείρισης της ασφάλειας, αντίγραφο του οποίου θα πρέπει να διατηρείται και επί του σκάφους. (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx)

Ο θαλάσσιος κίνδυνος στον κυβερνοχώρο αναφέρεται σε ένα μέτρο του βαθμού στον οποίο ένα ενεργητικό τεχνολογίας θα μπορούσε να απειληθεί από μια πιθανή περίπτωση ή γεγονός που μπορεί να οδηγήσει σε λειτουργικές αποτυχίες, αστοχίες ασφάλειας ή ασφάλειας ως συνέπεια της αλλοίωσης, απώλειας ή απώλειας πληροφοριών ή συστημάτων συμβιβασμός (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ως διαχείριση του κυβερνοχώρου νοείται η διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης και επικοινωνίας ενός σχετικού με τον κυβερνοχώρο κινδύνου και η αποδοχή, αποφυγή, μεταφορά ή μετριασμός του σε αποδεκτό επίπεδο, λαμβάνοντας υπόψη το κόστος και τα οφέλη των ενεργειών που αναλαμβάνονται στους ενδιαφερόμενους φορείς (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Ο γενικός στόχος είναι να υποστηριχθεί η ασφαλής και ασφαλής ναυτιλία, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους του κυβερνοχώρου (http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

4.2.2 OCIMF-Oil Companies International Marine Forum

4.2.2.1 TMSA 3 – Element 13: Maritime Security

Το TMSA 3 είναι το σύστημα αξιολόγησης δεξαμενοπλοίων και σχετικά με το cyber security στα δεξαμενόπλοια αναφέρει το Element 13 του TMSA 3 και εφαρμόζεται υποχρεωτικά από την 1η Ιανουαρίου 2018 (TMSA 3 - MARITIME SECURITY - ELEMENT 13).

Κύριος Στόχος
Η δημιουργία ενός ασφαλούς και προστατευμένου εργασιακού περιβάλλοντος ώστε να αναπτυχθεί μια προορατική προσέγγιση στη διαχείριση της ασφάλειας. Επιπρόσθετα, να μετριαστούν οι κίνδυνοι ασφαλείας και να ελαχιστοποιηθούν οι συνέπειες τυχόν παραβιάσεων της ασφάλειας που επηρεάζουν ή δυνητικά επηρεάζουν το προσωπικό και τα περιουσιακά στοιχεία σε όλες τις τοποθεσίες της εταιρείας (TMSA 3 - MARITIME SECURITY – ELEMENT 13).

Διαχείριση Ασφάλειας

Η αποτελεσματική διαχείριση της ασφάλειας απαιτεί τον συστηματικό προσδιορισμό των απειλών σε όλους τους τομείς της επιχείρησης, με μέτρα που εφαρμόζονται για τον μετριασμό των κινδύνων στο χαμηλότερο πρακτικό επίπεδο.
Λόγω της συνεχώς μεταβαλλόμενης κατάστασης της ασφάλειας στη θάλασσα, η εταιρεία διαθέτει σύστημα παρακολούθησης και διαχείρισης αλλαγών, που συμπληρώνεται από μια κλιμακωτή προσέγγιση της ασφάλειας (TMSA 3- MARITIME SECURITY – ELEMENT 13).

Η εταιρεία διασφαλίζει ότι:

- Τα σχέδια ασφάλειας καλύπτουν όλες τις πτυχές των δραστηριοτήτων τους.
- Υπάρχουν διαδικασίες για τον εντοπισμό απειλών που καλύπτουν όλες τις επιχειρηματικές δραστηριότητες.
- Έχουν ληφθεί μέτρα για την άμβλυνση και αντιμετώπιση των εντοπισμένων απειλών.
- Οι πληροφορίες ασφαλείας διαχειρίζονται και ελέγχονται.
- Υπάρχουν διαδικασίες για την αναφορά πραγματικών περιστατικών και πιθανών απειλών.
- Εκπονούνται αξιολογήσεις κινδύνου για δραστηριότητες για τον εντοπισμό και την άμβλυνση πιθανών απειλών για την ασφάλεια.
- Το προσωπικό λαμβάνει την κατάλληλη εκπαίδευση ασφαλείας που εφαρμόζεται στις ευθύνες του
- Οι διαδικασίες περιλαμβάνουν τον εντοπισμό απειλών για την ασφάλεια στον κυβερνοχώρο, την ύπαρξη κατάλληλων κατευθυντήριων και μετριαστικών μέτρων και την ενεργό προώθηση της ευαισθητοποίησης.
- Η ταξιδιωτική πολιτική περιλαμβάνει πρόβλεψη για την ελαχιστοποίηση των απειλών για την ασφάλεια του προσωπικού.
- Οι διαδικασίες ασφάλειας ενημερώνονται τακτικά λαμβάνοντας υπόψη τις τελευταίες κατευθύνσεις του κλάδου.
- Η διαχείριση ασφάλειας περιλαμβάνεται στο πρόγραμμα εσωτερικού ελέγχου.
- Εκτιμώνται και ασκούνται ασκήσεις για την δοκιμή της ετοιμότητας.
- Ανεξάρτητη εξειδικευμένη υποστήριξη παρέχεται, κατά περίπτωση, για την αντιμετώπιση των εντοπισμένων απειλών.
- Τα σκάφη διαθέτουν βελτιωμένο εξοπλισμό ασφάλειας και παρακολούθησης.
- Οι βελτιώσεις ασφαλείας εξετάζονται για συμπερίληψη στις προδιαγραφές επαναφοράς και νέα σχέδια κατασκευής.
- Η καινοτόμος τεχνολογία ασφάλειας δοκιμάζεται και εφαρμόζεται ανάλογα με την περίπτωση.

Ασφάλεια στη ναυτιλία

Σκοπός: Καθιέρωση και διατήρηση πολιτικών και διαδικασιών για την αντιμετώπιση και τον μετριασμό των εντοπισμένων απειλών ασφάλειας που καλύπτουν όλες τις δραστηριότητες της εταιρείας, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο (TMSA 3 - MARITIME SECURITY – ELEMENT 13).

ΠΑΡΑΓΡΑΦΟΣ 13.1 - TMSA 3

1) Υπάρχουν τεκμηριωμένα σχέδια ασφάλειας τα οποία καλύπτουν όλες τις πτυχές των δραστηριοτήτων συμπεριλαμβανομένων:

- Τοποθεσιών που βασίζονται στην ξηρά.
- Σκαφών.
- Προσωπικού.

Το προσωπικό που είναι υπεύθυνο για θέματα που αφορούν την ασφάλεια εντοπίζεται.

2) Η εταιρεία έχει τεκμηριώσει τις διαδικασίες που εφαρμόζονται για τον εντοπισμό των απειλών ασφάλειας που ισχύουν για τις περιοχές εμπορίας σκαφών και τις τοποθεσίες που βασίζονται στην ξηρά.

Οι απειλές κατά της ασφάλειας μπορεί να περιλαμβάνουν:

- Μικροκλοπές
- Βανδαλισμούς
- Λαθρεπιβάτες
- Κλοπή φορτίου
- Κυβερνοαπειλή
- Ανεπαρκής ασφάλεια λιμένων
- Εμπορία ανθρώπων, όπλων ή ναρκωτικών
- Λαθρεμπόριο
- Πειρατεία
- Σαμποτάζ και εμπρησμός
- Τρομοκρατία και τα επακόλουθα αποτελέσματα

Οι απειλές που θα εντοπισθούν, εξετάζονται όπως απαιτούν οι καταστάσεις.

3) Έχουν αναπτυχθεί μέτρα για τον μετριασμό και την αντιμετώπιση όλων των εντοπισμένων απειλών για τα σκάφη και τις τοποθεσίες που βρίσκονται στη ξηρά. Σε σκάφη και σε τοποθεσίες με βάση τις ακτές. Τα μέτρα μετριασμού μπορεί να περιλαμβάνουν:

- Έλεγχο πρόσβασης
- Τα μέτρα φυσικής ασφάλειας
- άσκηση και εκπαίδευση
- Αστυνομικές περιπολίες
- Έρευνες

Υπάρχουν σχέδια έκτακτης ανάγκης για την αντιμετώπιση ενδεχόμενων παραβιάσεων της ασφάλειας.

4) Υπάρχουν διαδικασίες για την απόκτηση, διαχείριση και αναθεώρηση των σημερινών πληροφοριών που σχετίζονται με την ασφάλεια. Οι πληροφορίες ασφαλείας λαμβάνονται από την εταιρεία από κατάλληλες πηγές που μπορεί να περιλαμβάνουν:

- Διεθνείς και εθνικές υπηρεσίες
- Περιφερειακά κέντρα παροχής πληροφοριών για την ασφάλεια στη θάλασσα
- Κράτος σημαίας
- Οργανισμοί της βιομηχανίας
- Τοπικοί πράκτορες
- Στρατιωτικές πηγές
- Ειδικοί σύμβουλοι

Το υπεύθυνο άτομο εξετάζει τις πληροφορίες και εκδίδει σχετική καθοδήγηση στις τοποθεσίες, το προσωπικό και τα πλοία που βασίζονται στην ξηρά, ανάλογα με την περίπτωση.

5) Οι διαδικασίες περιλαμβάνουν την αναφορά δυνητικών απειλών ασφάλειας και πραγματικών περιστατικών ασφάλειας Οι διαδικασίες αναφοράς μπορούν να περιλαμβάνουν:

- Εσωτερική αναφορά πλοίων
- Πλοίο προς την εταιρεία

- Σκάφος προς εξωτερικές αρχές
- Εταιρεία προς εξωτερικές αρχές

ΠΑΡΑΓΡΑΦΟΣ 13.2 TMSA 3

1) Εκπονούνται επίσημες εκτιμήσεις κινδύνων για τις δραστηριότητες της εταιρείας για τον εντοπισμό και την άμβλυνση πιθανών απειλών για την ασφάλεια. Οι αξιολογήσεις κινδύνου επανεξετάζονται τακτικά, ενημερώνονται και οι διαδικασίες της εταιρείας τροποποιούνται ανάλογα με τις ανάγκες. Οι αξιολογήσεις ειδικού κινδύνου για τα πλοία επανεξετάζονται πριν από την είσοδο σε περιοχές που χαρακτηρίζονται ως επικίνδυνες. Όταν η εκτίμηση επικινδυνότητας το κρίνει απαραίτητο, αναπτύσσονται, τεκμηριώνονται και εφαρμόζονται ειδικά μέτρα σκλήρυνσης του πλοίου. Εξετάζεται η ύπαρξη κατάλληλων υλικών / εξοπλισμού προστασίας των πλοίων, τα οποία στη συνέχεια μπορούν να καταγράφονται σε ειδικά μέτρα προστασίας του πλοίου / σχέδιο συλλογής.

2) Το προσωπικό που είναι υπεύθυνο για την ασφάλεια λαμβάνει εκπαίδευση κατάλληλη για το ρόλο και τις δραστηριότητες της εταιρείας.

   Η κατάρτιση αντικατοπτρίζει το πεδίο των δραστηριοτήτων της εταιρείας και, όπου απαιτείται, πληροί τις ελάχιστες διεθνείς ή εθνικές νομοθετικές απαιτήσεις. Εξετάζεται η ανάγκη κατάρτισης ενός αναπληρωτή για βασικούς ρόλους ασφαλείας Μια ενημέρωση για την ασφάλεια παρέχεται σε όλο το προσωπικό ως μέρος της διαδικασίας εξοικείωσης.

3) Οι πολιτικές και οι διαδικασίες περιλαμβάνουν την ασφάλεια στον κυβερνοχώρο και παρέχουν κατάλληλα μέτρα καθοδήγησης και μετριασμού.

   Οι κίνδυνοι για τα συστήματα πληροφορικής ενδέχεται να περιλαμβάνουν:
   - Σκόπιμες και μη εξουσιοδοτημένες παραβιάσεις
   - Αθέλητες ή τυχαίες παραβιάσεις
   - Ανεπαρκής ακεραιότητα του συστήματος, όπως firewalls ή / και συστήματα προστασίας από ιούς

   Τα συστήματα με άμεσες ή έμμεσες επικοινωνιακές συνδέσεις, τα οποία μπορεί να είναι ευάλωτα σε εξωτερική απειλή ή ακατάλληλη χρήση, εντοπίζονται. Μπορεί να περιλαμβάνουν συστήματα πλοήγησης, μηχανικής, ελέγχου και επικοινωνίας. Κατά την ανάπτυξη διαδικασιών, η εταιρεία μπορεί να ανατρέξει στις σχετικές σημερινές οδηγίες του κλάδου.

4) Η εταιρεία προωθεί ενεργά την ευαισθητοποίηση στον κυβερνοχώρο. Χρησιμοποιούνται αποτελεσματικά μέσα για την ενθάρρυνση της υπεύθυνης συμπεριφοράς από το προσωπικό της ξηράς, το προσωπικό των πλοίων και τρίτους. Μια τέτοια συμπεριφορά μπορεί να περιλαμβάνει:
   - Κλείδωμα των σταθμών εργασίας χωρίς παρακολούθηση
   - Διασφάλιση κωδικών πρόσβασης
   - Τη μη χρήση μη εξουσιοδοτημένου λογισμικού

• Υπεύθυνη χρήση των κοινωνικών μέσων
• Έλεγχο / πρόληψη της κακής χρήσης των φορητών συσκευών αποθήκευσης και μνήμης

ΠΑΡΑΓΡΑΦΟΣ 13.3 TMSA 3

1) Η πολιτική ταξιδιών είναι σε ισχύ ώστε να πραγματοποιείται ελαχιστοποίηση των απειλών για την ασφάλεια του προσωπικού. Η πολιτική βασίζεται στην εκτίμηση κινδύνου και περιλαμβάνει το προσωπικό των πλοίων, το προσωπικό της ξηράς και τους εργολάβους που ταξιδεύουν για εργασίες της επιχείρησης. Όπου ενδείκνυται, υπάρχουν περιορισμοί και οδηγίες για ταξίδια που χαρακτηρίζονται ως υψηλού κινδύνου. Η ταξιδιωτική πολιτική αναθεωρείται τακτικά ώστε να λαμβάνονται υπόψη οι αλλαγές στις απειλές για την ασφάλεια.

2) Οι διαδικασίες ασφάλειας ενημερώνονται λαμβάνοντας υπόψη την τρέχουσα καθοδήγηση.
Η καθοδήγηση του κλάδου μπορεί να περιλαμβάνει:

• Καλύτερες διαχειριστικές πρακτικές για την προστασία κατά της πειρατείας η οποία βρίσκεται στη Σομαλία
• Τη διακίνηση ναρκωτικών και η Κατάχρηση Φαρμάκων (ICS)
• Τη ναυτική ασφάλεια - Καθοδήγηση σχετικά με τον κώδικα ISPS (ICS)
• Διαγράμματα σχεδιασμού ασφάλειας
• Οδηγίες για την ασφάλεια στον κυβερνοχώρο από τη βιομηχανία και την κλάση
• Λειτουργίες διάσωσης μεγάλης κλίμακας στη θάλασσα (ICS)
• Περιφερειακό οδηγό για την καταπολέμηση της πειρατείας και της ένοπλης ληστείας κατά των πλοίων στην Ασία (ReCAAP-ISC)

Στα σκάφη της εταιρείας παρέχονται οι τελευταίες εκδόσεις σχετικών δημοσιεύσεων σχετικά με την ασφάλεια.

3) Η πολιτική ασφάλειας και οι συναφείς διαδικασίες εμπίπτουν στο πρόγραμμα εσωτερικού ελέγχου. Ο έλεγχος αξιολογεί τη συμμόρφωση με όλες τις πτυχές των διαδικασιών ασφαλείας της εταιρείας, συμπεριλαμβανομένης της προσωπικής ευαισθητοποίησης και συμπεριφοράς.

ΠΑΡΑΓΡΑΦΟΣ 13.3 TMSA 3

1) Εκτίμηση των μέτρων ασφαλείας και η ετοιμότητα της εταιρείας. Οι αξιολογήσεις μπορούν να διεξάγονται από εσωτερικό προσωπικό ή από εξωτερικούς πόρους.

2) Ανεξάρτητη εξειδικευμένη υποστήριξη χρησιμοποιείται για την άμβλυνση των εξειδικευμένων απειλών ασφάλειας.
Όλες οι συμβάσεις ειδικής υποστήριξης, τόσο επί του σκάφους όσο και στην ξηρά, υποστηρίζονται από ένα εκτεταμένο πεδίο εργασιών. Αυτή η στήριξη μπορεί να ανατεθεί για δραστηριότητες που συμπεριλαμβάνουν την εκπαίδευση, την ασφάλεια και τις αξιολογήσεις απειλών και τα καθήκοντα φύλαξης. Πριν από τη σύναψη μιας σύμβασης, η εταιρεία δεν διεξάγει εμπεριστατωμένη αξιολόγηση δέουσας επιμέλειας του προτεινόμενου συμβαλλομένου, συμπεριλαμβανομένης της συμμόρφωσης με τα σχετικά πρότυπα. Καθοδήγηση σχετικά με το συμβόλαιο των συμβούλων ασφαλείας επί του πλοίου και το πεδίο των εργασιών τους παρέχεται στον πλοίαρχο.

3) Τα σκάφη διαθέτουν βελτιωμένο εξοπλισμό ασφάλειας και παρακολούθησης. Παραδείγματα τέτοιου εξοπλισμού περιλαμβάνουν:

- Τα κανόνια νερού
- Εξοπλισμό θερμικής απεικόνισης
- Ραντάρ πρύμνης
- Ταινία εκτόξευσης
- Συστήματα εισόδου πληκτρολογίου
- Συστήματα παρακολούθησης και καταγραφής CCTV
- Ένα δευτερεύον μέσο ανεξάρτητης δορυφορικής τηλεφωνικής επικοινωνίας

4) Οι βελτιώσεις ασφαλείας εξετάζονται για συμπερίληψη στις προδιαγραφές επαναφοράς και τον σχεδιασμό νέας κατασκευής.

Οι βελτιώσεις και οι προδιαγραφές ενδέχεται να εξαρτώνται από:

- Την περιοχή των συναλλαγών
- Τον τύπο του σκάφους και το μέγεθος
- Τα επίπεδα επάνδρωσης.

5) Η εταιρεία συμμετέχει στη δοκιμή και εφαρμογή καινοτόμων συστημάτων τεχνολογίας ασφαλείας.
Αυτό μπορεί να περιλαμβάνει:

- Φυσικά μέτρα για τη βελτίωση της ασφάλειας
- Βελτιώσεις λογισμικού σε συστήματα πληροφορικής

4.2.2.2 SIRE - VIQ 7

Το Vessel Inspection Questionnaire (VIQ) αφορά επιθεωρήσεις μεγίστης σημασίας σε δεξαμενόπλοια μεταφοράς καυσίμων και χημικών αερίων. Σε περιπτώσεις των εταιρειών Shell, BP κτλ, το VIQ είναι απαραίτητο. Σε σχέση με το Cyber security δίνεται ιδιαίτερη έμφαση στο κεφάλαιο 7 του κανονισμού (VIQ version 7.0.05, 2019). Αυτό είναι ένα ερωτηματολόγιο το οποίο θα πρέπει να απαντηθεί ορθά από την εταιρεία σε τέτοιου είδους επιθεωρήσεις.

Σχετικά με την κυβερνοασφάλεια παρακάτω, παρουσιάζονται οι παράγραφοι του 7ου κεφαλαίου οι οποίοι σχετίζονται με αυτή:

7.14 Υπάρχουν πολιτικές και διαδικασίες για την ασφάλεια στον κυβερνοχώρο οι οποίες αποτελούν μέρος του Συστήματος Διαχείρισης Ασφάλειας και σχέδιο Cyber Response στο σκάφος;

Σημείωση: Οι διαδικασίες περιλαμβάνουν αξιολόγηση κινδύνου για θέματα όπως:

- Απειλές όπως από κακόβουλο λογισμικό όπως επιθέσεις ηλεκτρονικού "ψαρέματος"κλπ.
- Ταυτοποίηση και προστασία των ευάλωτων συστημάτων (ECDIS κλπ.)
- Μέτρα μετριασμού (έλεγχος USB κλπ.)
- Προσδιορισμός του βασικού προσωπικού εντός της επιχείρηση(συμπεριλαμβανομένου του για ποιόν ο πλοίαρχος αναφέρει ύποπτα περιστατικά)
- Αντίγραφα κρατούν οι βασικές επαφές (όπως ο DPA, ο CSO κλπ.)
- Διαχείριση και εγγραφή κωδικών πρόσβασης
- Συμμόρφωση με τον ανάδοχο

Σημείωση: Το σχέδιο Cyber Response περιλαμβάνει οδηγίες σχετικά με:

- Τι είδους «συμπτώματα» πρέπει να αναζητηθούν
- Τις άμεσες ενέργειες που πρέπει να αναληφθούν, και τέλος
- Το όνομα, τη θέση, τον αριθμό τηλεφώνου και το ηλεκτρονικό ταχυδρομείο για υπεύθυνο πρόσωπο που θα είναι σε θέση να επικοινωνήσει μαζί σας

7.15 Γνωρίζει το πλήρωμα την πολιτική της εταιρείας για τον έλεγχο της φυσικής πρόσβασης για όλα τα συστήματα IT/OT επί του πλοίου;

Σημείωση: Οι επιθεωρητές θα πρέπει να προσέχουν εάν η πρόσβαση στις θύρες USB στους τερματικούς σταθμούς IT/OT του πλοίου ελέγχεται ή υπάρχουν μέτρα για να μπλοκάρουν ή να κλειδώνουν τις θύρες σε αυτούς τους ακροδέκτες. Οι διαδικασίες θα πρέπει να περιλαμβάνουν την προστασία του κρίσιμου εξοπλισμού όπως το ECDIS, από επιθέσεις κακόβουλου λογισμικού και ιών. Επίσης, θα πρέπει να περιλαμβάνουν τον έλεγχο της πρόσβασης σε όλα τα τερματικά IT/OT του πλοίου συμπεριλαμβανομένης της πρόσβασης στους διακομιστές οι οποίοι θα πρέπει να βρίσκονται σε ασφαλή τοποθεσία. Οι διαδικασίες θα πρέπει επίσης να περιλαμβάνουν πρόσβαση από κάθε είδους τρίτους συμβαλλόμενους και τεχνικούς.

7.16 Έχει η εταιρεία πολιτική καθοδήγηση σχετικά με τη χρήση ιδιωτικών-προσωπικών συσκευών επί του σκάφους;

Οι προσωπικές συσκευές περιλαμβάνουν κινητό τηλέφωνο, τάμπλετ, φορητό υπολογιστή κτλ.

Επίσης, συσκευές αποθήκευσης όπως σκληρούς δίσκους, USB κτλ. Γίνεται έλεγχος αν η πολιτική εφαρμόζεται τόσο από το πλήρωμα όσο και από τους επισκέπτες στο πλοίο όπως για παράδειγμα όλους τους συμβαλλόμενους και τεχνικούς τρίτου μέρους.

7.17 Είναι η ευαισθητοποίηση σχετικά με το Cyber Security, ενεργά προωθημένη επί του πλοίου;

Τα παραδείγματα της ενεργής προώθησης περιλαμβάνουν:

- Υλικό ευαισθητοποίησης σχετικά με την ασφάλεια στον κυβερνοχώρο
- Κατάρτιση πληρώματος μέσω ταινιών
- Εξειδικευμένη εκπαίδευση πληρώματος
- Οδηγίες για τη διασφάλιση των κωδικών πρόσβασης στο σύστημα
- Υπεύθυνη χρήση των κοινωνικών μέσων
- Πολιτική σχετικά με τη χρήση των προσωπικών συσκευών και την ένταξή τους στο πλοίο, με τη συμμετοχή λιστών ελέγχου εξοικείωσης
- Μπορεί να συμπεριλαμβάνει συμφωνίες για την πολιτική των εγκεκριμένων πολιτικών χρήσης (AUP) των εργαζομένων
- Η εταιρεία να είναι πιστοποιημένη σύμφωνα με το πρότυπο ISO 27000

4.2.3 IACS

Ο IACS- International Association of Classification Society, είναι μια μη κερδοσκοπική οργάνωση καταχώρησης νηογνωμόνων η οποία θεσπίζει τα ελάχιστα τεχνικά πρότυπα και τις απαιτήσεις που αφορούν την ασφάλεια στη θάλασσα και την προστασία του περιβάλλοντος και εξασφαλίζει τη συνεπή εφαρμογή τους. Σχετικά με το Cyber security στη ναυτιλία ο IACS έχει θεσπίσει κάποιες συστάσεις σχετικά με την ασφάλεια στον κυβερνοχώρο (http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-changein-delivery-of-cyber-resilient-ships/).

Οι συστάσεις του IACS απορρέουν από εκτεταμένη συνεργασία σε ολόκληρη τη βιομηχανία και παρέχουν πολύ αναγκαίες οδηγίες σχετικά με τον τρόπο ανάπτυξης και διατήρησης της ακεραιότητας του κυβερνοχώρου των σκαφών.

Ο IACS δημοσίευσε 9 από τις 12 συστάσεις του σχετικά με την ασφάλεια στον κυβερνοχώρο με στόχο να καταστήσει δυνατή την παράδοση ανθεκτικών στο κυβερνοχώρο πλοίων, των οποίων η αντοχή μπορεί να διατηρηθεί καθ όλη τη διάρκεια της επαγγελματικής τους ζωής.

Αυτές οι συστάσεις είναι το αποτέλεσμα μιας μακροπρόθεσμης πρωτοβουλίας του IACS, η οποία έχει ωφεληθεί σημαντικά από την εισροή και τη στήριξη από τη βιομηχανία. Ο IACS αρχικά ασχολήθηκε με το θέμα της ποιότητας του λογισμικού με τη δημοσίευση του UR E22 το 2006.
Αναγνωρίζοντας την τεράστια αύξηση της χρήσης του κυβερνοχώρου επί του σκάφους και από τότε ανέπτυξε αυτή τη σειρά συστάσεων με σκοπό να αντικατοπτρίζει τις απαιτήσεις ανθεκτικότητας ενός πλοίου με πολλές περισσότερες αλληλεξαρτήσεις.
Ως αποτέλεσμα, οι συστάσεις του IACS αντιμετωπίζουν την ανάγκη για:
• Την κατανόηση της αλληλεπίδρασης μεταξύ των συστημάτων του πλοίου
• Την προστασία από συμβάντα πέρα από τα πιθανά σφάλματα λογισμικού
• Σε περίπτωση αποτυχίας προστασίας, την ανάγκη για κατάλληλη ανταπόκριση και τελικά την ανάκτηση των δεδομένων
• Των μέσων ανίχνευσης που απαιτούνται έτσι ώστε να μπορέσει να εφαρμοστεί η κατάλληλη απάντηση

Ο IACS αναγνώρισε επίσης σε πρώιμο στάδιο ότι για να μπορέσουν τα πλοία να είναι ανθεκτικά έναντι των περιστατικών στον κυβερνοχώρο, θα έπρεπε να συμμετέχουν όλα τα τμήματα του κλάδου ενεργά και έτσι συγκάλεσε μια κοινή ομάδα εργασίας (JWG) για τα συστήματα Cyber Security. Σημαντικό μέρος του έργου της ομάδας αυτής αποτέλεσε ο εντοπισμός βέλτιστων πρακτικών των κατάλληλων υφιστάμενων προτύπων στον τομέα του κινδύνου και της ασφάλειας στον κυβερνοχώρο και ο εντοπισμός μιας πρακτικής προσέγγισης κινδύνου.
Κατά συνέπεια, οι 12 συστάσεις του IACS, συλλογικά, δεν παρέχουν μόνο καθοδήγηση σχετικά με τους πιο πιεστικούς τομείς ανησυχίας, αλλά λειτουργούν ως δομικά στοιχεία για τον ευρύτερο στόχο της ανθεκτικότητας του συστήματος (http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-changein-delivery-of-cyber-resilient-ships/).

Ο IACS δρομολόγησε τις εν λόγω συστάσεις με την προσδοκία ότι θα εξελιχθούν ταχέως σε σχέση με τις παραδοσιακές τεχνικές και διαδικασίες σχετικά με τη διασφάλιση της ασφάλειας, εξαιτίας της εμπειρίας που αποκτήθηκε από την πρακτική εφαρμογή τους.
Επιπλέον, αναγνωρίζει ότι οι εν λόγω συστάσεις είναι μόνο ένα «ενδιάμεσο» προϊόν και ότι θα αποτελέσουν αντικείμενο συγχώνευσης σε ένα ευρύτερο έγγραφο με συνεκτικότερη γλώσσα, αλληλεπικαλύψεις που αφαιρούνται και κοινό υλικό ενοποιημένο.
Επίσης, αναγνωρίζει ότι η παράδοση αυτών των σημαντικών σειρών συστάσεων είναι μόνο η αρχή της συνεχούς προσπάθειας για τη διατήρηση της ακεραιότητας του κυβερνοχώρου των πλοίων. Ωστόσο, διατηρεί την πεποίθηση ότι η ευέλικτη και διαρθρωμένη προσέγγιση που υιοθετείται, θέτει σε καλό δρόμο την περαιτέρω εξέλιξη και ενίσχυση αυτών των προσφορών, με ταχύτητα και ανταπόκριση, με τρόπο πρακτικό και υποστηρίζοντας τις ανάγκες του μεγαλύτερου αριθμού ενδιαφερόμενων μερών της βιομηχανίας
(http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-changein-delivery-of-cyber-resilient-ships/).

Οι 12 συστάσεις είναι:
• Εγγραφή 153: Συνιστώμενες διαδικασίες για τη συντήρηση λογισμικού του εξοπλισμού και των συστημάτων πλοίων
• Εγγραφή 154: Σύσταση σχετικά με τις δυνατότητες χειρωνακτικής / τοπικής ρύθμισης για συστήματα μηχανημάτων που εξαρτώνται από το λογισμικό
• Εγγραφή 155: Σχέδιο έκτακτης ανάγκης για ενσωματωμένα συστήματα υπολογιστών
• Εγγραφή 156: Αρχιτεκτονική δικτύου
• Εγγραφή 157: Διασφάλιση Δεδομένων
• Εγγραφή 158: Φυσική ασφάλεια των ενσωματωμένων συστημάτων υπολογιστών
• Εγγραφή 159: Ασφάλεια δικτύων επί των ενσωματωμένων συστημάτων υπολογιστών
• Εγγραφή 160: Σχεδιασμός συστήματος πλοίων
• Εγγραφή 161: Λίστα απογραφής των συστημάτων που βασίζονται σε υπολογιστές.
• Εγγραφή 162: Ενσωμάτωση.
• Εγγραφή 163: Απομακρυσμένη Πρόσβαση
• Εγγραφή 164: Επικοινωνία και διεπαφές
(http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-changein-delivery-of-cyber-resilient-ships/).

4.2.4 ΠΡΟΤΥΠΟ ISO 27001

Σύμφωνα με το ISO 27001, ένα σύστημα διαχείρισης ασφάλειας πληροφοριών είναι: ¨Εκείνο το μέρος του συνολικού συστήματος διαχείρισης, το οποίο βασιζόμενο σε μία προσέγγιση επιχειρηματικού κινδύνου, εγκαθιδρυθεί, δημιουργεί, λειτουργεί, παρακολουθεί, ανασκοπεί, διατηρεί και βελτιώνει την ασφάλεια των πληροφοριών¨ (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

Μπορεί να ειπωθεί πως ένα σύστημα διαχείρισης ασφάλειας πληροφοριών είναι μία ολοκληρωμένη, οργανωμένη και συνεχή αντιμετώπιση των θεμάτων ασφαλείας.
Ένα σύστημα διαχείρισης ασφάλειας πληροφοριών έχει 2 γενικούς στόχους:
Α. Την Πρόληψη και Β. την Αντιμετώπιση.

Ένα σύστημα πρέπει να είναι έτσι σχεδιασμένο ώστε να εκπληρώνει και τους δύο αυτούς στόχους σε συνδυασμό και όχι τον κάθε ένα χωριστά. Το σύστημα θα πρέπει να περιέχει εκείνα τα στοιχεία που θα του επιτρέπουν να θωρακίζει τον οργανισμό απέναντι σε όσο το δυνατόν περισσότερους κινδύνους και ταυτόχρονα σε περίπτωση εμφάνισης προβλήματος να διαθέτει εκείνους τους μηχανισμούς που θα του επιτρέπουν να το αντιμετωπίσει αποτελεσματικά, με την μικρότερη δυνατή ζημιά και στον μικρότερο δυνατό χρόνο.

Πρέπει να τονιστεί ότι κανένα σύστημα ασφάλειας πληροφοριών δεν είναι 100% αδιάβλητο. Η τεχνολογία βρίσκεται σε συνεχή εξέλιξη και γι' αυτόν τον λόγο οι πρακτικές που ακολουθούμε θα πρέπει να είναι ενημερωμένες έτσι ώστε να μην εκθέτουν σε κίνδυνο τον οργανισμό. Η λύση σε κάθε περίπτωση είναι η όσο το δυνατόν καλύτερη προετοιμασία (πρόληψη) και όσο το δυνατόν καλύτερη αντιμετώπιση σε περίπτωση εμφάνισης περιστατικού(INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

- **Η δομή του προτύπου**

Το πρότυπο αποτελείται από 10 βασικές παραγράφους, ενώ ακολουθείται από το παράρτημα Α (Annex A), που είναι κανονιστικό και αναφέρεται στους μηχανισμούς και στις απαιτήσεις ανά είδος υποδομής και ιδιαιτεροτήτων συστήματος (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

Σκοπός:
Το πρότυπο ISO 27001 παρέχει τις ελάχιστες απαιτήσεις για τη διαχείριση της ασφάλειας πληροφοριών. Απευθύνεται στους υπευθύνους υλοποίησης της ασφάλειας σε έναν οργανισμό. Περιγράφει μία κοινή βάση για την ανάπτυξη επιπέδων ασφαλείας μέσα στον οργανισμό, την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών και τη δημιουργία εμπιστοσύνης κατά τις συναλλαγές ανάμεσα σε οργανισμούς. Το πρότυπο αυτό δεν είναι πάνω από τις νομικές απαιτήσεις κάθε χώρας και κάθε σύστημα που εφαρμόζεται στις εταιρείες θα πρέπει να συνδυάζει τις απαιτήσεις του προτύπου με τις νομικές απαιτήσεις κάθε χώρας .
Το πρότυπο είναι εφαρμόσιμο σε έναν οργανισμό που θα ήθελε να:
• Σχεδιάσει
• Δημιουργήσει
• Λειτουργήσει
• Παρακολουθήσει
• Ελέγξει

• Διατηρήσει και βελτιώσει το σύστημα διαχείρισης και ασφάλειας πληροφοριών πάντα σε συμφωνία με τους σκοπούς του οργανισμού στα πλαίσια της ασφάλειας (INTERNATIONAL STANDARD ISO/ IEC 27000:2016).

➢ **Εφαρμογή**

Οι απαιτήσεις του προτύπου είναι γενικές και μπορούν να εκπληρωθούν από όλους τους οργανισμούς ανεξάρτητα του μεγέθους, της οργανωτικής δομής του αντικειμένου και του τομέα δραστηριοποίησης. Η κάλυψη των απαιτήσεων των παραγράφων 4 έως 10 του προτύπου είναι υποχρεωτική, ενώ όλα τα περιεχόμενα του παραρτήματος Α (Annex A) είναι προαιρετικά και εξαρτάται από τη δυνατότητα εφαρμογής του σε κάθε οργανισμό. Σε κάθε περίπτωση, αυτή η εξαίρεση από τις παραγράφους του παραρτήματος Α (Annex A), θα πρέπει να καταγράφεται και να αιτιολογείται κατάλληλα. Τέλος, οι όποιες εξαιρέσεις δε θα πρέπει να επηρεάζουν την ικανότητα να παρέχουν ένα επίπεδο ασφάλειας αντίστοιχο με αυτό που έχει προσδιοριστεί στην εκτίμηση κινδύνου και πάντα σε συμφωνία με τις ισχύουσες νομικές απαιτήσεις (INTERNATIONAL STANDARD ISO/ IEC 27000:2016)

Πιο αναλυτικά οι παράγραφοι 4 έως 10 (INTERNATIONAL STANDARD ISO/ IEC 27000:2016:

❖ Η Παράγραφος 4 αναφέρεται στο Πλαίσιο του οργανισμού το οποίο αποτελείται από:

- ✓ Την κατανόηση του οργανισμού και του πλαισίου του.
- ✓ Την κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών της επιχείρησης.
- ✓ Τον καθορισμό του πεδίου εφαρμογής του συστήματος διαχείρισης της ασφάλειας των πληροφοριών.
- ✓ Το σύστημα διαχείρισης της ασφάλειας των πληροφοριών.

❖ Η Παράγραφος 5 αφορά την ηγεσία και αποτελείται από:

- ✓ Την ηγεσία και τη δέσμευση.
- ✓ Την πολιτική που εφαρμόζεται.
- ✓ Τους οργανωτικούς ρόλους, τις ευθύνες και τις αρχές.

❖ Η Παράγραφος 6 αφορά το σχεδιασμό – προγραμματισμό και πραγματοποιείται:

- ✓ Με τις δράσεις για την αντιμετώπιση των κινδύνων και των ευκαιριών.
- ✓ Με τους στόχους για την ασφάλεια των πληροφοριών και τον προγραμματισμό για την επίτευξη τους.

❖ Η Παράγραφος 7 αφορά την υποστήριξη του συστήματος και πιο συγκεκριμένα:

- ✓ Τους πόρους που χρησιμοποιεί.
- ✓ Τις αρμοδιότητες του συστήματος.
- ✓ Την επίγνωση.
- ✓ Την επικοινωνία.
- ✓ Τις τεκμηριωμένες πληροφορίες.

❖ Η Παράγραφος 8 αναφέρεται στη λειτουργία του συστήματος και πραγματοποιείται από:

- ✓ Τον λειτουργικό σχεδιασμό και έλεγχο.
- ✓ Την αξιολόγηση κινδύνου ασφάλειας πληροφοριών - Risk Assessment.
- ✓ Την διαχείριση κινδύνων ασφάλειας πληροφοριών – Risk Treatment.

❖ Η Παράγραφος 9 αφορά την αξιολόγηση της απόδοσης και πραγματοποιείται:

- ✓ Με την παρακολούθηση, μέτρηση, ανάλυση, και αξιολόγηση του συστήματος.
- ✓ Με τον εσωτερικό έλεγχο – Internal Audit.
- ✓ Με επισκόπηση της διαχείρισης.

❖ Η Παράγραφος 10 αφορά τη βελτίωση και επιτυγχάνεται με:
- ✓ Τη μη συμμόρφωση και τις διορθωτικές ενέργειες που θα πρέπει να εφαρμοστούν στο σύστημα.
- ✓ Και τέλος με τη συνεχή βελτίωση.

Πέρα από το πρότυπο ISO 27000 υπάρχουν κανονισμοί οι οποίοι αφορούν συγκεκριμένα ήδη πλοίων. Έτσι, προς το παρόν έχει τεθεί σε εφαρμογή ο κανονισμός TMSA3 ο οποίος αφορά τα τάνκερς. Αυτός ο κανονισμός καλύπτει σε ασφαλιστικό επίπεδο τους ιδιοκτήτες οι οποίοι εφαρμόζοντας τους κανονισμούς μπορούν να έχουν πλήρη ασφαλιστική κάλυψη και από την άλλη τους ασφαλιστές οι οποίοι μπορούν να διαχειρίζονται τον κίνδυνο. Αξίζει να σημειωθεί πως το 2021 έρχεται υποχρεωτικός κανονισμός και για τα Bulk Carriers.

4.2.5 Πρότυπο IEC 62443 (OT): Cyber security for Industrial Automation & Control Systems

Το πρότυπο IEC 62443 είναι για την επιχειρησιακή τεχνολογία (OT), ότι είναι το πρότυπο ISO 27000 για την τεχνολογία πληροφοριών (IT).

Το IEC 62443 είναι στην πραγματικότητα μια σειρά προτύπων, τεχνικών εκθέσεων και σχετικών πληροφοριών που καθορίζουν διαδικασίες για την ασφάλεια των βιομηχανικών συστημάτων αυτοματισμού και ελέγχου (IACS). Αυτά τα έγγραφα είναι το αποτέλεσμα της διαδικασίας δημιουργίας προτύπων IEC όπου οι προτάσεις ANSI / ISA-62443 (Επιτροπή ISA99) και άλλες πληροφορίες (όπως το WIB) υποβάλλονται σε επιτροπές των εκάστοτε χωρών. Τα σχόλια εξετάζονται από διάφορες επιτροπές του IEC 62443 όπου συζητούνται και, εάν είναι απαραίτητο, γίνονται αλλαγές. Το IEC αναπτύσσει παγκόσμια πρότυπα υπό τη σημαία της Παγκόσμιας Συνεργασίας Προτύπων, η οποία περιλαμβάνει τα ISO και τα ITU ως μέλη.

Το πρότυπο IEC 62443 προσφέρει τις οδηγίες του οργανισμού σας για τη βελτίωση της ψηφιακής ασφάλειας και ασφάλειας του περιβάλλοντος IACS. Η εφαρμογή του προτύπου βελτιώνει το επίπεδο ασφάλειας στον κυβερνοχώρο του περιβάλλοντος OT- ή ICS / SCADA.

Ο κοινό-στόχος για τα πρότυπα IEC 62443 είναι οι «Τελικοί χρήστες» (End Users) και οι «Πάροχοι λύσεων» (Solution Porviders). Ο όρος «Παροχείς λύσεων» χρησιμοποιείται ως γενικός όρος για τους «Κατασκευαστές» (Manufacturers), «Ολοκληρωτές συστήματος» (System Integrators) και «Προμηθευτές» (Vendors), αλλά και οποιαδήποτε εταιρεία είναι ελεύθερη να εφαρμόσει το πρότυπο.

Το πρότυπο IEC 62443 αποτελείται από τέσσερις κατηγορίες: «Γενικά», «Πολιτικές & Διαδικασίες», «Σύστημα» και «Συστατικό»:

IEC 62443 1-X: Γενικά

Αυτή η κατηγορία περιέχει θεμελιώδεις πληροφορίες σχετικά με έννοιες, μοντέλα και ορολογία. Αυτά τα μέρη του προτύπου χρησιμοποιούνται ως βάση για τις άλλες κατηγορίες του προτύπου IEC 62443. «Πολιτικές & Διαδικασίες», «Σύστημα» και «Συστατικό».

IEC 62443 2-X: Πολιτικές και διαδικασίες
Η κατηγορία «Πολιτικές & Διαδικασίες» απευθύνεται κυρίως σε «Τελικούς χρήστες» και «Παρόχους λύσεων» και περιλαμβάνει τις διάφορες πτυχές για τη δημιουργία και τη διατήρηση ενός αποτελεσματικού Συστήματος Διαχείρισης Ασφάλειας στον κυβερνοχώρο (CSMS).

IEC 62443 3-X: Σύστημα
Τα μέρη του προτύπου σε αυτήν την κατηγορία περιγράφουν τις τεχνικές απαιτήσεις για το σχεδιασμό του συστήματος και παρέχουν κατευθυντήριες αρχές για την ασφαλή ανάπτυξη και ολοκλήρωση των συστημάτων. Το επίκεντρο αυτής της κατηγορίας είναι στους «Προμηθευτές λύσεων» και στο κέντρο αυτής της κατηγορίας βρίσκεται το μοντέλο ζώνης και αγωγών.

IEC 62443 4-X: Συστατικό
Η τελευταία κατηγορία περιέχει όλες τις τεχνικές οδηγίες για την ανάπτυξη προϊόντων, από τους «Κατασκευαστές», για παράδειγμα, για χρήση στο περιβάλλον IACS. Οι «Ολοκληρωτές Συστήματος» και οι «Τελικοί Χρήστες» μπορούν ακόμη να κάνουν χρήση αυτής της κατηγορίας λαμβάνοντας τις απαιτήσεις σε αυτά τα πρότυπα ως βάση για την επιλογή και την αγορά ασφαλών εξαρτημάτων που θα χρησιμοποιηθούν στα συστήματά τους.

5. BIMCO

Το **Baltic and International Maritime Council (BIMCO)** είναι η μεγαλύτερη διεθνής ναυτιλιακή ένωση στον κόσμο με περισσότερα από 100 χρόνια λειτουργίας, με πάνω από 2.300 μέλη και παρουσία σε 130 χώρες.

Βασικός στόχος του BIMCO είναι η διευκόλυνση των εμπορικών δραστηριοτήτων των μελών της, η ανάπτυξη τυποποιημένων συμβάσεων και ρητρών, καθώς και η παροχή ποιοτικών πληροφοριών, συμβουλών και εκπαίδευσης. Επιπλέον, προωθεί τις δίκαιες εμπορικές πρακτικές, το ελεύθερο εμπόριο και την ελεύθερη πρόσβαση στις αγορές, όντας υπέρμαχος της εναρμόνισης και της τυποποίησης όλων των ναυτιλιακών δραστηριοτήτων.

Συγκεκριμένα οι κατευθυντήριες γραμμές του BIMCO (BIMCO-ICS CS ON BOARD SHIPS, 2018) για τον έλεγχο της κυβερνοασφάλειας είναι οι παρακάτω:

- Ευαισθητοποίηση ως προς το Cyber Security από όλους
- Προσδιορισμός των απειλών
- Εντοπισμός ευπαθειών
- Αξιολόγηση της έκθεσης σε κινδύνους
- Ανάπτυξη μέτρων προστασίας και ανίχνευσης
- Καθιέρωση σχεδίων έκτακτης ανάγκη
- Απάντηση στα περιστατικά ασφάλειας στον κυβερνοχώρο

6. Νηογνώμονες

Οι νηογνώμονες παίζουν πολύ σημαντικό ρόλο στην καθοδήγηση των ναυτιλιακών εταιρειών σχετικά με το Cyber Security. Εκτός από οργανισμοί ελέγχου και πιστοποίησης των ναυτιλιακών εταιρειών, παίζουν πλέον και ρόλο συμβουλευτικό επειδή κατέχουν εξειδικευμένα άτομα με γνώσεις για το συγκεκριμένο θέμα. Παρακάτω παρουσιάζονται μερικοί από αυτούς και συγκρίνονται ώστε να δούμε τα κριτήρια επιλογής ενός νηογνώμονα.

6.1 DNVGL

Ο DNVGL είναι ο Νορβηγικός και ο Γερμανικός νηογνώμονας και οι υπηρεσίες που προσφέρει είναι ("Cyber Security Management Plan" DNVGL Confidential document):

- **Συνιστώμενη πρακτική σχετικά με την διαχείριση της ανθεκτικότητας στον κυβερνοχώρο:** Αυτή η πρακτική μπορεί να βρεθεί στον διαδικτυακό τόπο της εταιρείας και παρέχεται δωρεάν. Αυτό βοηθάει στην αξιολόγηση, βελτίωση και επαλήθευση της ανθεκτικότητας του ενεργητικού των εταιρειών και του προσωπικού τους στον κυβερνοχώρο.
- **Αξιολόγηση ασφάλειας στον κυβερνοχώρο:** Πραγματοποιείται από τις υψηλά καταρτισμένες ομάδες του οργανισμού σε συνεργασία με τα πληρώματα και τους υπαλλήλους στα γραφεία της εταιρείας έτσι ώστε να αναγνωριστούν τα κενά στις άμυνες της εταιρείας και στα αντίμετρα, τόσο προληπτικά όσο και αντιδραστικά, στα συστήματα πληροφορικής και τα συστήματα λειτουργίας.

Στόχος είναι η βοήθεια ώστε να δημιουργηθεί και να διατηρηθεί ένα αποτελεσματικό και οικονομικά αποδοτικό σύστημα ασφάλειας στον κυβερνοχώρο της κάθε εταιρείας.

• **Βελτίωση ασφάλειας στον κυβερνοχώρο:** Αυτό επιτυγχάνεται χρησιμοποιώντας συστηματικές μεθόδους αξιολόγησης, ώστε να κλείνουν αποτελεσματικά τα χάσματα στον κυβερνοχώρο και να υποστηρίζεται η ανάπτυξη σχεδίων βελτίωσης που αφορούν τα συστήματα, τον ανθρώπινο παράγοντα και τις διαδικασίες διαχείρισης.

• **Εκπαίδευση:** Παροχή προγραμμάτων εκπαίδευσης τα οποία καλύπτουν, απειλές, περιστατικά, κανονισμούς και μαθήματα πρόληψης απειλών. Τα προγράμματα εκπαίδευσης περιλαμβάνουν και ηλεκτρονική μάθηση εξ αποστάσεως η οποία μπορεί να πραγματοποιηθεί στο σκάφος ή στο γραφείο, έτσι ώστε τα πληρώματα να μπορούν να αντιμετωπίσουν τις βασικές πτυχές οποιουδήποτε συστήματος ασφαλείας στον κυβερνοχώρο καλύπτοντας με αυτόν τον τρόπο, τον ανθρώπινο παράγοντα.

• **Δοκιμές κοινωνικής μηχανικής:** Πραγματοποίηση μέτρησης επιπέδου ευαισθητοποίησης του προσωπικού σε σχέση με την ασφάλεια στον κυβερνοχώρο. Αυτό γίνεται με μετρήσεις από τις δοκιμές διείσδυσης χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής και phishing.

• **EU GDPR:** Βοήθεια συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (GDPR) μέσω έργων χάσματος και βελτίωσης.

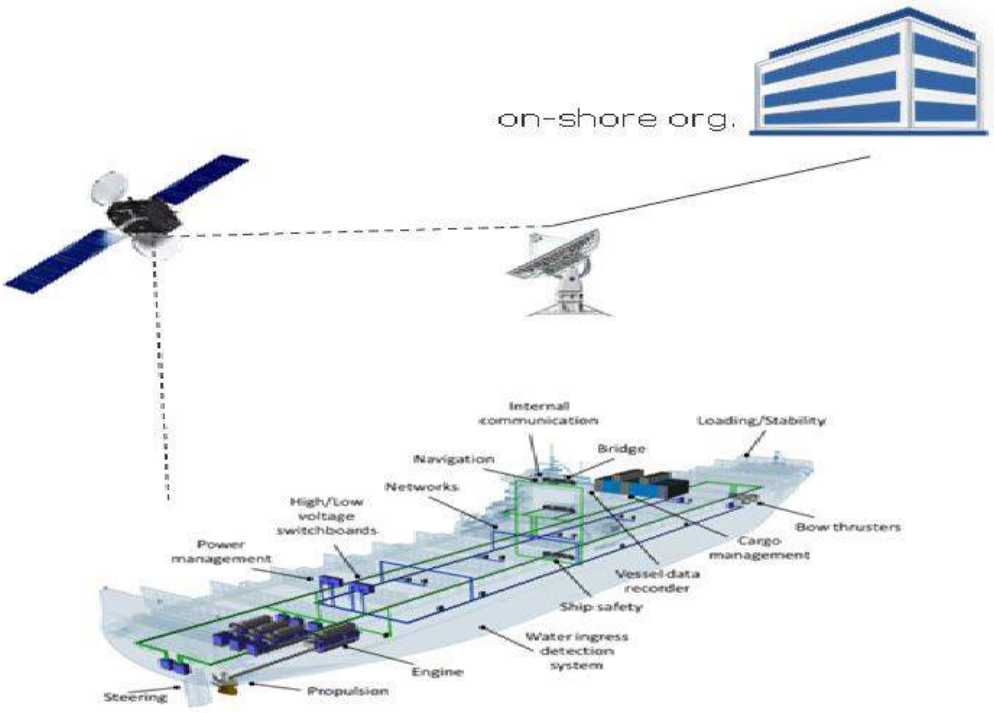
• **Εκπαιδευτικές δοκιμές αντιμετώπισης περιστατικών:** Εκτελούνται ασκήσεις για την εκπαίδευση και την επαλήθευση της απόκρισης στον κυβερνοχώρο τόσο στα πλοία όσο και στο γραφείο μιας εταιρείας. Αυτό συμβαίνει για να είναι προετοιμασμένοι για το χειρότερο,

• **Δοκιμή διείσδυσης - Penetration testing:** Δοκιμή της ανθεκτικότητας των φραγμών των συστημάτων μιας εταιρείας ώστε να μπορεί να διασφαλίσει τα περιουσιακά της στοιχεία και να τα καθιστά ασφαλή. Οι έλεγχοι διείσδυσης προσφέρουν πλήρη και αποτελεσματική επικύρωση των συστημάτων και των διαδικασιών τους.

• **Επαλήθευση - Verification:** Παροχή ελέγχου από τρίτους των απαιτήσεων ασφάλειας στον κυβερνοχώρο καθ' όλη τη διάρκεια ζωής ενός νεόδμητου πλοίου και στα πλοία που είναι ήδη σε λειτουργία.

• **Πιστοποίηση - certification:** Η DNV GL πιστοποιεί σύμφωνα με το ISO / IEC 27001 (η πιστοποίηση θα περιορίσει τη δυνατότητα παροχής συμβουλευτικών υπηρεσιών).

• **Έγκριση τύπου – Type Aproval:** Προσφέρει ένα πρόγραμμα έγκρισης τύπου για ασφάλεια στον κυβερνοχώρο έτσι ώστε να γίνεται επαλήθευση των εξαρτημάτων που εφαρμόζονται σε πλοία.



Εικόνα. Απεικόνιση επικοινωνίας γραφείου-πλοίου (DNVGL PUBLICATION)

6.2 ABS

Ο ABS είναι ο αμερικάνικος νηογνώμονας του οποίου το πρόγραμμα σχετικά με την ασφάλεια στον κυβερνοχώρο είναι μια συγκεκριμένη ναυτιλιακή προσέγγιση για τον εντοπισμό και την αντιμετώπιση του κυβερνο-επιχειρησιακού κινδύνου για θαλάσσια και υπεράκτια περιουσιακά στοιχεία και στόλους (CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES- ABS)

ΠΩΣ ΔΟΥΛΕΥΕΙ

Εξίσωση Cyber Risk FCI (Function –Connection –Identity) (Cyber security Advanced Solution – ABS).

- Έγκριση τύπου – Type Aproval: Προσφέρει ένα πρόγραμμα έγκρισης τύπου για ασφάλεια στον κυβερνοχώρο έτσι ώστε να γίνεται επαλήθευση των εξαρτημάτων που εφαρμόζονται σε πλοία.
- Λειτουργία (Function): Λογισμικό που ελέγχει μηχανές σε περιουσιακά στοιχεία.
- Σύνδεση (Connection). Φύση και αριθμός ψηφιακών διεπαφών που υποδεικνύουν την πολυπλοκότητα της ασφάλειας στον κυβερνοχώρο.
- Ταυτότητα (Identity). Άνθρωποι ή μηχανήματα που στέλνουν ή λαμβάνουν δεδομένα μέσω ψηφιακών διεπαφών.
- Υπολογιστής Δείκτη Κινδύνου (Risk Index Calculator)
- Μεθοδολογία θαλάσσιου ειδικού κινδύνου.
- Μέτρηση και υπολογισμός.
- Με δυνατότητα επέκτασης σε περιουσιακά στοιχεία και πλοία

ΥΠΗΡΕΣΙΕΣ

- Αξιολόγηση ασφάλειας στον κυβερνοχώρο (Cyber Security assessment)
- Κατάρτιση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο (Cyber Security Awareness Training)
- Γραφείο διαχείρισης κυβερνοασφάλειας (OT Cyber Management Office).
- Έλεγχος εγγράφων συστήματος (Controls System Documents)
- Αντιμετώπιση περιστατικών (Cyber Incident Response)
- Διαχείριση αλλαγών (Management of Change)
- Πρόγραμμα Standup (επαναφορά συστήματος)

6.3 BV - BUREAU VERITAS

Ο Bureau Veritas είναι ο γαλλικός νηογνώμονας και παρέχει υποστήριξη σε προγραμματιστές, κατασκευαστές και υπεύθυνους λήψης αποφάσεων που στοχεύουν σε προϊόντα πιο ασφαλή και αποδοτικά καθ 'όλη τη διάρκεια του κύκλου ζωής τους, από το σχεδιασμό έως τη λειτουργία (CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS).

Με τον Bureau Veritas ως πάροχο λύσεων που απευθύνεται στο σύστημα, μπορούν να επωφεληθούν το υλικό του συστήματος, το λογισμικό, η παρτίδα, οι άνθρωποι και η διαδικασία. Όποια και αν είναι η ανάγκη της εταιρείας και ο βαθμός ωριμότητάς της στον κυβερνοχώρο, παρέχεται βοήθεια σχετικά με τον χειρισμό των παρακάτω πτυχών (CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS):

- Αξιολόγηση της συμμόρφωσης στον κυβερνοχώρο διάγνωση, ανάλυση απειλών & αξιολόγηση κινδύνων
- Υπηρεσίες πιστοποίησης σύμφωνα με τα πρότυπα ISO 27001 IEC 62443, CYBER ESSENTIALS
- Υπηρεσίες πιστοποίησης σύμφωνα με τις κατευθυντήριες γραμμές του Bureau Veritas [BV-sW-200, BV-CAR CYBERSEC]
- Έλεγχοι επιτήρησης
- Δοκιμές κατά γνωστών ευπαθειών (CVE, CWE)
- Εταιρική υποστήριξη συμβουλευτικών υπηρεσιών για Cybersecurity Πλαίσιο αφοσιωμένης υποστήριξης, στρατηγική για ασφάλεια στον κυβερνοχώρο, ασφάλεια από τον σχεδιασμό, προσόντα και παρακολούθηση.
- Εκπαίδευση και ευαισθητοποίηση Σχετικά με τις απαιτήσεις του IEC 62443 και άλλα πρότυπα.

6.4 Lloyd's Register

Ο LR είναι ο αγγλικός νηογνώμονας και συγκεκριμένα με το θέμα της κυβερνοασφάλειας, δημιούργησε μια αποδοτική προσέγγιση όσον αφορά την αξιολόγηση της συμμόρφωσης με τις κατευθυντήριες γραμμές BIMCO, οι οποίες βασίζονται σε μεγάλο βαθμό στην Εθνικό πλαίσιο για τα πρότυπα και την τεχνολογία (NIST). Η αξιολόγηση των απειλών Cyber Security είναι το πρώτο βήμα που συνιστά η BIMCO και η NIST κατά την προσέγγιση της θέσης του κυβερνητικού συστήματος ναυτικής οργάνωσης και χάρη στην πρόσφατη εξαγορά της Nettitude, είμαστε σε θέση να προσφέρουμε ένα ολοκληρωμένο πλαίσιο για την αξιολόγηση απειλών και τη

διαχείριση κινδύνου τόσο διαχείριση στόλου γραφείων όσο και πλοία (https://www.lr.org/en/bimco-guidelines/).

Τι προσφέρει:

- **Υπηρεσίες πληροφοριών απειλής - Threat Intelligence Services**

Η αξιολόγηση απειλών και η μοντελοποίηση απειλών αποτελούν ζωτικά εργαλεία για την παροχή συναφών και αποτελεσματικών δραστηριοτήτων ασφάλειας σε ένα σύστημα. Όπως τονίζεται στο πλαίσιο BIMCO, μέχρι να γνωστοποιείται το από πού προέρχονται οι απειλές και τι τρωτά σημεία ή αδυναμίες υπάρχουν, δεν είναι γνωστό που να εφαρμόζονται οι έλεγχοι. Μπορεί να υποστηριχθεί η κατανόηση όλων αυτών των πληροφοριών σε ρεαλιστικά εργαστήρια και μπορεί επίσης να βοηθήσει στην εφαρμογή μιας ενεργού και σχετικής μεθοδολογίας κινδύνου σύμφωνα με τις απαιτήσεις της BIMCO (https://www.lr.org/en/bimco-guidelines/).

- **Αξιολόγηση κινδύνου- Risk Assesment**

παρέχουν στους έμπειρους ανώτερους συμβούλους ασφαλείας πληροφοριών στο χώρο της εταιρείας, για να αυξήσουν την κατανόηση και το προφίλ του κινδύνου γύρω από τα δεδομένα και τα συστήματα, αξιολογώντας τη στάση ασφαλείας των ναυτιλιακών οργανισμών για να καθορίσουν μια κατάλληλη στρατηγική και ένα σχέδιο δράσης για βελτίωση (https://www.lr.org/en/cyber-security/).

- **Έλεγχος διαδικασιών ασφάλειας Cyber Security**

Αναλαμβάνουν έναν έλεγχο διαδικασιών ασφαλείας στον κυβερνοχώρο που βασίζεται σε υψηλή ποιότητα. Ο έλεγχος θα διεξάγεται από έναν ελεγκτή με πιστοποίηση ISO 27001 και το αντικείμενο του ελέγχου θα συμφωνηθεί μεταξύ ελεγκτή και εταιρείας και θα βασίζεται σε μια επιλογή από συμφωνημένους ελέγχους, σε αντίθεση με κάθε έλεγχο. Αυτό θα διασφαλίσει ότι ο έλεγχος ολοκληρώνεται σε σχετικά σύντομο χρονικό διάστημα (https://www.lr.org/en/cyber-security/).

- **Έλεγχος επί του σκάφους – on board audit**

Ο κύριος στόχος του επιτόπιου ελέγχου είναι να προσδιοριστεί η συμμόρφωση του πλοίου με τις κατευθυντήριες γραμμές του BIMCO και να καθοριστεί η αποτελεσματικότητα των μέτρων ασφαλείας, των πολιτικών, των διαδικασιών και της ετοιμότητας για τα περιστατικά που σχετίζονται με τον κυβερνοχώρο. Ως αποτέλεσμα αυτής της δραστηριότητας, παρέχει πλήρη έκθεση των ευρημάτων με συστάσεις / χάρτες πορείας για βελτίωση και συμμόρφωση με το επιλεγμένο επίπεδο συμμόρφωσης BIMCO (https://www.lr.org/en/cyber-security/).

- **Αξιολόγηση ευπάθειας ή δοκιμή διείσδυσης- Vulnerability assessment or Penetration Testing**

Η αξιολόγηση ευπάθειας μπορεί να παρασχεθεί σε υπολογιστικά συστήματα (πλοήγηση, έλεγχος φορτίου, διαχείριση ισχύος, επικοινωνία κ.λπ.), δίκτυα πλοίων και οποιαδήποτε αυτοματοποίηση στο επιλεγμένο σκάφος. Εάν προσδιοριστεί κάποιος συγκεκριμένος στόχος, μπορεί επίσης να εκτελεστεί δοκιμή διείσδυσης. Η δοκιμή διείσδυσης είναι η προσπάθεια να εκμεταλλευτούν ενεργά τις αδυναμίες στο περιβάλλον από την πλευρά ενός εισβολέα με άμεση πρόσβαση στο δοκιμαζόμενο δίκτυο (https://www.lr.org/en/cyber-security/.

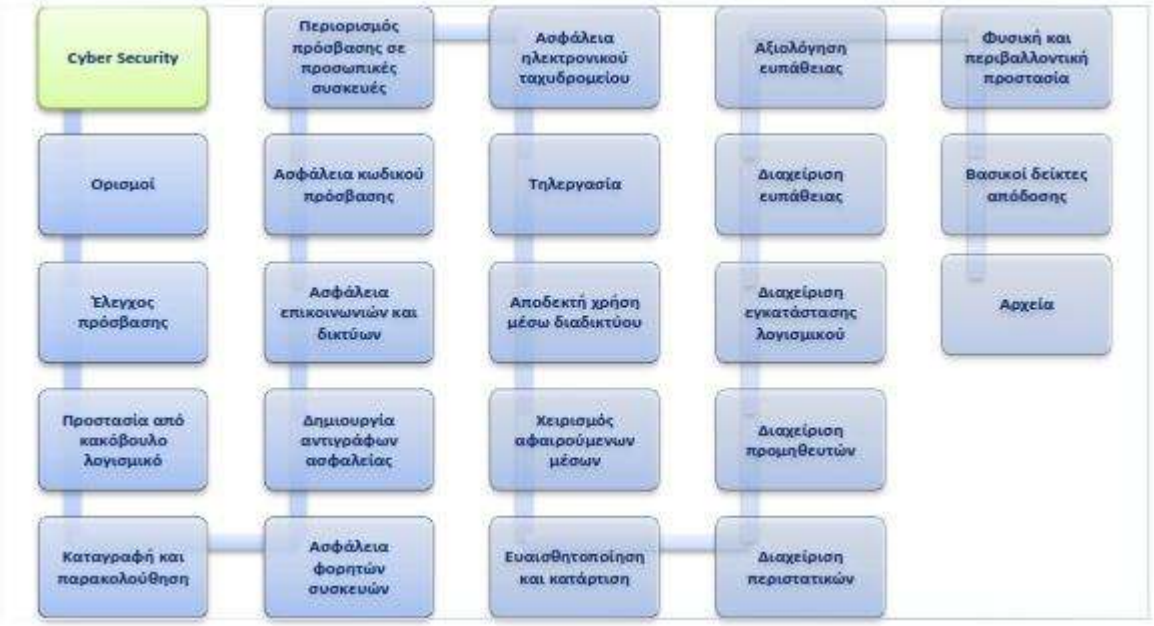
Συμπέρασμα:
Από την παραπάνω παρουσίαση μερικών νηογνωμόνων προκύπτει ότι οι υπηρεσίες που προσφέρουν στις ναυτιλιακές εταιρείες για τη ασφάλεια των πληροφοριών των πληροφοριών τους είναι ίδιες και αυτό συμβαίνει επειδή ακολουθούν τους κανονισμούς. Ενδεχομένως να αλλάζουν οι χρεώσεις καθώς και ο τρόπος που ενεργούν απέναντι στα θέματα ασφάλειας των ναυτιλιακών εταιρειών. Ωστόσο, πέρα από την ελεγκτική πλευρά που έχουν οι νηογνώμονες, επιβεβαιώνεται η συμβουλευτική πλέον φύση αυτών των εταιρειών απέναντι στις ναυτιλιακές εταιρείες.

7. Cyber Security σε μια ναυτιλιακή εταιρεία

Το Cyber Security σε μια ναυτιλιακή χωρίζεται σε δύο κατηγορίες οι οποίες όμως αλληλοσυνδέονται. Το Cyber Security για την εταιρεία και για τα πλοία της. Έτσι λοιπόν μια
ναυτιλιακή εταιρεία θα πρέπει να έχει δύο διαφορετικούς οδηγούς οι οποίοι αφορούν την ασφάλεια στον κυβερνοχώρο της και να είναι διαθέσιμοι σε όλους της τους υπαλλήλους.
Παρακάτω, κατασκευάστηκαν δύο οδηγοί οι οποίοι αφορούν γραφείο και πλοίο και λειτουργούν σαν εσωτερικές διαδικασίες της εταιρείας οι οποίες βασίζονται στα guidelines καθώς και στους απαιτούμενους κανονισμούς (BIMCO, 2018), (Kenneth J. Knapp, 2009).

7.1 Οδηγός Cyber Security εταιρείας

Στο παρακάτω σχήμα, βλέπουμε όλα τα σημεία που δίνει έμφαση και τις διαδικασίες που ακολουθεί μια ναυτιλιακή εταιρεία σχετικά με το Cyber Security για το γραφείο:



Εικόνα. Διαδικασίες Cyber Security Εταιρείας

Μια ναυτιλιακή εταιρεία εφαρμόζει κάποιες διαδικασίες οι οποίες λειτουργούν ως οδηγός και είναι διαθέσιμος προς όλους τους εργαζομένους, ώστε να προστατεύει τα δεδομένα και τα συστήματά της από οποιαδήποτε επίθεση στον κυβερνοχώρο (Yong-Chan Lee, Sang-Kyum Park, Woo-Kun Lee, Jun Kang, 2017).

Αυτός ο οδηγός περιλαμβάνει:
• **Ορισμούς:** Θεωρείται απαραίτητο κομμάτι έτσι ώστε οι εργαζόμενοι να κατανοήσουν τη σημασία της ασφάλειας του κυβερνοχώρου για την εταιρεία και τους κινδύνους που έρχονται αντιμέτωποι.

• **Έλεγχος πρόσβασης:** Αυτό καθορίζει τα δικαιώματα των χρηστών και την πρόσβασή τους στο σύστημα. Για παράδειγμα, άλλα δικαιώματα πρόσβασης έχουν οι διαχειριστές συστήματος και άλλα δικαιώματα έχουν οι υπάλληλοι πρακτικής άσκησης (Huge Boyes, 2014). Η πρόσβαση καθορίζεται από τα καθήκοντα που πρόκειται να εκτελέσει ο κάθε υπάλληλος ανάλογα με τη θέση του στην εταιρεία. Επίσης, η πρόσβαση των προμηθευτών στην εταιρεία καθορίζεται έτσι ώστε να μην απειλείται το σύστημα ασφάλειας της εταιρείας και δίνεται πρόσβαση σε συγκεκριμένα σημεία που αφορούν τις ανάγκες που έχει η εταιρεία τον συγκεκριμένο προμηθευτή (Kimberly Tam, Kevin Jones, 2019). Αυτό πραγματοποιείται ζητώντας πρόσβαση από τον υπεύθυνο ασφάλειας της εταιρείας έτσι ώστε να είναι ενημερωμένο το σύστημα για τις άδειες πρόσβασης από εξωτερικούς προμηθευτές ανά πάσα στιγμή. Η άδεια αυτή θα πρέπει να έχει συγκεκριμένη χρονική διάρκεια η οποία μετά το πέρας της θα πρέπει να καταργείται (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).

• **Προστασία από κακόβουλο λογισμικό (malware):** Αυτό συνεπάγεται την αξιολόγηση του λογισμικού πριν την εγκατάσταση στο σύστημα (Kimberly Tam, Kevin Jones, Maria Papadaki, 2012). Έπειτα την εγκατάσταση και τη διαμόρφωση ώστε να ενημερώνεται αυτόματα μέσω διαδικτύου. Επίσης θα πρέπει να γίνει διαμόρφωση των ρυθμίσεων του υπολογιστή. Αυτό περιλαμβάνει την απενεργοποίηση της αυτόματης εκτέλεσης USB και ότι μόνο εξουσιοδοτημένα USB μπορούν να συνδεθούν στο δίκτυο, αποκλεισμός περιήγησης σε μη ασφαλής σελίδες, την απενεργοποίηση αναδυόμενων παραθύρων και την απενεργοποίηση μακροεντολών του EXCEL. Επίσης, θα πρέπει να γίνεται καταχώρηση των εταιρικών τηλεφώνων και υπολογιστών για κρυπτογράφηση και συμμόρφωση με τις απαιτήσεις ασφαλείας του συστήματος και δεν θα πρέπει να επιτρέπεται η εγκατάσταση άγνωστου λογισμικού από τους απλούς χρήστες σε εταιρικούς υπολογιστές πριν από τον έλεγχο και την άδεια του IT τμήματος της εταιρείας. Τέλος, θα πρέπει να γίνεται επέκταση του κεντρικού λειτουργικού συστήματος σε διακομιστές και υπολογιστές (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).

• **Καταγραφή και Παρακολούθηση:** Τα συστήματα ICT (Information and Communication Technologies) της εταιρείας θα πρέπει να παρακολουθούνται ώστε να διασφαλίζουν την ταυτοποίηση των απειλών. Η καταγραφή και παρακολούθηση πραγματοποιείται στα συστήματα Firewall, στα συστήματα ανίχνευσης και πρόληψης εισβολών, σε πύλες άλλων δικτύων, server, σε φορητούς υπολογιστές και κινητά τηλέφωνα. Θα πρέπει να υπάρχει αυτόματη ειδοποίηση ώστε να παρέχεται άμεση αντίδραση σε οποιαδήποτε απειλή. Για τα αρχεία προσωπικών δεδομένων, θα πρέπει να λαμβάνεται υπόψη η νομοθεσία (2472/1997, GDPR). Τέλος, οι διαχειριστές του συστήματος απαγορεύεται να διαγράψουν ή να απενεργοποιήσουν τους μηχανισμούς καταγραφής για τους δικούς τους λογαριασμούς (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

• **Ασφάλεια κωδικού πρόσβασης:** Περιλαμβάνει τους κανόνες δημιουργίας όπως το ελάχιστο μήκος του κωδικού πρόσβασης, να αποτελείται από κεφαλαία και πεζά γράμματα καθώς και αριθμητικούς χαρακτήρες και σύμβολα. Επίσης δεν θα πρέπει να περιλαμβάνεται το όνομα χρήστη στον κωδικό πρόσβασης και να μην επαναλαμβάνονται οι προηγούμενοι κωδικοί. Αυτό γίνεται μέσω μια διαδικασίας ελέγχου του συστήματος η οποία δεν επιτρέπει στον χρήστη την δημιουργία ενός κωδικού που περιλαμβάνει τα παραπάνω. Η αλλαγή του κωδικού θα πρέπει να πραγματοποιείται εντός ορισμένου χρονικού πλαισίου και όχι σε μικρότερο διάστημα από μία μέρα για παράδειγμα της ζωής του κωδικού. Ο χρήστης θα πρέπει να κρατάε μυστικό τον κωδικό του, να μην τον αποθηκεύει αυτόματα στο σύστημα του υπολογιστή του και μόνο το IT τμήμα επιτρέπεται να γνωρίζει τον κωδικό του (Huge Boyes, 2014).

• **Ασφάλεια επικοινωνιών και δικτύων:** Σε αυτό το στάδιο γίνεται σχεδιασμός ασφάλειας δικτύων αναγνωρίζοντας τις πιθανές απειλές, το επίπεδο εμπιστοσύνης μεταξύ συστήματος και δικτύων που πρόκειται να συνδεθούν στο σύστημα, η διαθεσιμότητα του συστήματος καθώς και η γεωγραφική απόσταση και η μελλοντική εξάπλωση. Επίσης, χρησιμοποιούνται συστήματα εντοπισμού και πρόληψης εισβολών στο σύστημα για την κεντρική διαχείριση και παρακολούθηση των δικτύων καθώς και εικονικά δίκτυα VLAN. Χρησιμοποιείται ισχυρή κρυπτογράφηση έτσι ώστε να διασφαλιστεί η εμπιστευτικότητα των δεδομένων που μεταδίδονται μέσω κάποιου δημόσιου δικτύου. Το δίκτυο υποδομών της επιχείρησης χωρίζεται σε πολλά εικονικά δίκτυα ανάλογα με τις ανάγκες και της απαιτήσεις του σχεδιασμού ασφαλείας. Τα συστήματα όπως φυσικής ασφάλειας, τηλεφωνικό κέντρο και λειτουργικά όπως κλιματισμός, συνδέονται αποκλειστικά σε VLAN χωρίς τη δυνατότητα πρόσβασης στο κύριο δίκτυο του συστήματος. Στο δίκτυο WiFi μπορούν να συνδέονται φορητοί υπολογιστές και εταιρικά κινητά, προσωπικές συσκευές καθώς και μπορεί να υπάρχει και σύνδεση στο ιντερνέτ από επισκέπτες. Τέλος, η φυσική ασφάλεια η οποία αφορά τον εξοπλισμό δικτύου προτείνεται να προστατεύεται με την τοποθέτηση σε κατάλληλα διαμορφωμένα ράφια ή σε άξονες δικτύου και να έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα σε αυτά (Kimberly Tam, Kevin Jones, Maria Papadaki, 2012).

• **Δημιουργία αντιγράφων ασφαλείας:** Θα πρέπει να δημιουργούνται αντίγραφα ασφαλείας κυρίως για τα κρίσιμα αρχεία τα οποία αφορούν τις ρυθμίσεις του συστήματος καθώς και στους εταιρικούς υπολογιστές όλα τα αρχεία που είναι αποθηκευμένα στον φάκελο «τα έγγραφα μου» των χρηστών. Όλα αυτά τα δεδομένα θα πρέπει να κρυπτογραφούνται και να διατηρούνται στο σύστημα. Αυτή η διαδικασία πραγματοποιείται μέσω κάποιου μηχανισμού του συστήματος η οποία δημιουργεί αντίγραφα ασφαλείας αυτόματα και στη συνέχεια τα κρυπτογραφεί. Η περίοδος που πρέπει να διατηρούνται τα αντίγραφα αυτά ορίζεται συνήθως σε ένα χρόνο και έπειτα από το πέρας αυτού πραγματοποιείται καταστροφή σύμφωνα με το πρότυπο ISO 27001. Ειδικά αντίγραφα ασφαλείας δημιουργούνται μόνο κατά την αναβάθμιση του συστήματος. Τέλος θα πρέπει να γίνεται δοκιμή και επαναφορά αντιγράφων ασφαλείας κάθε ορισμένο χρονικό διάστημα ώστε να δοκιμάζεται η ακεραιότητα και η πληρότητα του περιεχομένου τους (ISO 27001, Regulations) (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

• **Ασφάλεια φορητών συσκευών:** Θα πρέπει να εφαρμόζεται κρυπτογράφης πλήρους δίσκου και οι συσκευές που δεν είναι κρυπτογραφημένες δεν θα πρέπει να χρησιμοποιούνται για επιχειρησιακούς σκοπούς. Εάν πραγματοποιηθεί απώλεια, ζημιά ή κλοπή της συσκευής θα πρέπει να αναφερθεί άμεσα στον υπεύθυνο ασφαλείας του

τμήματος πληροφορικής. Για τη σύνδεση στις συσκευές απαιτείται PIN και δεν θα πρέπει να μοιράζονται με τα υπόλοιπα μέλη μιας οικογένειας. Θα πρέπει επίσης να συνδέονται σε ασφαλή δίκτυα. Οι φορητοί υπολογιστές θα πρέπει να ελέγχονται αυτόματα για μη συμμόρφωση μέσω των προτύπων ασφαλείας της εταιρείας, σε περίπτωση μη συμμόρφωσης απαγορεύεται αυτόματα η πρόσβαση σε δίκτυο της εταιρείας. Επίσης η οθόνη είναι ρυθμισμένη να κλειδώνει αυτόματα έπειτα από 15 λεπτά αδράνειας. Η πρόσβαση σε μη ασφαλής σελίδες είναι περιορισμένη και το λογισμικό προστασίας είναι προεγκατεστημένο σε όλους τους φορητούς υπολογιστές της εταιρείας (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer – Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012)

• **Περιορισμός πρόσβασης στο δίκτυο από τις προσωπικές φορητές συσκευές:** οι προσωπικές φορητές συσκευές όπως και οι συσκευές επισκεπτών στην εταιρεία έχουν δικαίωμα να συνδέονται μόνο στα ασύρματα δίκτυα της εταιρείας τα οποία αφορούν τους επισκέπτες. Μετά την απομάκρυνση από την εταιρεία η εταιρεία διατηρεί το δικαίωμα να διαγράφει απομακρυσμένα εταιρικά δεδομένα από συσκευές σε περίπτωση συμβάντος η τερματισμού της απασχόλησης (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

• **Τηλεργασία:** Η τηλεργασία αφορά τη δυνατότητα των υπαλλήλων της εταιρείας να εργάζονται από διαφορετικές περιοχές εκτός της εταιρείας. Γι αυτό το λόγο οι εργαζόμενοι που χρησιμοποιούν τέτοιου είδους συσκευές θα πρέπει να γνωρίζουν σχετικά με τους κινδύνους που αντιμετωπίζουν και να μην αφήνουν τις συσκευές τους ανοιχτές χωρίς επίβλεψη ώστε να αποφευχθεί η διαρροή δεδομένων. Επίσης στις συσκευές αυτές εφαρμόζονται πρόσθετα στοιχεία ασφαλείας όπως ακριβώς και στις συσκευές κινητών τηλεφώνων. Επιπρόσθετα, όταν τερματίζεται κάποια σχέση εργασίας οι συσκευές επιστρέφονται στην εταιρεία και τα δεδομένα που εμπεριέχουν καταστρέφονται. Τέλος, δύναται να εφαρμοστεί έλεγχος των ιδιόκτητων συσκευών σχετικά με τις εταιρικές πληροφορίες (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

• **Ασφάλεια ηλεκτρονικού ταχυδρομείου:** Αυτό αφορά τους ιδιωτικούς λογαριασμούς των χρηστών της εταιρείας οι οποίοι είναι κατασκευασμένοι για να εξυπηρετούν επιχειρηματικούς σκοπούς και έχουν περιορισμένη πρόσβαση σε προσωπική επικοινωνία. Το σύστημα αποστολής και λήψης email επιτρέπει την ανταλλαγή μηνυμάτων ορισμένου μεγέθους (π.χ. ως 30Mb). Οι υπάλληλοι είναι υπεύθυνοι προσωπικά για τη σωστή χρήση των λογαριασμών τους και θα πρέπει να συμβαδίζει σε σχέση με τις πολιτικές της εταιρείας οι οποίες αφορούν την ασφάλεια. η εταιρεία κατά κανόνα δεν έχει πρόσβαση στις επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου κατ' εξαίρεση όμως όταν κριθεί απαραίτητο επειδή μπορεί κάτι να επηρεάσει την εταιρεία ως προς τα επίπεδα ασφάλειάς της η εταιρεία μπορεί να επέμβει με την παρακολούθηση των επικοινωνιών (Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, 2012).

• **Αποδεκτή χρήση μέσω διαδικτύου:** Είναι η πρόσβαση των χρηστών στο διαδίκτυο μέσω εγκεκριμένου από την εταιρεία εξοπλισμού. Η χρήση προσωπικών μόντεμ απαγορεύονται βάση πολιτικής της εταιρείας. Η εταιρία επίσης έχει περιορισμένη πρόσβαση σε διαδικτυακούς τόπους που θεωρεί επικίνδυνους, έχει δικαίωμα να αναθεωρεί περιεχόμενα σελίδων και απαγορεύει την είσοδο σε σελίδες που εμπεριέχουν ακατάλληλο περιεχόμενο. Ο χρήστης έχει αποκλειστική ευθύνη σχετικά με τις αγοροπωλησίες που πραγματοποιεί μέσω διαδικτύου και αποθηκεύει προσωπικά δεδομένα και κάρτες (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Χειρισμός αφαιρούμενων μέσων:** Απαγορεύεται η πρόσβαση από μη εξουσιοδοτημένες συσκευές στο σύστημα της εταιρείας. Η μεταφορά πληροφοριών από εξωτερικούς παράγοντες στην εταιρεία γίνεται μόνο μέσω ενός υπολογιστή ο οποίος είναι για επισκέπτες και δεν είναι συνδεδεμένος στο ιντερνέτ. Όλα τα εξωτερικά μέσα όπως κάμερες, USB και εξωτερικούς σκληρούς επιτρέπεται να συνδέονται στο σύστημα ύστερα από εξουσιοδότηση από το IT. Για οποιαδήποτε προσπάθεια σύνδεσης από κάποια συσκευή πραγματοποιείται αυτόματη σάρωση. Θα πρέπει να διασφαλίζεται η κατάλληλη χρήση και η ασφάλεια των πληροφοριών σε εξωτερικές συσκευές αποθήκευσης καθώς και να διασφαλίζεται η αποθήκευση των συσκευών σε ασφαλές μέρος για την αποφυγή κλοπής και κατόπιν εισβολής στο σύστημα. Σε περίπτωση κλοπής η καταστροφής συσκευής οι εργαζόμενοι έχουν αποκλειστική ευθύνη και θα πρέπει να ενημερώνουν άμεσα τους υπεύθυνους (YoungChan Lee, Sang-Kyun Park,Woo-Kun Lee, Jun Kang, 2017).

• **Ευαισθητοποίηση και κατάρτιση:** Σε αυτό το στάδιο οι χρήστες του συστήματος θα πρέπει να γνωρίζουν τους βασικούς κανόνες σχετικά με τους κινδύνους για την ασφάλεια στον κυβερνοχώρο και την αδυναμία των τεχνικών ελέγχων να αποτρέψουν κάποια πιθανή επίθεση.
Οι τακτικές που πρέπει να ακολουθούνται είναι:

- Όχι απάντηση σε μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία σχετίζονται με οικονομικές συναλλαγές ή προσωπικές πληροφορίες εκτός εάν ο χρήστης γνωρίζει την πηγή.
- Όχι άνοιγμα συνημμένων αρχείων ή συνδέσμων. Κατ' εξαίρεση μόνο κατόπιν επιβεβαίωσης με τον αποστολέα.
- Όχι παροχή κωδικών πρόσβασης με οποιοδήποτε τρόπο.
- Όχι ενημέρωση λογισμικού χωρίς σχετική άδεια και απενεργοποίηση τοίχους προστασίας.

Η εκπαίδευση σχετικά με την ασφάλεια στον κυβερνοχώρο είναι υποχρεωτική και εφαρμόζεται σε όλο το προσωπικό μέσω ηλεκτρονικής διδασκαλίας ή διδασκαλίας στην τάξη. Σε περιπτώσεις νεοεισερχόμενων στην εταιρεία η διαδικασία ολοκληρώνεται κατά την περίοδο προσαρμογής (Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respico, 2018).

• **Διαχείριση Εγκατάστασης λογισμικού:** Όλα τα λογισμικά που χρησιμοποιεί η εταιρεία θα πρέπει να είναι αγορασμένα από την ίδια από το τμήμα IT και να γίνεται έλεγχος του προμηθευτεί αλλά και του τρόπου που δουλεύουν. Η εγκατάσταση του λογισμικού στην εταιρεία πραγματοποιείται μόνο από τον υπεύθυνο του τμήματος IT καθώς και τυχόν πληροφορίες παρέχονται από το συγκεκριμένο τμήμα. Επίσης θα πρέπει να βεβαιώνεται ότι ο πάροχος υπηρεσιών είναι εξουσιοδοτημένος και εκτελεί τη συντήρηση του λογισμικού (Kimberly Tam, Kevin Jones, 2019).

• **Διαχείριση ευπάθειας:** Οι σταθμοί εργασίας και οι διακομιστές που ανήκουν στην εταιρεία θα πρέπει να έχουν εγκατεστημένες τις ενημερώσεις ασφαλείας λειτουργικού συστήματος για την προστασία τους από τις γνωστές ευπάθειες. Η ευπάθεια θα πρέπει να συμμορφώνεται με τις ακόλουθες ελάχιστες βασικές απαιτήσεις για να εξασφαλιστε η ασφάλεια του συστήματος και των δεδομένων του τα οποία βρίσκονται στο προεπιλεγμένο λειτουργικό σύστημα, service pack, επείγουσες επιδιορθώσεις και επίπεδο επιπέδου. Οι ενημερώσεις ασφαλείας θα πρέπει να δοκιμάζονται πριν από την εγκατάσταση από τους διαχειριστές του συστήματος. Οι διακομιστές και οι σταθμοί εργασίας ενημερώνονται περιοδικά μέσω κεντρικής πλατφόρμας (για παράδειγμα μήνες για διακομιστές, 1 μήνα για σταθμούς εργασίας). Όταν απελευθερωθούν οι

κρίσιμες ενημερώσεις, η ευπάθεια αναγνωρίζεται αμέσως (Kimberly Tam, Kevin Jones, 2019).

• **Αξιολόγηση ευπάθειας:** Η εταιρεία θα πρέπει να διενεργεί εκτιμήσεις ευπάθειας όλων των περιουσιακών της στοιχείων και των πληροφοριών εντός της περιμέτρου του κτιρίου των γραφείων της (διακομιστές, σταθμοί εργασίας, δίκτυα, κτλ). Αυτό θα πρέπει να γίνεται σε κατάλληλη χρονική στιγμή ώστε να μη γίνει διακοπή κάποιας λειτουργίας. Τα αποτελέσματα θα πρέπει να αντιμετωπίζονται ως εμπιστευτικές πληροφορίες. Η σάρωση θα πραγματοποιείται μέσω ενός εργαλείου κεντρικά εγκατεστημένου το οποίο θα αποδίδει τιμές σοβαρότητας των ευπαθειών του συστήματος. Το IT τμήμα θα πρέπει να εξετάζει τα ευρήματα ανάλογα με τη σοβαρότητα που έχουν για το σύστημα για παράδειγμα τα κρίσιμα σημεία ευπάθειας θα πρέπει να αντιμετωπιστούν εντός ενός μηνός από την ανακάλυψή τους ενώ τα τρωτά σημεία υψηλής σοβαρότητας θα πρέπει να αντιμετωπιστούν μέσα σε 3 μήνες από την ανακάλυψή τους. Τέλος έπειτα από το διάστημα των τριών μηνών θα πρέπει να πραγματοποιηθεί νέα αξιολόγηση έτσι ώστε να διασφαλιστεί ότι τα σημεία κρίσιμης σοβαρότητας δεν απειλούν πια το σύστημα (Kimberly Tam, Kevin Jones, 2019).

• **Διαχείριση προμηθευτών:** Σε γενικές γραμμές η εταιρεία θα πρέπει να γνωρίζει πολύ καλά τους προμηθευτές της και να διαχειρίζεται πολύ σωστά αυτό το κομμάτι ώστε να αποφευχθεί οποιαδήποτε διείσδυση στο σύστημά της. Για το λόγο αυτό θα πρέπει να υπάρχει γραπτή σύμβαση μεταξύ εταιρείας- προμηθευτή όπου θα αναγράφονται όλες οι απαιτήσεις ασφαλείας της εταιρείας και θα πρέπει να τηρούνται από τον προμηθευτή. Ο προμηθευτής θα πρέπει να συμφωνεί σε μη αποκάλυψη πληροφοριών της εταιρείας ώστε να διατηρείται η εμπιστευτικότητα μεταξύ πελάτη-προμηθευτή.
Επίσης θα πρέπει να υπάρχει συμφωνία επεξεργασίας προσωπικών δεδομένων σε περιπτώσεις που χρειάζεται και θα πρέπει να βασίζεται στα πρότυπα που επιτάσσει η εκάστοτε νομοθεσία. Τέλος το σύστημα ποιότητας του προμηθευτή σχετικά με τις δραστηριότητες του κύκλου ζωής του λογισμικού κτλ θα πρέπει να εμπεριέχει τεκμηριωμένες διαδικασίες για την ασφάλεια στον κυβερνοχώρο (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017).

• **Διαχείριση περιστατικού:** Σε αυτή την περίπτωση, σε πρώτη φάση η εταιρεία θα πρέπει να έχει τη δυνατότητα να κατηγοριοποιήσει το περιστατικό. Τα περιστατικά κατηγοριοποιούνται ως εξής:

1. Άρνηση παροχής υπηρεσίας.
2. Κακόβουλος κώδικας.
3. Μη εξουσιοδοτημένη πρόσβαση στο σύστημα.
4. Ακατάλληλη χρήση από άτομο που δεν έχει τη γνώση στο σύστημα.

Όλα τα παραπάνω κατηγοριοποιούνται σε σχέση με το πόσο επηρεάζουν την ακεραιότητα, την διαθεσιμότητα και την εμπιστευτικότητα του συστήματος (Kimberly Tam, Kevin Jones, 2019).
Κάποια παραδείγματα περιστατικών είναι όταν μολύνεται το σύστημα από κάποιο κακόβουλο λογισμικό, βλάβες ή υπερφόρτωση υλικού ή λογισμικού, παραβίαση ψηφιακών δεδομένων, μη εξουσιοδοτημένη πρόσβαση σε κάποιο σταθμό εργασίας, διακομιστές κ.α., λήψη ανεπιθύμητων μηνυμάτων, κατεστραμμένα αρχεία ή τα αρχεία δεν λειτουργούν, κτλ. Στη συνέχεια θα πρέπει να τεθεί κατάσταση προτεραιότητας αντιμετώπισης περιστατικού σε σχέση με τον παγκόσμιο κύκλο κυβερνοασφάλειας.
Τα κριτήρια αφορούν τον αντίκτυπο και το πόσο επείγον είναι το περιστατικό για την εταιρεία.

Οι κύριες φάσεις χειρισμού των περιστατικών από την εταιρεία είναι:

1. Προετοιμασία
2. Ανίχνευση
3. Ταξινόμηση
4. Περιορισμός- εξάλειψη
5. Ανάκτηση
6. Δραστηριότητα μετά το συμβάν

• **Φυσική και περιβαλλοντική προστασία:** Αυτό συνεπάγεται ότι η εταιρεία αποτελείται από ασφαλείς περιοχές με πρόσβαση σε αυτή με τη χρήση χειριστηρίων εισόδου. Επίσης, μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ασφαλείς περιοχές και αυτό ύστερα από έγκριση του υπεύθυνου ασφάλειας. Υπάρχει προστασία από περιβαλλοντικές απειλές και χρήση UPS σε περιπτώσεις διακοπής ρεύματος ώστε να αποφευχθεί η διαγραφή των αρχείων. Επιπρόσθετα, η είσοδος στην εταιρεία θα πρέπει να γίνεται βάση ελέγχου όπως επιβάλλει η πολιτική ελέγχου φυσικής πρόσβασης (Huge Boyes, 2014).

• **Βασικοί δείκτες απόδοσης:** είναι οι στόχοι KPIs. Γίνεται ανασκόπηση του συστήματος από τη διοίκηση της εταιρείας ώστε να αποφευχθούν επιθέσεις και να τεθεί το σύστημα αποδοτικό (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts , 2017).

• **Αρχεία:** Σχετικά με τα αρχεία θα πρέπει να ελέγχονται τα δικαιώματα πρόσβασης να εφαρμόζονται ετήσιοι έλεγχοι δικαιωμάτων πρόσβασης και τέλος να εφαρμόζεται δοκιμή δημιουργίας αντιγράφων ασφαλείας(BIMCO, 2018).

7.2 Οδηγός Cyber Security On Board

Με τον ίδιο τρόπο που μια εταιρεία έχει την ανάγκη να προστατεύσει τα δεδομένα και τα συστήματά της στο γραφείο, χρησιμοποιεί έναν παρόμοιο οδηγό και για τα πλοία της.
Παρακάτω βλέπουμε κάποιους βασικούς κανόνες οι οποίοι συνδέονται με το Cyber Security On Board.

Εικόνα. Διαδικασίες Cyber Security στο πλοίο

Πιο αναλυτικά σχετικά με τον οδηγό των διαδικασιών για Cyber Security που εφαρμόζονται στο πλοίο:

• **Σκοπός:** Ο σκοπός του οδηγού που αφορά τα πλοία είναι να καθοριστούν οι απαιτήσεις ασφαλείας που σχετίζονται με τον κυβερνοχώρο και αφορούν τον κώδικα ISM σε μια ναυτιλιακή.

• **Ορισμοί:** Όπως και στον οδηγό για το γραφείο, έτσι και στον οδηγό για το πλοίο ορίζονται οι ορισμοί οι οποίοι αφορούν την ασφάλεια στον κυβερνοχώρο.

• **Έλεγχος πρόσβασης:** Το πλήρωμα θα πρέπει να διαθέτει δικαιώματα στο δίκτυο του πλοίου ανάλογα με τα καθήκοντα που καλείται να εκτελέσει και δεν πρέπει να χορηγούνται πρόσθετα δικαιώματα σε άτομα. Αυτό θα δίνεται μόνο από τον διαχειριστή του συστήματος και κανείς άλλος δεν θα έχει δικαίωμα να αλλάζει ή να προβάλλει τα δικαιώματα των χρηστών. Ο διαχειριστής μπορεί επίσης να δώσει δικαιώματα προνομιακής πρόσβασης σε άτομα που κάνουν μια πιο εξειδικευμένη δουλειά στο πλοίο καθώς και να καθορίσουν το χρονικό διάστημα σύνδεσης όπου το πλήρωμα θα αποσυνδέεται από τον υπολογιστή όταν ολοκληρωθούν οι εργασίες και θα τίθεται συγκεκριμένος χρόνος όπου θα ενεργοποιείται η προφύλαξη οθόνης (Hugh Boyes 2014).

• **Προστασία από κακόβουλο λογισμικό:** για να μειωθεί ο κίνδυνος προσβολής από κάποιο ιό θα πρέπει όπως εφαρμόζεται και στο γραφείο να εφαρμόζονται και στο πλοίο αντίστοιχα μέτρα προστασίας. Το σύστημα στο πλοίο ελέγχεται κεντρικά από τους διαχειριστές του συστήματος δηλαδή από την εταιρεία (Joseph DiRenzo – Nicole K. Drumhiller - Fred S. Roberts, 2017). Το πρόγραμμα προστασίας υποστηρίζει on line ενημερώσεις για κακόβουλο λογισμικό, καθημερινές προγραμματισμένες σαρώσεις, αφαίρεση αυτόματων σαρώσεων μέσων που δεν είναι του συστήματος και η χρήση USB θα πρέπει να είναι εξουσιοδοτημένη από το τμήμα πληροφορικής της εταιρείας (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Ασφάλεια κωδικών πρόσβασης:** Οι κωδικοί πρόσβασης θα πρέπει να προστατεύονται και να μην είναι σε κοινή θέα πάνω στο πλοίο και δεν επιτρέπεται να αλλάζουν οποιουδήποτε πάνω στο πλοίο. Οι πλοίαρχοι θα πρέπει να αλλάζουν κωδικούς σε κάθε αλλαγή αρχηγίας ώστε να διασφαλίζεται η εμπιστευτικότητα των πληροφοριών και των συστημάτων στο πλοίο. Επίσης, οι κωδικοί πρόσβασης δεν πρέπει να διαμοιράζονται μέσω ηλεκτρονικού ταχυδρομείου. Επιπρόσθετα, οι κωδικοί δεν θα πρέπει να ίδιοι με τους προηγούμενους και θα πρέπει να τηρούν κάποιους συγκεκριμένους κανόνες κατά τη δημιουργία τους όπως ακριβώς γίνεται και στο γραφείο (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017) (Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts, 2017)

• **Ασφάλεια δικτύου:** για να είναι ασφαλές ένα δίκτυο θα πρέπει να λαμβάνονται υπ όψιν οι αρχές ασφαλείας κατά τον σχεδιασμό του. Οι αρχές ασφάλειας περιλαμβάνουν το επίπεδο κρισιμότητας των πληροφοριών που μεταφέρονται, τις πιθανές απειλές, το επίπεδο εμπιστοσύνης μεταξύ συστημάτων και δικτύου που πρόκειται να συνδεθούν σε αυτό, τη διαθεσιμότητα του δικτύου η οποία απαιτεί επίπεδα, τα μέτρα προστασίας σε σχέση με τοποθεσίες που έχουν πρόσβαση στο δίκτυο, τον διαχωρισμό των δικτύων βάση διαφορετικών επιχειρηματικών επιπέδων και τέλος τείχη προστασίας και χρήση εικονικών δικτύων με τα οποία εξασφαλίζεται μόνο η εξουσιοδοτημένη κυκλοφορία στο δίκτυο (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Αντίγραφα ασφαλείας:** με τον ίδιο τρόπο του γραφείου έτσι και για το πλοίο θα πρέπει να δημιουργούνται αντίγραφα ασφαλείας και για το πλοίο. Αυτά θα πρέπει να αποθηκεύονται σε ασφαλή τοποθεσία, να αναπτυχθεί μια αυτοματοποιημένη διαδικασία για την δημιουργία τους και οι διαχειριστές του συστήματος να διασφαλίζουν ότι τα αντίγραφα ολοκληρώθηκαν με επιτυχία και να επαληθεύουν την ποσότητα που δημιουργήθηκε. Η μέθοδος που χρησιμοποιείται είναι αυτοματοποιημένη και πραγματοποιείται κάθε ορισμένο χρονικό διάστημα από τους διαχειριστές του συστήματος. Για παράδειγμα μια φορά την εβδομάδα μπορούμε να έχουμε ένα πλήρες αντίγραφο ασφαλείας (Young-Chan Lee, Sang-Kyun Park, WooKun Lee, Jun Kang, 2017).

• **Έλεγχος πρόσβασης ιδιωτικών συσκευών:** Σχετικά με τις προσωπικές συσκευές έχουν δικαίωμα να συνδέονται μόνο στο ασύρματο δίκτυο του πληρώματος και οι επισκέπτες στο ίδιο δίκτυο μόνο κατόπιν έγκρισης του πλοιάρχου (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Διαχείριση αφαιρούμενων μέσων:** Αυτό το κομμάτι αφορά όλες τις αφαιρούμενες συσκευές αποθήκευσης. Η πολιτική της εταιρείας απαγορεύει την πρόσβαση τέτοιου είδους συσκευών χωρίς εξουσιοδότηση στα συστήματα του πλοίου. Οι θήρες ΟΤ για πρόσβαση σε αυτές τις συσκευές ξεμπλοκάρονται μόνο για επιχειρησιακούς σκοπούς

και αυτό γίνεται λίγο πριν από κάθε είδος εργασίας. Η μεταφορά δεδομένων πραγματοποιείται μόνο μέσω ενός υπολογιστή για επισκέπτες και ελέγχεται αυστηρά και η φόρτιση φορητών συσκευών μέσω USB θήρας απαγορεύεται. Κάθε πλοίο διαθέτει συγκεκριμένο αριθμό εξουσιοδοτούμενων μέσων τα οποία ορίζονται από τον υπεύθυνο ασφάλειας της εταιρείας καθώς ορίζεται και ποιος θα έχει δικαιώματα πρόσβασης σε αυτά (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Ασφάλεια ηλεκτρονικού ταχυδρομείου:** Το e-mail του πλοίου θα πρέπει να χρησιμοποιείται αποκλειστικά και μόνο για επιχειρησιακούς σκοπούς της εταιρείας και η προσωπική χρήση απαγορεύεται ρητά. Υπεύθυνος για τη σωστή χρήση του ηλεκτρονικού ταχυδρομείου είναι ο πλοίαρχος και η χρήση του θα πρέπει να ακολουθεί τους κανόνες ασφαλείας της εταιρείας (Kimberly Tam, Kevin Jones, 2019).

• **Αποδεκτή χρήση Internet:** Η χρήση του διαδικτύου στο πλοίο είναι περιορισμένη και αυτό γίνεται ώστε να μην επηρεάζεται η ασφαλή λειτουργία του σκάφους και να παρέχεται ασφάλεια πληροφοριών. Ο κατάλογος των επιτρεπόμενων σελίδων εξετάζεται ετησίως από τον υπεύθυνο για την ασφάλεια στον κυβερνοχώρο της εταιρείας. Το πλήρωμα μπορεί να χρησιμοποιεί το Internet μόνο από προσωπικές συσκευές με τη σύνδεση στο δίκτυο πληρώματος που παρέχεται στο πλοίο. Το ακατάλληλο περιεχόμενο επίσης ελέγχεται μέσω firewall στο δίκτυο πληρώματος. Τέλος, στο πλήρωμα απαγορεύεται να παρακάμπτει τους κανόνες ασφαλείας ώστε να τίθεται σε κίνδυνο η εταιρεία και η πρόσβαση μπορεί να παρακολουθείται σε περιπτώσεις που η εταιρεία κρίνει ότι υπόκειται σε κίνδυνο (BIMCO, 2018).

• **Απάντηση περιστατικού και σχέδιο αποκατάστασης:** Τα περιστατικά που παρουσιάζονται ενδέχεται να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος του σκάφους. Για αυτό το λόγο τα περιστατικά κατηγοριοποιούνται ως εξής:

1. Άρνηση παροχής υπηρεσίας.
2. Κακόβουλος κώδικας.
3. Μη εξουσιοδοτημένη πρόσβαση.
4. Ακατάλληλη χρήση.

Όπως και στο γραφείο έτσι και για το πλοίο έχουμε αναφορικά κάποια συμπτώματα ασφαλείας τα οποία μπορούν να επηρεάσουν την ομαλή λειτουργία του σκάφους. Αυτά περιλαμβάνουν την δυσλειτουργία του συστήματος υλικού ή λογισμικού, κάποιος ιός ο οποίος δεν ενημερώνεται σε σταθμούς λειτουργίας, όταν δεν λειτουργούν οι κωδικοί πρόσβασης, άνοιγμα ύποπτων συνημμένων, εκτέλεση άγνωστων προγραμμάτων, κατεστραμμένα αρχεία, σφάλματα σταθμών εργασίας κ.α.
Θα μπορούσαν να συμπεριληφθούν και άλλα πολλά όμως αυτό αποσκοπεί στο επίπεδο συνειδητοποίησης και όσα αναφέρονται παραπάνω αποτελούν ένα μικρό παράδειγμα. Όταν δεν υπάρχει βεβαιότητα για κάποιο περιστατικό, αυτό αντιμετωπίζεται ως πραγματικό και σε κάθε περίπτωση θα πρέπει ο πλοίαρχος να επικοινωνεί με τον υπεύθυνο ασφαλείας της εταιρείας (Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 2017).

• **Φυσική ασφάλεια:** Ο κρίσιμος εξοπλισμός του σκάφους θα πρέπει να προστατεύεται από τυχόν φυσικές καταστροφές ή απροσεξία του πληρώματος. Τα συστήματα δεν πρέπει ποτέ να παραμένουν χωρίς επίβλεψη και το πλήρωμα θα πρέπει να μην καπνίζει και να μην τρώει σε αυτές τις κρίσιμες περιοχές. Τα συστήματα UPS θα πρέπει να είναι σε θέση να προστατεύουν τα συστήματα σε περιπτώσεις διακοπής ρεύματος. Σχετικά με τους επισκέπτες υπάρχει ειδικό δίκτυο γι αυτούς επί του σκάφους και δεν επιτρέπεται

η πρόσβασή τους οπουδήποτε θέτει σε κίνδυνο το σκάφος και κατ' επέκταση τη εταιρεία. Τυχόν επιδιορθώσεις του συστήματος θα πραγματοποιούνται μόνο από εξουσιοδοτημένο προσωπικό (Huge Boyes, 2014).

• **Επίγνωση και εκπαίδευση:** Το σημείο αυτό αφορά την ευαισθητοποίηση και την εκπαίδευση του πληρώματος σε σχέση με το Cyber Security. Όπως και στο γραφείο έτσι και στο πλοίο δίνονται κάποιες βασικές οδηγίες σχετικά με τη χρήση αλλά και με τη συμπεριφορά του πληρώματος ώστε να διασφαλίζονται οι πληροφορίες της εταιρείας και τα περιουσιακά της στοιχεία από κακόβουλους χρήστες (Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respico, 2018).

• **Αρχεία:** Όπως και στο γραφείο θα πρέπει και στο πλοίο για τα αρχεία να διατηρείται μητρώο πρόσβασης και να ελέγχονται τα δικαιώματα των χρηστών που έχουν πρόσβαση σε αυτά. Τέλος να εφαρμόζεται δοκιμή δημιουργίας αντιγράφων ασφαλείας (BIMCO, 2018).

8. Συμπεράσματα

Στα πλαίσια της διαχείρισης της ασφάλειας του θαλάσσιου περιβάλλοντος και της ναυτιλιακής ιδιοκτησίας ο IMO έδωσε διορία στην αγορά της ναυτιλίας, να ενσωματώσει πρακτικές κυβερνοασφάλειας, εντός των συστημάτων ασφαλείας των πλοίων.

Εν συνεχεία η MSC (Επιτροπή Ναυτικής Ασφάλειας) πρακτικά ενέκρινε τις απαιτήσεις του Κώδικα ISM, μέσω του ψηφίσματος MSC.428 (98), καθιστώντας τον στόχο ακόμη πιο δομημένο. Στην πράξη πλοιοκτήτες και εφοπλιστές θα πρέπει να έχουν διασφαλίσει ότι μπορούν να διαχειριστούν το ρίσκο και την ασφάλεια των συστημάτων που διαλειτουργούν σε επίπεδο πληροφορίας, μέσω των συστημάτων ασφαλείας τους, το αργότερο έως την πρώτη ετήσια αναθεώρηση του Document of Compliance που ακολουθεί την 01/01/2021.

Την περίοδο που διανύουμε το Cyber Safety και το Risk Management αποτελούν ήδη μέρος ελέγχου από Oil Majors (TMSA v.3, Element 13) και σύντομα τέτοιες πρακτικές θα υιοθετηθούν ως υποχρεωτικές απαιτήσεις ελέγχου, καλύπτοντας τις ακόλουθες κατηγορίες πλοίων:

- Επιβατηγά πλοία, συμπεριλαμβανομένων των επιβατικών μεταφορών υψηλής ταχύτητας.
- Πετρελαιοφόρα, χημικά δεξαμενόπλοια, πλοία μεταφοράς αερίου, πλοία χύδην φορτίου και μεταφορικά μέσα 500 GRT και άνω.
- Άλλα φορτηγά πλοία και κινητές μονάδες γεώτρησης ανοικτής θάλασσας 500 GRT και άνω.

Σε αυτό το σημείο θα πρέπει να γίνει μια ειδική αναφορά, καθώς ο Κώδικας ISM αναφέρεται σε Cyber Safety και Cyber Risk Management. Πάραυτα, η αγορά πληροφορικής δείχνει να έχει παρερμηνεύσει τις επιταγές του Κώδικα ISM, δίνοντας έμφαση στο Cyber Security .

Ξεκαθαρίζοντας λίγο περισσότερο τα πράγματα αναφέρεται πως το Cyber Safety αφορά στην ικανότητα ενός οργανισμού να ενεργεί με ασφάλεια και υπευθυνότητα σε επίπεδο διαλειτουργικότητας συστημάτων που διαχειρίζονται ψηφιακή πληροφορία.

Επιπλέον το Cyber Risk Management αφορά στη διαχείριση του εντοπισμένου κινδύνου από την άποψη της πιθανότητας εμφάνισης του σε σχέση με μια αρχιτεκτονική, ενώ παράλληλα καταβάλει συντονισμένες προσπάθειες για την ελαχιστοποίηση, την παρακολούθηση και τον έλεγχο των επιπτώσεων.

Τέλος, ξεκαθαρίζεται οριστικά πως το Cyber Security είναι μέρος του Safety & Risk Management καθώς αφορά στις τεχνικές και τεχνολογίες προστασίας υπολογιστικών συστημάτων, δικτύων και δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή επιθέσεις που αποσκοπούν στην εκμετάλλευσή τους. Πρέπει να γίνει αντιληπτό πως σε ένα πληροφοριακό οικοσύστημα το οποίο βρίσκεται στη θάλασσα, δεν αρκεί το CIA που συναντούμε σε shore-side επίπεδο. Οι υποδομές και διαδικασίες ελέγχου που πλέον απαιτούνται σε ένα πλοίο επεκτείνουν το CIA σε Confidentiality, Integrity, Availability, Reliability, Auditability και Security, για τα συστήματα που διαλειτουργούν και τη πληροφορία που συναλλάσουν μέσω υποδομών IT.

Από την άλλη πλευρά δε φαίνεται η διοίκηση της αγοράς της ναυτιλίας να έχει καταλάβει ουσιαστικά τι σημαίνει αυτό το ορόσημο. Για αρχή ο ρόλος του IT management αλλάζει οριστικά. Για τη Ναυτιλιακή βιομηχανία η έννοια ασφάλεια είναι ισοδύναμη της έννοιας ποιότητα. Ως συνέπεια αυτού, το IT αποκτά ουσιαστική θέση στην αλυσίδα αξίας των Ναυτιλιακών Επιχειρήσεων. Στην πράξη, από το 2021 και μετά, η μη συμμόρφωση θα επηρεάσει την ποιότητα των Ναυτιλιακών επιχειρήσεων, από το HSQE μέχρι το Operations, και σε βάθος χρόνου ακόμη και το Chartering. Εφόσον πρακτικά ο ρόλος του IT αλλάζει σε μια Ναυτιλιακή Επιχείρηση, είναι αναμενόμενο η ευθύνη περί συμμόρφωσης και μετασχηματισμού να ξεκινήσει από τα τμήματα IT. Ένας IT manager Ναυτιλιακής καλείται να επαναπροσδιορίσει τον ρόλο του και να συμπεριφερθεί όπως οι υπόλοιποι managers που συμμετέχουν ενεργά στην αλυσίδα αξίας. Ο IT manager πρέπει να καθορίσει τους στόχους του με ποσοτικό και ποιοτικό τρόπο, ορίζοντας KPIs που μπορούν να διατηρηθούν στο διηνεκές, συμβάλλοντας σε ένα υγιές SMS.

Μία τυπική λίστα σημείων ελέγχου αντικατοπτρίζοντας πλήρως τις επιταγές του ISM Κώδικα, έχει ήδη δώσει το IMCA. Συγκεκριμένα απαιτείται:

- Inventory of Authorized and Unauthorized Devices Actively Managed
- Inventory of Authorized and Unauthorized Software Actively Managed
- Secure Configurations for HW and SW on Workstations and Servers
- Malware Defenses & Boundary Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Secure Configurations for Network Devices
- Limitation and Control of Access to Network Ports
- Maintenance, Monitoring and Analysis of Audit Logs
- Control the Use of Administrative Privileges
- Control Access Based on Need to Know
- Account Monitoring and Control
- Data Protection
- Incident Response and Management

- Secure Network Engineering
- Security Skills Assessment & Training
- Continuous Vulnerability Assessment and Remediation
- Red Team Exercises

Συνεπώς για να επιτύχει ένας IT Manager τα ανωτέρω διατηρώντας υψηλά επίπεδα Confidentiality, Integrity, Availability, Reliability, Auditability και Security θα χρειαστεί να επαναπροσδιορίσει τα IT περιβάλλοντα των πλοίων στις παρακάτω διαχειριστικές κατευθύνσεις.

- Homogeneity in Architecture, Assets & Policies Management
- ICT Standardization and Governance
- ICT Hygiene vs Threat Vectors (Threat Intelligence)
- Systems State & Security Continuous Monitoring
- Live Systems & Software Update/Configuration Management
- Systems, Applications and Software Test Environments Prior Deployment
- Change Controls and Methods for Systems and Software
- Live Data & ICT Protection
- Disaster Recovery in Place and Always Active
- Identity Governance and Management
- Risk & Vulnerability Assessment
- Live Camera Auditing for Incident Response
- Minimization of Service Attendances Needed
- 24/7 Systems Visibility and Proactive Response Practices
- Concurrent IT and Comms Management
- Processes on USB Logical and Physical Controls
- Seamless Ship-Shore Collaboration

Βλέποντας πλέον τον όγκο των υπηρεσιών που απαιτούνται σε συνάρτηση με τις υποδομές, είναι λογικό να αντιληφθούμε ότι τυπικά, μια ναυτιλιακή εταιρεία χρειάζεται αρκετούς υπαλλήλους να απασχολούνται αποκλειστικά με την πληροφορική των πλοίων, κάτι το οποίο επιχειρησιακά είναι πολύ πιθανό να μην ασπαστεί η διοίκηση.

Ένας IT Manager θα πρέπει να μετρήσει τις δυνατότητές του και της ομάδας του, σχετικά με την διαχείριση των νέων απαιτήσεων, και ως εκ τούτου να παρουσιάζει επιχειρησιακή ευελιξία, παρέχοντας παράλληλα ένα βέλτιστο και ομοιογενές επιχειρησιακό αποτέλεσμα προς την εταιρεία.

Εφόσον έχει εντοπιστεί τι μπορεί και τι δε μπορεί να υποστηρίξει μια Ναυτιλιακή Επιχείρηση σε επίπεδο στόλου, θα πρέπει διαχειριστικά να καλύψει τις απαιτήσεις αναζητώντας υποστήριξη και συνεχή μεταφορά τεχνογνωσίας από την αγορά.

Μια ομάδα με τις παρακάτω αξίες, παρουσιάζοντας επιχειρησιακά Shared Resource & Selective Outsourcing μοντέλο παροχής υπηρεσιών, με εμπειρία σε εν πλω συστήματα, δύναται να ενισχύσει on demand τον IT Manager στα σημεία όπου παρουσιάζει αδυναμίες. Ενδεικτικά χαρακτηριστικά είναι τα κάτωθι:

- Team Reputation & No Customer Dropouts
- Flexible and Real Financial Tools for Customers
- Tailored Contractual Responsibilities
- Tailored Customer Experience
- ITIL Oriented Support Center & Live 24/7 Reports

- ❖ Combined IT & SatComms Engineering Expertise
- ❖ Prince2 Framework on Projects Implementation
- ❖ Continuous Know-how Transfer
- ❖ Compliance Guidance & Reporting
- ❖ IT - HSQE Interfacing Guidance
- ❖ Direct Support to Vessel Team
- ❖ Training Support to Customer

Έχοντας ερμηνεύσει ακριβώς το στόχο του Κώδικα ISM στην κατεύθυνση του Cyber Management και Risk Assessment, είναι πλέον ξεκάθαρο πως πρακτικά η συμμόρφωση αποτελεί μια προσεκτική απόφαση σε επίπεδο management, και αφορά στην προσεκτική επιλογή εξειδικευμένων συνεργατών, καθώς ελάχιστοι μπορούν να εγγυηθούν την απρόσκοπτη, αδιάλειπτη και μη διαβλητή λειτουργία ενός ολοκληρωμένου πληροφοριακού οικοσυστήματος το οποίο βρίσκεται ανοικτά της θάλασσας, χωρίς να υπάρχει φυσική δυνατότητα παρέμβασης.

.

Αναφορές

1. TMSA 3 - TMSA 3- “MARITIME SECURITY – ELEMENT 13” VERSION 2017
2. VIQ version 7.0.05, 2019
3. BIMCO - ICS CS ON BOARD SHIPS
4. IMO – “ISM Code and Guidelines on Implementation of the ISM Code” http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
5. IMO – “Maritime cyber risk” - MSC-FAL.1/Circ.3, 5 July 2017 http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security
6. INTERNATIONAL STANDARD ISO/IEC 27001:2016 4th edition 2016-02-15 http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27000-2016-english.pdf
7. IACS - “Recommendations on Cyber Safety Mark Step change of Cyber Security resilient”, http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-stepchange-in-delivery-of-cyber-resilient-ships/
8. IMO No:9288447 Cyber Security Management Plan. DNVGL
9. CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES – ABS
10. CYBER SECURITY SOLUTIONS FOR INDUSTRY – BUREAU VERITAS
11. Cyber security resilience management for ships and mobile offshore units in operation – DNVGL, September 2016
12. Cyber security Advanced Solution – ABS.