ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΝΑΥΠΗΓΩΝ ΜΗΧΑΝΙΚΩΝ

Πτυχιακή εργασία

Κυβερνοασφάλεια στη Ναυτιλία, Νομοθεσία και Βέλτιστες Πρακτικές

Maritime Cybersecurity, Legislation and Best Practices

Συγγραφείς:

Ανδρέου Λουκάς

Α.Μ.: 17021

Γιακουμάκης Ιωάννης

Α.Μ.: 17109

Επιβλέπων: Δρ. Σέρρης Μιχαήλ

Αιγάλεω, 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΝΑΥΠΗΓΩΝ ΜΗΧΑΝΙΚΩΝ

Πτυχιακή εργασία

Τίτλος: Κυβερνοασφάλεια στη Ναυτιλία, Νομοθεσία και Βέλτιστες Πρακτικές

Συγγραφείς

Ανδρέου Λουκάς 17021

Γιακουμάκης Ιωάννης 17109

Επιβλέπων

SERRIS MICHAIL
Digitally signed by SERRIS MICHAIL
Date: 2021.08.28 09:32:57 +03'00'

Ονοματεπώνυμο,

Δρ. Σέρρης Μιχαήλ, Λέκτορας ΠΑ.Δ.Α.

Ημερομηνία εξέτασης

24/06/2021

Εξεταστική Επιτροπή

Sotiria Dimitrellou
Digitally signed by Sotiria Dimitrellou
Date: 2021.06.30 13:30:51 +03'00'

Ονοματεπώνυμο,

Δρ. Δημητρέλλου Σωτηρία
Αναπληρώτρια Καθηγήτρια ΠΑ.Δ.Α.

Dimitrios Nikolaos Pagonis
Digitally signed by Dimitrios Nikolaos Pagonis
DN: c=GR, o=University of West Attica, ou=Class A - Private Key created and stored in hardware CSP, sn=Pagonis, givenName=Nikolaos, givenName=Dimitrios, serialNumber=3318122797, cn=Dimitrios Nikolaos Pagonis, email=d.n.pagonis@uniwa.gr
Date: 2021.06.30 12:48:18 +03'00'

Ονοματεπώνυμο,

Δρ. Παγώνης Δημήτριος - Νικόλαος
Αναπληρωτής Καθηγητής ΠΑ.Δ.Α.

SERRIS MICHAIL
Digitally signed by SERRIS MICHAIL
Date: 2021.08.28 09:33:58 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΩΝ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Οι κάτωθι υπογεγραμμένοι Γιακουμάκης Ιωάννης του Γεωργίου, με αριθμό μητρώου 17109 και Ανδρέου Λουκάς του Γεωργίου με αριθμό μητρώου 17021 φοιτητές του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Ναυπηγών Μηχανικών, δηλώνουμε υπεύθυνα ότι:

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

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

Οι Δηλούντες

Ανδρέου Λουκάς Γιακουμάκης Ιωάννης

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε τις οικογένειές μας για την υπομονή που έδειξαν σε αυτό το δύσκολο εγχείρημα και κατά το διάστημα εκπόνησης της παρούσας Πτυχιακής. Επίσης να ευχαριστήσουμε τον κ. Αθανάσιο Βόσβολη, Διευθυντή του τμήματος Εκπαίδευσης του Αμερικάνικου Νηογνώμονα για τις πολύτιμες συμβουλές του και το υποστηρικτικό υλικό που μας διέθεσε, καθώς και τον Πλοίαρχο Λ.Σ. Πουλημένο Ιωάννη Διευθυντή Διεύθυνσης Επιχειρήσεων Λ.Σ. Ε.Λ-ΑΚΤ καθώς δίχως την πολύτιμη βοήθειά του δεν θα ήταν εφικτή η ολοκλήρωση του εγχειρήματος αυτού.

Επίσης να ευχαριστήσουμε τον επιβλέποντα καθηγητή κ. Σέρρη Μιχαήλ καθώς και τα μέλη της Εξεταστικής Επιτροπής για την συμμετοχή τους,

ΠΕΡΙΛΗΨΗ

Εν έτει 2020 όπου κυριαρχεί η ηλεκτρονική πληροφόρηση και ανταλλαγή δεδομένων μέσω του διαδικτύου, αυξάνεται και η ανάγκη για την ασφάλεια των δεδομένων αυτών. Η ναυτιλία φυσικά δεν θα μπορούσε να μείνει έξω από αυτή την τεχνολογική εξέλιξη, καθώς σημαντικό μέρος των διαδικασιών διαχείρισης και παρακολούθησης ενός πλοίου και του φορτίου του, γίνεται πλέον μέσω του διαδικτύου. Αυτό βέβαια έχει σαν αποτέλεσμα το πλοίο ή η ναυτιλιακή εταιρία να είναι πιο ευάλωτοι σε ένα κίνδυνο κυβερνοεπίθεσης. Καθώς η τεχνολογία εξελίσσεται ολοένα και με πιο γρήγορους ρυθμούς είναι σχεδόν αδύνατο τα συστήματα ασφαλείας και προστασίας δεδομένων να είναι συνεχώς ενημερωμένα, καθώς νέα είδη απειλών ανακαλύπτονται και εφαρμόζονται σε καθημερινή βάση. Στην παρούσα πτυχιακή εργασία θα αναφέρουμε το θεσμικό πλαίσιο που διέπει ως σήμερα την κυβερνοασφάλεια των πλοίων, καθώς και τις βέλτιστες πρακτικές που μπορούν να εφαρμοστούν για την αποφυγή μιας ενδεχόμενης κυβερνοεπίθεσης.

Λέξεις κλειδιά: Κυβερνοεπίθεση, κυβερνοασφάλεια στη ναυτιλία, προστασία δεδομένων, συστήματα ασφαλείας, βέλτιστες πρακτικές κυβερνοασφάλειας, απειλές, προστασία δεδομένων, ασφάλεια δεδομένων, ασφάλεια πληροφοριών, διαχείριση κινδύνου, αξιολόγηση κινδύνου, εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, συστήματα ασφαλείας, σύστημα διαχείρισης της ασφάλειας, πρότυπα διαχείρισης της ασφάλειας, κυβερνοασφάλεια.

ABSTRACT

In 2020, while electronic information and data exchange over the internet dominates, the need for the security of such data is also increasing. Shipping, of course, could not be left out of this technological development, as an important part of the management and monitoring processes of a ship and its cargo, is now done via the internet. This, of course, means that the ship or shipping company is more vulnerable to a cyber-attack. As technology evolves faster and faster, it is almost impossible for security and data protection systems to be constantly up to date, as new types of threats are discovered and implemented on a daily basis. In this graduate work we will mention the institutional framework that has so far governing ship's cybersecurity, as well as best practices that can be applied to prevent a possible cyber-attack.

Keywords: Cyber-attack, maritime cybersecurity, data protection, security systems, best practices in cybersecurity, threats, data security, information security, risk management, risk assessment, confidentiality, integrity, availability, security systems, security management system, safety management standards, cyber security.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

ΠΙΝΑΚΑΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΠΙΝΑΚΑΣ ΑΚΡΩΝΥΜΙΩΝ

Συντμήσεις	*Περιγραφή*
AIS	*automatic identification system*
OAuth	open standard for authorization, commonly used as a way for internet users to log in to third party websites using their Google, Facebook, Microsoft, Twitter, One Network, etc.
BIMCO	Baltic and International Maritime Council
CCTV	closed circuit television
CS	Cyber security
CIAA	confidentiality, integrity, availability & authenticity
CSET	cyber security evaluation tool
DCS	distributed control system
DDoS	distributed denial of service (attack)
DNS	domain name system
DoS	denial of service (attack)
DP	dynamic positioning
GS	Grundschutz (German): basic protection
GPS	global positioning system
IMO	International Maritime Organization
ISDS	integrated software dependent systems
IP	internet protocol
IPS	intrusion prevention system
ISM Code	International Safety Management Code (i.e. SOLAS Chapter IX)
ISMS	information security management system
ISO	International Organization for Standardization
ISPS Code	International Ship and Port facility Security Code
IT	information technology
KPI	key performance indicator
LAN	local area network
MSC	(IMO) Maritime Safety Committee
N/A	not applicable
OT	operational technology
PA	public address
PC	personal computer
PDCA	plan-do-check-act
PMS	planned maintenance system
QR	quick response (code)
RP	recommended practice
SCADA	supervisory control and data acquisition
SR	security requirement
USB	universal serial bus
VDR	voyage data recorder
VLAN	virtual local area network
VoIP	voice over IP

VPN	virtual private network
WLAN	wireless local area network

1 ΕΙΣΑΓΩΓΗ

Μετά την 25η Μαΐου 2018 όπου ξεκίνησε να εφαρμόζεται ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) ,η ασφάλεια στον κυβερνοχώρο έχει καταστεί ακόμη πιο σημαντική για όλους τους επιχειρηματικούς τομείς, συμπεριλαμβανομένης και της ναυτιλίας. Πολλές βιομηχανίες ανησυχούν για παραβιάσεις δεδομένων, που πολλές φορές επιφέρουν αυστηρά πρόστιμα. Εκτός από τις ανησυχίες παραβίασης δεδομένων, ένα κενό ασφάλειας στον κυβερνοχώρο θα μπορούσε να θέσει σε κίνδυνο τις επιχειρηματικές δραστηριότητες καθώς και τα άτομα που ασχολούνται με τη ναυτιλία.

Για να κατανοήσουμε λίγο καλύτερα πόσο έχει εισχωρήσει το Internet στην ζωή μας, αρκεί να ρίξουμε μια ματιά στο πως αλληλοεπιδράμε στην καθημερινότητά μας αλλά και στον τρόπο που εργαζόμαστε. Τι πιο χαρακτηριστικό παράδειγμα από το πρόσφατο lockdown που προκλήθηκε από την πανδημία του Covid-19. Εκεί που για ένα μεγάλο μέρος του πληθυσμού το Internet ήταν απλά ένα μέσο επικοινωνίας και ψυχαγωγίας, εν μια νυκτί έγινε ένα χρήσιμο και συνάμα απαραίτητο εργαλείο το οποίο παρείχε πρωτίστως ασφάλεια στην μη εξάπλωση και μετάδοση του ιού, τηλεκπαίδευση για χιλιάδες μαθητές και φοιτητές όλων των βαθμίδων, και τηλεργασία για εκατομμύρια πολίτες. Μέσω τηλεδιασκέψεων και αποδοτικής εργασίας από το σπίτι, το σύνολο των επιχειρήσεων κατάφεραν να κρατηθούν όρθιες και να συντηρήσουν την αγορά εργασίας. Αυτό βέβαια απαιτεί την αναβάθμιση των ψηφιακών υποδομών των κρατών ως συνέπεια του τεράστιου όγκου δεδομένων τα οποία διακινούνται καθημερινώς, και ταυτόχρονα την ανάγκη προστασίας των δεδομένων αυτών.

Η προστασία των δεδομένων αυτών δεν είναι πρωτόγνωρο πρόβλημα. Καθώς οδεύουμε προς την Βιομηχανία 4.0 (Industry 4.0 – Τέταρτη Βιομηχανική Επανάσταση), υποστηριζόμενη από τα ασύρματα συστήματα 5ης γενιάς (5G), η οποία διέπεται από την ανταλλαγή δεδομένων και την αυτοματοποίηση στην τεχνολογία παραγωγής, εντοπίζονται καθημερινά περιστατικά παραβίασης των προσωπικών δεδομένων καθώς και των πληροφοριών. Ειδικά δε στον τομέα της ναυτιλίας, οι πληροφορίες οι οποίες μπορεί να διαρρεύσουν επηρεάζουν ζωτικά σημεία του πλοίου καθώς και της ναυτιλιακής εταιρίας. Όλα αυτά δείχνουν τον δρόμο προς την εξεύρεση λύσεων και βέλτιστων πρακτικών ειδικά στον ναυτιλιακό τομέα όπου πέρα των συνηθισμένων κανονισμών που εφαρμόζονται στους υπόλοιπους τομείς της βιομηχανίας, εφαρμόζονται επιπλέον κανονισμοί και πρακτικές τις οποίες θα αναφέρουμε και θα αναλύσουμε παρακάτω.

Ο κίνδυνος στον κυβερνοχώρο στον κλάδο της ναυτιλίας (Maritime Cyber Risk) ορίζεται ως η απειλή που μπορεί να δεχτεί ένας όγκος δεδομένων ή ακόμα και οι ηλεκτρονικές συσκευές, από μια κυβερνοεπίθεση, η οποία μπορεί να οδηγήσει σε βλάβες που σχετίζονται με την ακεραιότητα του πλοίου, την απώλεια-διαρροή ευαίσθητων δεδομένων σχετικά με το εμπόρευμα του πλοίου, το δρομολόγιό του, την ασφάλεια ναυσιπλοΐας ή και την απώλεια προσωπικών δεδομένων του πληρώματός του.

Στην παρούσα μελέτη θα εξετάσουμε, σε όσο το δυνατό αναλυτικό βαθμό, τα θέματα νομοθεσίας και βέλτιστων πρακτικών που αφορούν την ασφάλεια στον Κυβερνοχώρο στον τομέα της ναυτιλίας.

2 ΟΡΙΣΜΟΙ

Για να μπορέσουμε να κατανοήσουμε επακριβώς την απειλή στον κυβερνοχώρο θα πρέπει πρώτα να εξηγήσουμε τους ορισμούς οι οποίοι θα μας απασχολήσουν σε αυτή την εργασία αλλά και στο εγγύς μέλλον της καθημερινότητάς μας. Γενικότερα ο κίνδυνος στον κυβερνοχώρο ορίζεται ως τον λειτουργικό κίνδυνο των IT και OT συστημάτων, με συνέπεια να επηρεάζεται η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα των πληροφοριακών αυτών συστημάτων. (Cebula and Young, 2010) .

2.1 Θαλάσσιος Κίνδυνος Στον Κυβερνοχώρο (Maritime Cyber Risk)

Ο θαλάσσιος κίνδυνος στον κυβερνοχώρο (Maritime Cyber Risk) είναι η περίπτωση κατά την οποία ένα περιουσιακό τεχνολογικό στοιχείο ,μπορεί να απειληθεί, και θα έχει ως συνέπεια πιθανές δυσλειτουργίες στον τομέα της ναυτιλίας, στην ασφάλεια ή στην ασφάλεια ως συνέπεια της διαφθοράς, απώλειας ή παραβίασης πληροφοριών ή συστημάτων. (www.imo.org).

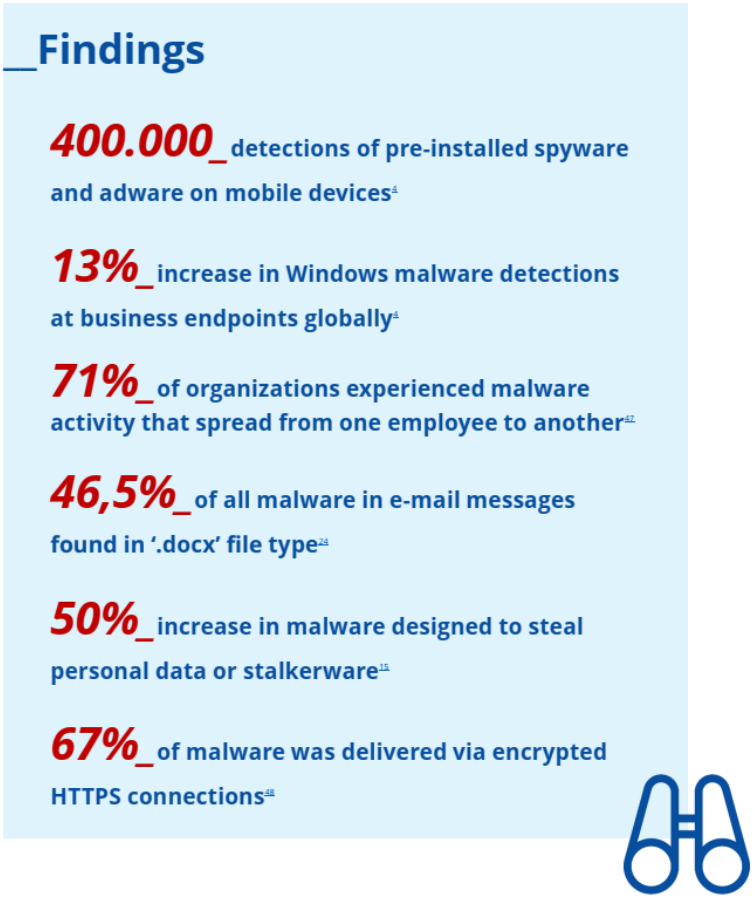
2.2 Διαχείριση Κίνδυνων Στον Κυβερνοχώρο (Cyber Risk Management)

Ως διαχείριση κινδύνων στον κυβερνοχώρο νοείται η διεργασία κατά την οποία γίνεται προσδιορισμός, ανάλυση, αξιολόγηση και κοινοποίηση μιας διαδικτυακής απειλής και στη συνέχεια ακολουθεί η αποδοχή, ή αποφυγή, ή μεταφοράς ή μείωσής του σε επίπεδο όπου αυτό θεωρείται αποδεκτό, βάσει του κόστους και των οφελών από τις δράσεις που αναλαμβάνουν οι διαχειριστές ή οι πλοιοκτήτες. (www.imo.org).

2.3 Κακόβουλο Λογισμικό (Malware)

Το κακόβουλο λογισμικό είναι ένας κοινός τύπος κυβερνοεπίθεσης με τη μορφή λογισμικού. Οι οικογένειες του κακόβουλου λογισμικού περιλαμβάνουν cryptominers, ιούς, ransomware, worms και spyware. Κοινοί στόχοι τους είναι η κλοπή πληροφοριών ή ταυτότητας, η κατασκοπεία και η διακοπή κάποιας υπηρεσίας.

Τα πρωτόκολλα διαδικτύου (Web Protocols) και ηλεκτρονικού ταχυδρομείου (e-mail Protocols) είναι οι πιο συνήθεις φορείς επίθεσης που χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού. Ωστόσο, με την εκμετάλλευση τρωτών σημείων ενός συστήματος, ορισμένες οικογένειες κακόβουλου λογισμικού είναι σε θέση να εξαπλωθούν ακόμη περισσότερο μέσα σε ένα δίκτυο ηλεκτρονικών υπολογιστών.



Σχήμα 2.1 Στατιστικά επιθέσεων έτους 2019 μέσω Malware.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.4 Διαδικτυακές Επιθέσεις (Web-Based Attacks)

Οι διαδικτυακές επιθέσεις είναι μια ελκυστική μέθοδος με την οποία οι παράγοντες απειλής μπορούν να εξαπατούν τα θύματα χρησιμοποιώντας διαδικτυακά συστήματα και υπηρεσίες ως φορέα. Αυτό καλύπτει ένα μεγάλο εύρος επιθέσεων, για παράδειγμα διευκολύνοντας κακόβουλες διευθύνσεις URL (Uniform Resource Locator) ή κακόβουλο κώδικα για να κατευθυνθεί ο χρήστης

ή το θύμα στην επιθυμητή ιστοσελίδα ή τη λήψη κακόβουλου περιεχομένου για οικονομικό κέρδος, κλοπή πληροφοριών ή ακόμη και για εκβιασμό μέσω ransomware.

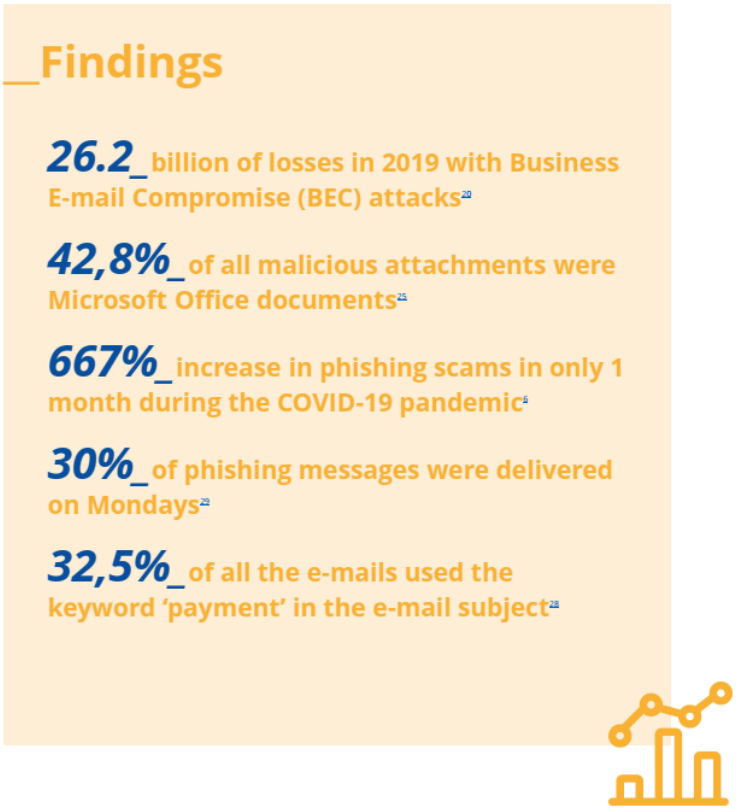
Οι διαδικτυακές επιθέσεις μπορούν να επηρεάσουν τη διαθεσιμότητα ιστοσελίδων, εφαρμογών και διεπαφών προγραμματισμού εφαρμογών (Application Program Interface - API), παραβιάζοντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

2.5 Ηλεκτρονικό Ψάρεμα (Phishing)

Phishing είναι η δόλια προσπάθεια να κλαπούν τα δεδομένα των χρηστών, όπως τα διαπιστευτήρια σύνδεσης, πληροφορίες πιστωτικών καρτών, ή ακόμα και τα χρήματα χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής. Αυτός ο τύπος επίθεσης συνήθως παρουσιάζεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, που φαίνεται να αποστέλλονται από αξιόπιστη πηγή, με σκοπό να πείσει τον χρήστη να ανοίξει κακόβουλο συνημμένο ή να ακολουθήσει μια «κακόβουλη» διεύθυνση URL.

Μία ειδική περίπτωση της κατηγορίας αυτής το «spear phishing» βασίζεται σε εκ των προτέρων έρευνα για τα θύματα, έτσι ώστε η απάτη φαίνεται πιο αυθεντική, καθιστώντας το είδος αυτής της επίθεσης ως ένα από τα πιο επιτυχημένα είδη επίθεσης στα δίκτυα των επιχειρήσεων.

Στο μέλλον, το ηλεκτρονικό ταχυδρομείο συνεχίζει να είναι ο «νούμερο ένα» μηχανισμός για το phishing, αλλά όχι για πολύ. Βλέπουμε ήδη μια αύξηση στη χρήση των κοινωνικών μέσων ενημέρωσης μηνυμάτων, WhatsApp και άλλα που ευνοούν την, μέσω και αυτών, διεξαγωγή επιθέσεων phishing. Η πιο σχετική αλλαγή θα είναι στις μεθόδους που χρησιμοποιούνται για την αποστολή των μηνυμάτων, τα οποία θα γίνουν πιο εξελιγμένα με την υιοθέτηση της Ανταγωνιστικής Τεχνητής Νοημοσύνης (Adversarial Artificial Intelligence) για την προετοιμασία και την αποστολή των μηνυμάτων.



Σχήμα 2.2 Στατιστικά επιθέσεων έτους 2019 μέσω Phishing.

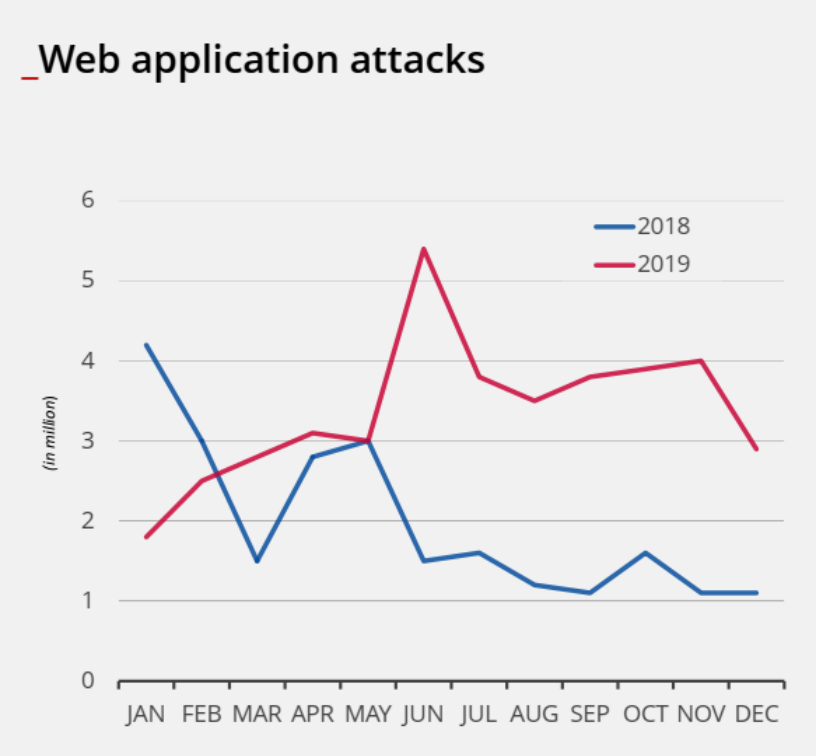
Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.6 Επιθέσεις Διαδικτυακών Εφαρμογών (Web Application Attacks)

Οι διαδικτυακές εφαρμογές και τεχνολογίες έχουν γίνει βασικό μέρος του διαδικτύου υιοθετώντας διαφορετικές χρήσεις και λειτουργίες. Η αύξηση της πολυπλοκότητας των διαδικτυακών εφαρμογών και των ευρέως διαδιδομένων υπηρεσιών τους, δημιουργεί προκλήσεις για την εξασφάλιση τους έναντι απειλών με ποικίλα κίνητρα, όπως οικονομική ζημία ή ζημία φήμης στην κλοπή κρίσιμων ή προσωπικών πληροφοριών.

Οι διαδικτυακές υπηρεσίες και εφαρμογές εξαρτώνται κυρίως από βάσεις δεδομένων για την αποθήκευση ή την παράδοση των απαιτούμενων πληροφοριών. Οι επιθέσεις δέσμης ενεργειών μεταξύ τοποθεσιών (Cross-site Scripting attacks -XSS) είναι ένα παράδειγμα τέτοιας απειλής. Σε αυτόν τον τύπο επίθεσης, ο επιτιθέμενος χρησιμοποιεί τεχνικές για να αποσπάσει κωδικούς πρόσβασης που υπάρχουν σε φόρμες για την είσοδο σε διαδικτυακές εφαρμογές. Έτσι, αυτές

οδηγούν σε άλλες κακόβουλες λειτουργίες, όπως η ανακατεύθυνση σε μια κακόβουλη τοποθεσία του διαδικτύου.



Σχήμα 2.3 Διάγραμμα επιθέσεων διαδικτυακών εφαρμογών 2018-2019.

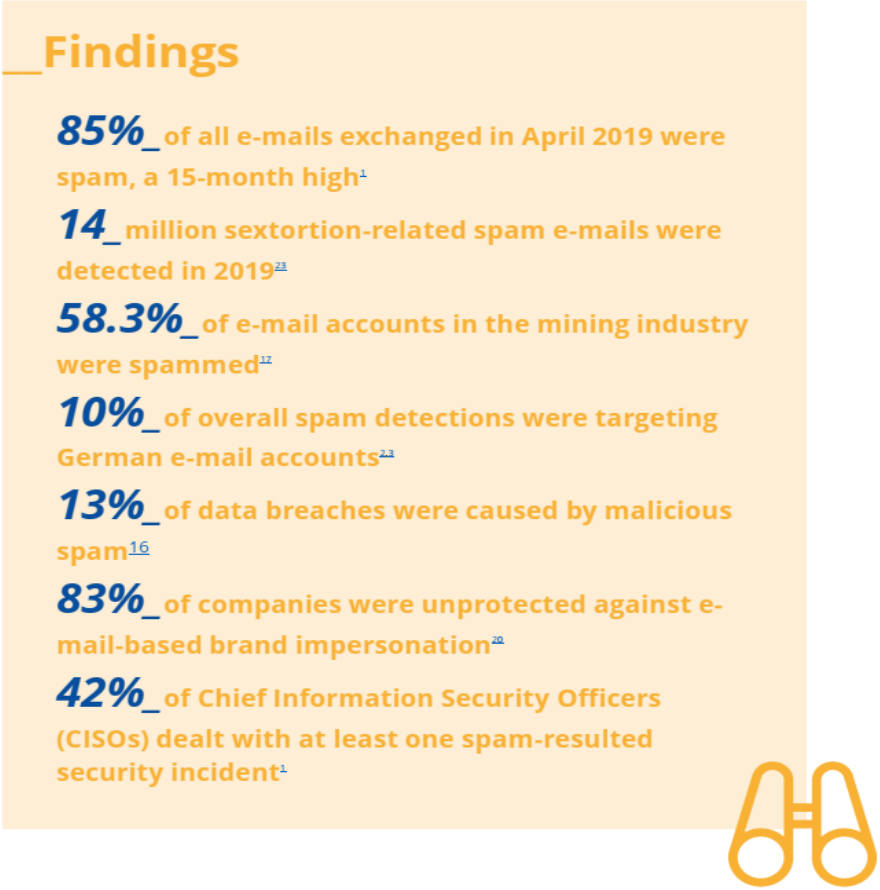
Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.7 Ανεπιθύμητα Μηνύματα (Spam Messages)

Η λήψη ανεπιθύμητων μηνυμάτων είναι μια ενόχληση, αλλά μπορεί επίσης να δημιουργήσει μια ευκαιρία για έναν κακόβουλο παράγοντα να κλέψει προσωπικές πληροφορίες ή να εγκαταστήσει κακόβουλο λογισμικό. Η ανεπιθύμητη αλληλογραφία αποτελείται από την αποστολή αυτόκλητων μηνυμάτων σε μεγάλες ποσότητες. Θεωρείται απειλή για την ασφάλεια στον κυβερνοχώρο όταν χρησιμοποιείται ως φορέας επίθεσης για τη διανομή ή την ενεργοποίηση άλλων απειλών.

Μια άλλη αξιοσημείωτη πτυχή είναι πώς το spam μπορεί μερικές φορές να συγχέεται ή να ταξινομηθεί εσφαλμένα ως phishing. Διαφέρουν στο γεγονός ότι το phishing είναι μια στοχευμένη δράση χρησιμοποιώντας τακτικές κοινωνικής μηχανικής, που αποσκοπεί να κλαπούν τα δεδομένα των χρηστών, ενώ το spam είναι μια τακτική για την αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μια μαζική λίστα. Οι επιθέσεις ηλεκτρονικού "ψαρέματος"

μπορούν να χρησιμοποιήσουν τακτικές ανεπιθύμητης αλληλογραφίας για τη διανομή μηνυμάτων, ενώ τα ανεπιθύμητα μηνύματα μπορούν να συνδέσουν το χρήστη με έναν «επικίνδυνο» ιστότοπο για την εγκατάσταση κακόβουλου λογισμικού και την κλοπή προσωπικών δεδομένων.

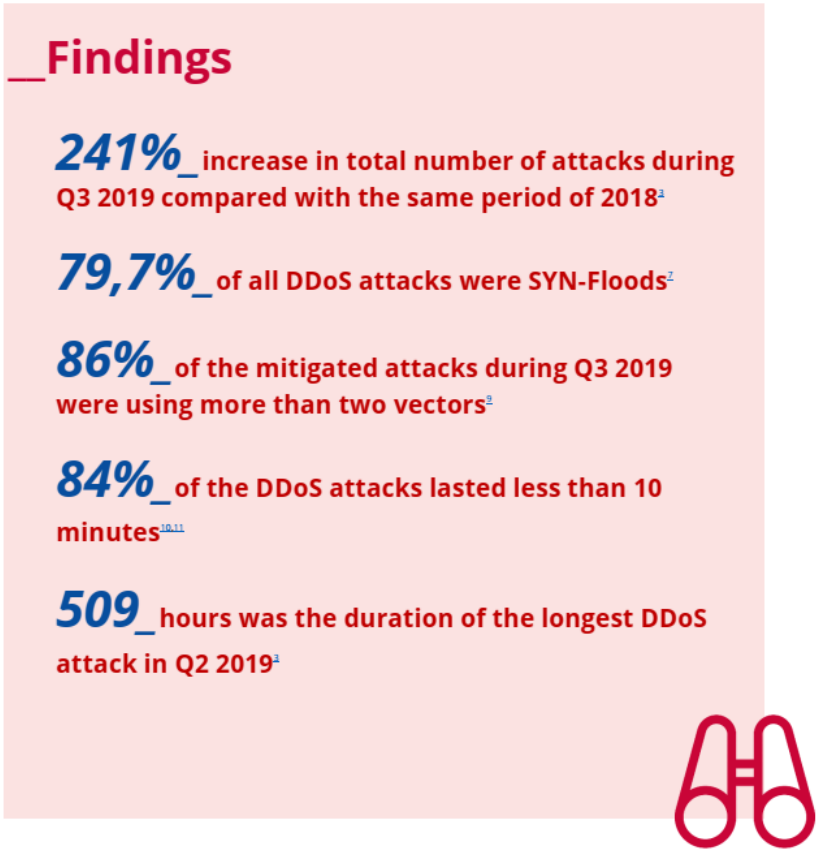


Σχήμα 2.4 Στατιστικά ανεπιθύμητων μηνυμάτων έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.8 Επιθέσεις Κατανεμημένης Άρνησης Υπηρεσίας (Distributed Denial Of Service Ddos)

Οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) είναι γνωστό ότι παρουσιάζονται όταν οι χρήστες ενός συστήματος ή υπηρεσίας δεν έχουν πρόσβαση στις σχετικές πληροφορίες, υπηρεσίες ή άλλους πόρους. Αυτό είναι υλοποιήσιμο εξαντλώντας την υπηρεσία ή υπερφορτώνοντας το δίκτυο. Ιστορικά, οι υπηρεσίες DDoS διαφημίστηκαν στο dark web, αλλά τώρα χρησιμοποιούν τα κοινά κοινωνικά κανάλια μέσων όπως YouTube όπου προωθούν τις υπηρεσίες τους.

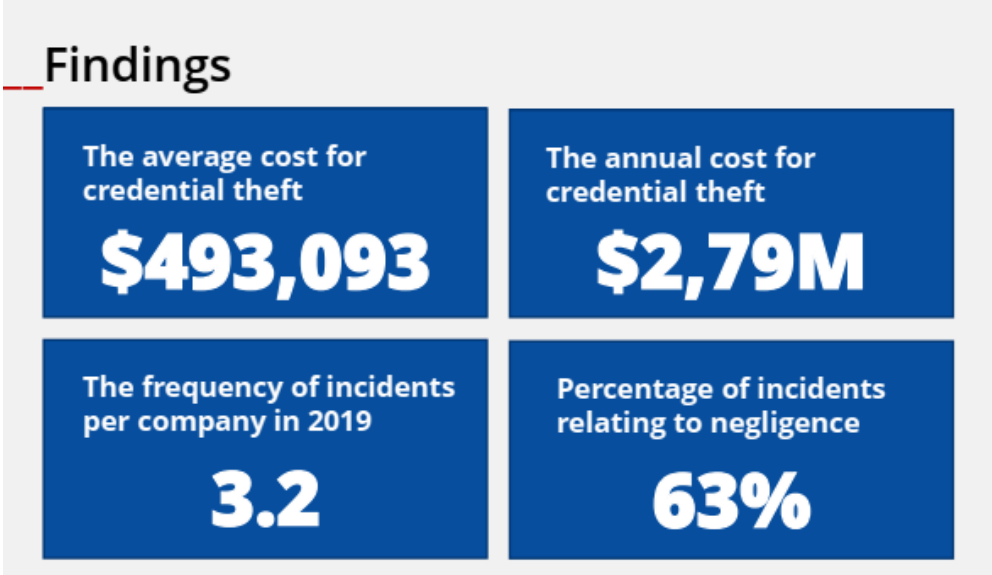


Σχήμα 2.5 Στατιστικά επιθέσεων DDoS έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.9 Κλοπή Ταυτότητας (Identity Theft)

Κλοπή ταυτότητας ή απάτη ταυτοποίησης είναι η παράνομη χρήση των προσωπικών αναγνωρίσιμων πληροφοριών ενός θύματος (Personal Identifiable Information - PII) από έναν απατεώνα, στην προσπάθειά του να μιμηθεί το εν θέματι πρόσωπο και να αποκτήσει οικονομικό πλεονέκτημα και άλλα οφέλη.

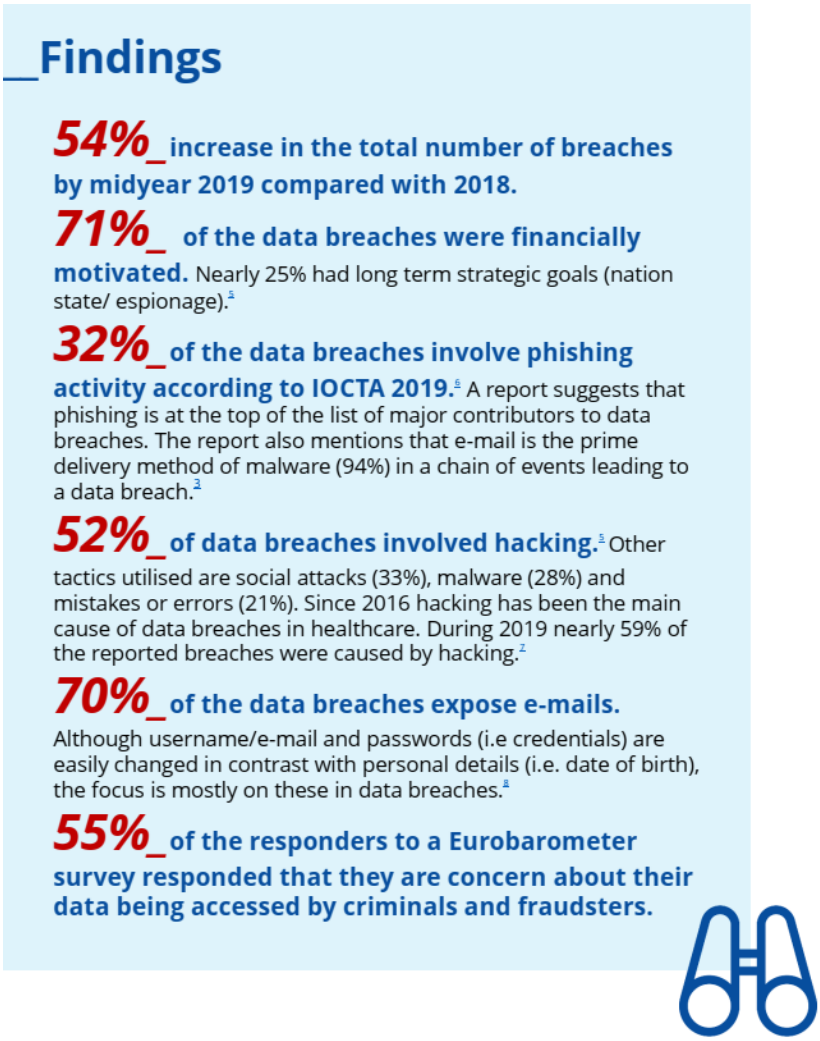


Σχήμα 2.6 Το κόστος των επιθέσεων κλοπής ταυτότητας έτους 2019.
Πηγή: https://www.ibm.com/downloads/cas/LQZ4RONE

2.10 Παραβίαση Δεδομένων (Data Breach)

Η παραβίαση δεδομένων είναι ένα είδος περιστατικού κυβερνοασφάλειας στο οποίο οι πληροφορίες (ή μέρος ενός συστήματος πληροφοριών) είναι προσβάσιμες χωρίς τη σωστή εξουσιοδότηση, συνήθως με κακόβουλη πρόθεση, με αποτέλεσμα την πιθανή απώλεια ή κατάχρηση των εν λόγω πληροφοριών. Περιλαμβάνει επίσης «ανθρώπινο λάθος» που συμβαίνει συχνά κατά τη διαμόρφωση και την ανάπτυξη ορισμένων υπηρεσιών και συστημάτων και μπορεί να οδηγήσει σε ακούσια έκθεση δεδομένων.

Σε πολλές περιπτώσεις, οι εταιρείες ή οι οργανισμοί δεν γνωρίζουν ότι υπάρχει παραβίαση δεδομένων στο περιβάλλον τους λόγω της πολυπλοκότητας της επίθεσης και μερικές φορές εξαιτίας της έλλειψης ορατότητας και ταξινόμησης των πληροφοριών του συστήματος. Με βάση την έρευνα, χρειάζονται περίπου 206 ημέρες για να εντοπιστεί μια παραβίαση δεδομένων σε έναν οργανισμό. Έτσι, χρειάζεται πάρα πολύ χρόνο για να αποκατασταθούν και να ανακτηθούν τα δεδομένα και να επιστρέψει ένα σύστημα στο φυσιολογικό επίπεδο λειτουργίας.



Σχήμα 2.7 Στατιστικά επιθέσεων παραβίασης δεδομένων έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.11 Εσωτερικές Απειλές (Insider Threats)

Η εσωτερική απειλή αφορά εμπιστευτικές πληροφορίες και είναι μια ενέργεια που εκτελείται από κάποιον ή μια ομάδα ατόμων, που συνδέονται ή εργάζονται για το πιθανό θύμα. Υπάρχουν διάφορα πρότυπα που σχετίζονται με εσωτερικές απειλές εμπιστευτικών πληροφοριών. Ένα γνωστό μοτίβο απειλής εμπιστευτικών πληροφοριών (γνωστό και ως «κατάχρηση προνομίων») συμβαίνει όταν ξένοι συνεργάζονται με εσωτερικούς παράγοντες για να αποκτήσουν μη εγκεκριμένη πρόσβαση σε περιουσιακά στοιχεία.

Οι πέντε (5) τύποι εσωτερικής απειλής μπορούν να καθοριστούν σύμφωνα με το σκεπτικό και τους στόχους τους είναι οι εξής παρακάτω:

1) οι απρόσεκτοι εργαζόμενοι που χειρίζονται εσφαλμένα δεδομένα, παραβιάζουν τις πολιτικές χρήσης και εγκαθιστούν μη εξουσιοδοτημένες εφαρμογές
2) οι εσωτερικοί εκπρόσωποι που κλέβουν πληροφορίες για λογαριασμό των ξένων
3) οι δυσαρεστημένοι εργαζόμενοι που επιδιώκουν να βλάψουν την επιχείρησή τους
4) οι κακόβουλοι εσωτερικοί φορείς που είναι εμπιστευτικοί και που χρησιμοποιούν τα υπάρχοντα δικαιώματα για να κλέψουν πληροφορίες για προσωπικό όφελος
5) τα ανήμπορα τρίτα μέρη που θέτουν σε κίνδυνο την ασφάλεια μέσω πληροφοριών, κατάχρησης ή κακόβουλης πρόσβασης ή χρήσης ενός περιουσιακού στοιχείου.

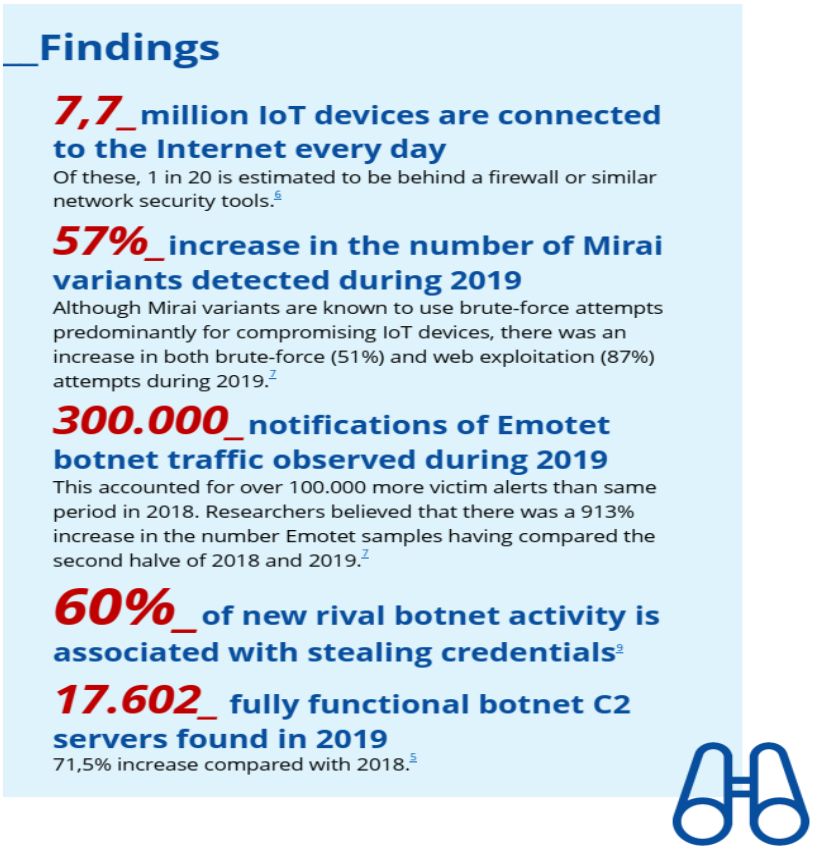
Και οι πέντε τύποι εσωτερικών απειλών εμπιστευτικών πληροφοριών θα πρέπει να μελετώνται συνεχώς, καθώς η αναγνώριση της ύπαρξής τους και ο τρόπος λειτουργίας τους θα πρέπει να καθορίζουν τη στρατηγική του οργανισμού για την ασφάλεια και την προστασία των δεδομένων.

Σχήμα 2.8 Στατιστικά επιθέσεων εσωτερικών απειλών έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.12 Botnet

Το botnet είναι ένα δίκτυο συνδεδεμένων συσκευών που έχουν μολυνθεί από κακόβουλο λογισμικό bot. Αυτές οι συσκευές χρησιμοποιούνται συνήθως από κακόβουλους παράγοντες για τη διεξαγωγή επιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS).



Σχήμα 2.9 Στατιστικά επιθέσεων botnet έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.13 Φυσική Χειραγώγηση Κλοπή, Ζημία, Απώλεια (Physical Manipulation, Damage, Theft And Loss)

Η φυσική παραποίηση, η ζημιά, η κλοπή και η απώλεια έχουν αλλάξει δραστικά τα τελευταία χρόνια. Οι συσκευές, είναι σημαντικό να γίνουν αφαιρούμενες (για να αποτραπεί έτσι η κλοπή τους) και για τις περισσότερες εφαρμογές του επονομαζόμενου «Διαδικτύου των πραγμάτων» (Internet of Things - IoT). Το IoT μπορεί να ενισχύσει τη φυσική ασφάλεια με πιο προηγμένες και σύνθετες λύσεις.

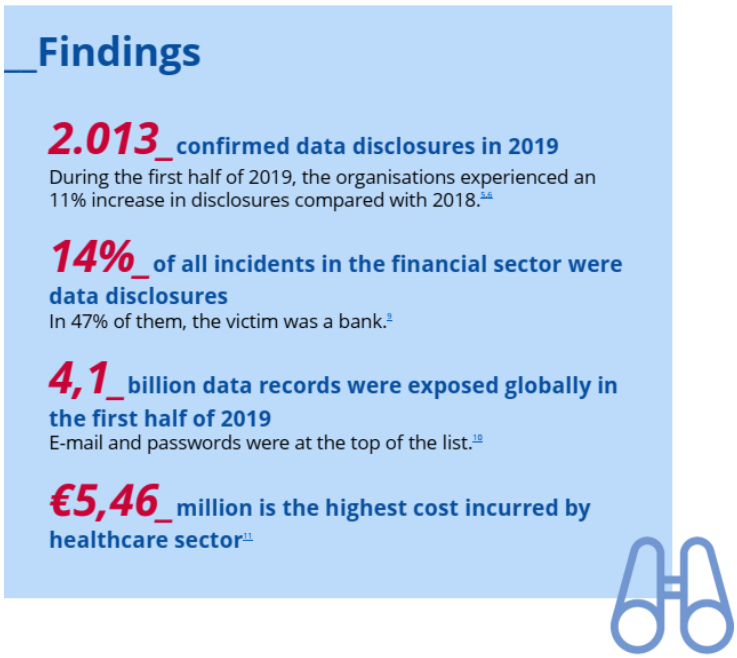
Με αυτόν τον τρόπο, τα συστήματα IP (Internet Protocol) που βασίζονται στην ασφάλεια με έξυπνους αισθητήρες, κάμερες Wi-Fi, έξυπνο φωτισμό ασφαλείας, drones και ηλεκτρονικές κλειδαριές μπορούν να παρέχουν δεδομένα επιτήρησης που αξιολογούνται από μηχανισμούς τεχνητής νοημοσύνης (Artificial Intelligence - AI) και μηχανικής μάθησης (Machine Learning - ML) για τον εντοπισμό απειλών και την αντιμετώπιση με ελάχιστη καθυστέρηση και μέγιστη ακρίβεια.

Σχήμα 2.10 Στατιστικά επιθέσεων μέσω φυσικής χειραγώγησης έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.14 Διαρροή Πληροφοριών (Information Leakage)

Παραβίαση δεδομένων νοείται όταν τα δεδομένα τα οποία βρίσκονται υπό την κατοχή ενός οργανισμού ή μιας εταιρίας, παραβιαστούν, με αποτέλεσμα να παραβιαστεί η εμπιστευτικότητα, η διαθεσιμότητα ή η ακεραιότητά τους. Μια παραβίαση δεδομένων προκαλεί συχνά διαρροή πληροφοριών, η οποία αποτελεί μία από τις σημαντικότερες απειλές στον κυβερνοχώρο, και καλύπτει μια μεγάλη ποικιλία πληροφοριών που έχουν παραβιαστεί, από προσωπικές αναγνωρίσιμες πληροφορίες (Personal Identifiable Information - PII), οικονομικά δεδομένα που αποθηκεύονται σε υποδομές πληροφορικής έως προσωπικές πληροφορίες υγείας (Personal Health Information - PHI) που φυλάσσονται στα αποθετήρια των παρόχων υγειονομικής περίθαλψης.



Σχήμα 2.11 Στατιστικά επιθέσεων μέσω διαρροής πληροφοριών έτους 2019.
Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.15 Ransomware

Το Ransomware έχει γίνει ένα δημοφιλές όπλο στα χέρια των κακόβουλων παραγόντων που προσπαθούν να βλάψουν κυβερνήσεις, επιχειρήσεις και άτομα σε καθημερινή βάση. Σε αυτές τις περιπτώσεις, το θύμα μιας Ransomware επίθεσης, μπορεί να υποστεί οικονομικές απώλειες

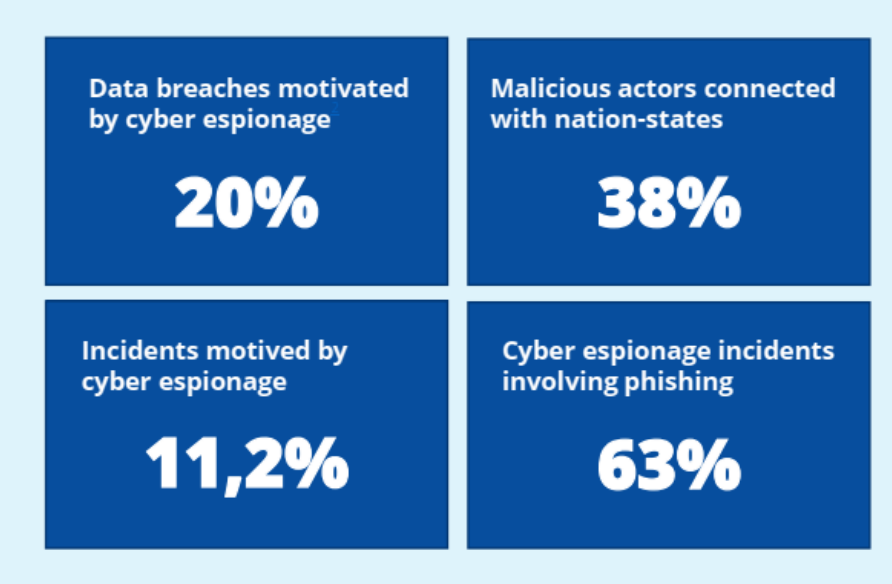
είτε με την καταβολή των λύτρων που απαιτούνται ή με την καταβολή του κόστους της ανάκτησης από την απώλεια, εάν δεν συμμορφώνονται με τις απαιτήσεις του εισβολέα.

Σχήμα 2.12 Στατιστικά επιθέσεων και επιζήμιο κόστος μέσω Ransomware έτους 2019.
Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.16 Κυβερνοκατασκοπεία (Cyber Espionage)

Η Κυβερνοκατασκοπεία θεωρείται απειλή και κίνητρο στην στρατηγική για την κυβερνοασφάλεια. Ορίζεται ως η χρήση δικτύων υπολογιστών για την παράνομη πρόσβαση σε εμπιστευτικές πληροφορίες, συνήθως σε αυτές που κατέχει μια κυβέρνηση ή άλλος οργανισμός.

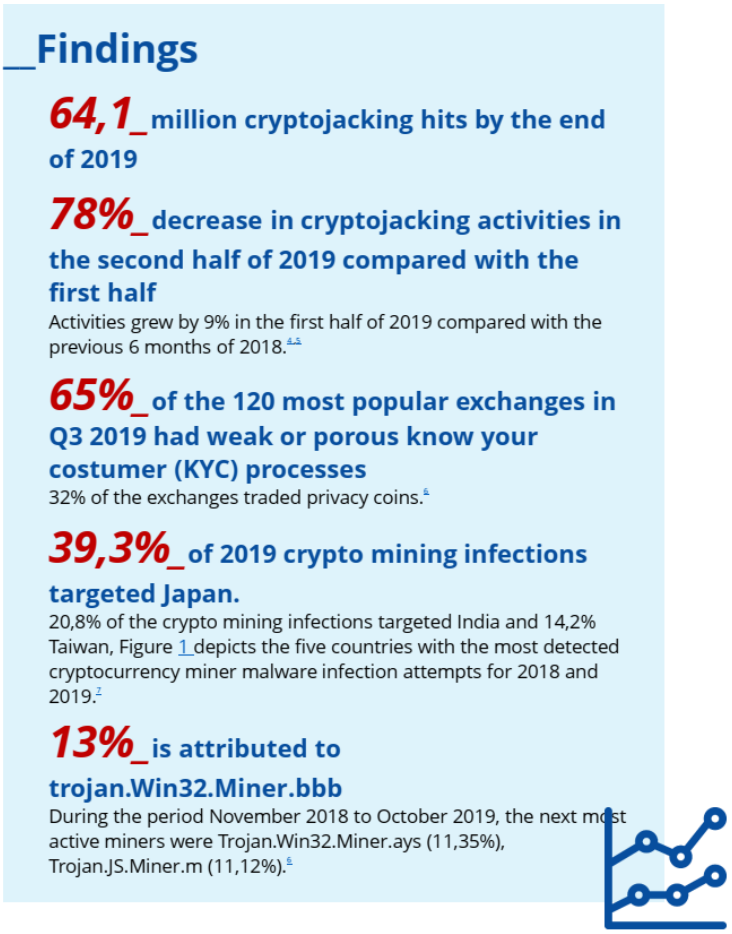
Η κατασκοπεία στον κυβερνοχώρο επικεντρώνεται στην καθοδήγηση της γεωπολιτικής και στην κλοπή κρατικών και εμπορικών μυστικών, δικαιωμάτων πνευματικής ιδιοκτησίας και ιδιόκτητων πληροφοριών σε στρατηγικούς τομείς. Επίσης, η Κυβερνοκατασκοπεία κινητοποιεί παράγοντες από την οικονομία, τη βιομηχανία και τις ξένες υπηρεσίες πληροφοριών, καθώς και παράγοντες που εργάζονται για λογαριασμό τους.



Σχήμα 2.13 Στατιστικά επιθέσεων σχετιζόμενα με κυβερνοκατασκοπεία έτους 2019.
Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

2.17 Crypto Jacking

Cryptojacking (επίσης γνωστή ως cryptomining) είναι η μη εξουσιοδοτημένη χρήση των πόρων μιας συσκευής για την εξόρυξη κρυπτονομισμάτων. Οι στόχοι περιλαμβάνουν οποιαδήποτε συνδεδεμένη συσκευή, όπως υπολογιστές και κινητά τηλέφωνα. Αυτό το είδος της επίθεσης δεν έχει προσελκύσει μεγάλη προσοχή από τις υπηρεσίες επιβολής του νόμου και η καταχρηστική δραστηριότητά της σπάνια αναφέρεται, κυρίως λόγω των σχετικά λίγων αρνητικών συνεπειών της. Ωστόσο, οι οργανισμοί ενδέχεται να παρατηρήσουν υψηλότερο κόστος στον τομέα της πληροφορικής, υποβαθμισμένα εξαρτήματα υπολογιστών, αυξημένη κατανάλωση ηλεκτρικής ενέργειας και μειωμένη παραγωγικότητα των εργαζομένων η οποία οφείλεται σε απαρχαιωμένους υπολογιστές.



Σχήμα 2.14 Στατιστικά επιθέσεων σχετιζόμενα με Cryptojacking έτους 2019.

Πηγή: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

3 ΔΙΕΘΝΕΣ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

3.1 Η Συνθήκη Της Βουδαπέστης

Προκειμένου να καταπολεμηθεί το έγκλημα από τον κυβερνοχώρο σε διεθνές επίπεδο, το 1997 το Συμβούλιο της Ευρώπης (The Council Of Europe) σχημάτισε μια επιτροπή από εξειδικευμένους επιστήμονες έχοντας κατά νου να δημιουργήσει νομοθεσία τέτοια που να μπορεί να χειριστεί αποτελεσματικά την υπόθεση των έκνομων πράξεων στον κυβερνοχώρο. Οι πράξεις αυτές αφορούσαν, ειδικότερα, την προστασία δεδομένων ηλεκτρονικής μορφής (Data), ηλεκτρονικών υπολογιστών καθώς και δικτύων ηλεκτρονικών υπολογιστών από παράνομες δραστηριότητες που αφορούν έννοιες όπως το απόρρητο η διαθεσιμότητα και η ακεραιότητα.

Ως αποτέλεσμα, της προσπάθειας που ξεκίνησε, ήταν η Σύμβαση με αριθμό 185 που υπογράφτηκε στις 23-11-2001 στη Βουδαπέστη. Η Σύμβαση αυτή είναι η πρώτη σε Διεθνές επίπεδο που αφορά εγκλήματα που διαπράχθηκαν μέσω του διαδικτύου αλλά και άλλων δικτύων υπολογιστών. Τα εγκλήματα αυτά αφορούσαν την παραβίαση πνευματικών δικαιωμάτων, απάτη που να συντελείται μέσω ηλεκτρονικού υπολογιστή, παιδική πορνογραφία και παραβίαση της ασφάλειας δικτύων ηλεκτρονικών υπολογιστών. Επίσης, η Σύμβαση περιέχει διαδικασίες όπως η αναζήτηση και η παρακολούθηση δικτύων υπολογιστών. Βασικό της μέλημα είναι ακολουθήσει μία κοινή γραμμή που έχει ως στόχο την προστασία της κοινωνίας από τους διαδικτυακούς κινδύνους, θεσπίζοντας την κατάλληλη νομοθεσία και ενθαρρύνοντας μία σωστά λειτουργικής και άμεσης – από πλευρά αντίδρασης – διεθνούς συνεργασίας.

Η Συνθήκη της Βουδαπέστης ορίζει ότι κάθε συμβαλλόμενο μέρος θα πρέπει να θεσπίσει νομοθεσία και άλλα μέτρα που μπορεί να είναι απαραίτητα για τον ορισμό δικαιοδοσίας για κάθε αδίκημα που διαπράττεται και σχετίζεται με τον κυβερνοχώρο και σχετίζεται με πλοία που είναι συμβαλλόμενα με την εν λόγω σύμβαση. Αυτό σημαίνει πως τα συμβαλλόμενα, με τη σύμβαση, κράτη θα πρέπει να διαθέτουν τα νομοθετικά «εργαλεία», σε εθνικό πια επίπεδο, με βάση τα οποία θα μπορούν να αντιμετωπίσουν κάθε επίθεση από τον κυβερνοχώρο που συμβαίνει επί ενός πλοίου που φέρει τη σημαία του.

Για τη Συνθήκη της Βουδαπέστης θα αναφερθούμε και όταν αναλύεται το Ευρωπαϊκό Νομοθετικό πλαίσιο όσον αφορά το έγκλημα από τον κυβερνοχώρο στη ναυτιλία. Επίσης, σημειώνουμε πως στις αρχές του έτους 2018 επικυρώθηκε η Σύμβαση της Βουδαπέστης από 56 κράτη συνολικά. (www.emsa.eu)

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

Οι κατευθυντήριες γραμμές για την ασφαλή λειτουργία των πλοίων καθορίζονται στον διεθνή κώδικα ISM διαχείρισης της ασφάλειας του IMO. Ο κώδικας αυτός εγκρίθηκε αρχικά από τον I.M.O το 1993 και κατέστη υποχρεωτικός από το 1998. Ο κώδικας ISM εφαρμόζεται στα επιβατηγά πλοία ανεξάρτητα από τη χωρητικότητα και τα φορτηγά πλοία τους άνω των 500 Κοχ. (Κόροι Ολικής Χωρητικότητας – μονάδα μέτρησης της μεταφορικής ικανότητας του πλοίου). Δεν εφαρμόζεται στα σκάφη μη εμπορικής χρήσης.

3.2.1 Στόχοι Του Κώδικα ISM

Οι στόχοι του κώδικα ISM αφορούν στην διασφάλιση της ασφάλειας στη θάλασσα, στην πρόληψη και αποφυγή των ανθρώπινων τραυματισμών - απωλειών ζωών και η αποφυγή επιπτώσεων στο περιβάλλον, (ιδίως στο θαλάσσιο) και στην ιδιοκτησία. Σύμφωνα με τον κώδικα ISM, στόχοι της διαχείρισης της ασφάλειας από την μεριά της ναυτιλιακής εταιρείας είναι:

1. Να παρέχει ασφαλείς πρακτικές για τη λειτουργία του πλοίου καθώς και ασφαλές περιβάλλον εργασίας.
2. Να αξιολογεί όλους τις κινδύνους που έχουν εντοπιστεί στα πλοία, στο προσωπικό και στο περιβάλλον. Μετά από την αξιολόγηση να γίνεται η ανάλογη θέσπιση καταλλήλων προστατευτικών μέτρων.
3. Να βελτιώνει συνεχώς τις δεξιότητες διαχείρισης τις ασφάλειας του προσωπικού που είναι όχι μόνο στη ξηρά και εντός του πλοίου, συμπεριλαμβανομένης και της προετοιμασίας σε καταστάσεις έκτακτου ανάγκης που είναι συνδεδεμένες με την ασφάλεια και με την προστασία του περιβάλλοντος.

3.2.2 Απαιτήσεις Του Κώδικα ISM

Όσον αφορά τις απαιτήσεις του κώδικα ISM έχουμε να πούμε ότι κάθε ναυτιλιακή εταιρεία θα πρέπει να αναπτύξει, να εφαρμόσει και να διατηρήσει ένα σύστημα διαχείρισης της ασφάλειας (Safety Management System, SMS) που περιλαμβάνει τις ακόλουθες λειτουργικές απαιτήσεις:

1. Να σχηματίζει μία πολιτική ασφάλειας και προστασίας για το περιβάλλον.

2. Να περιλαμβάνει οδηγίες και διεργασίες οι οποίες είναι σύμφωνες με τη νομοθεσία του κράτους σημαίας αλλά και με τη διεθνή νομοθεσία για την ασφαλή λειτουργία των πλοίων και την προστασία του περιβάλλοντος.
3. Να θέτει καθορισμένα επίπεδα εξουσίας και κανάλια επικοινωνίας μεταξύ του προσωπικού ξηράς και του πλοίου.
4. Να περιλαμβάνει διαδικασίες αναφοράς ατυχημάτων και μη συμμόρφωσης με τις διατάξεις του κώδικα.
5. Να περιλαμβάνει διαδικασίες προετοιμασίας και αντιμετώπισης καταστάσεων έκτακτης ανάγκης.
6. Να περιλαμβάνει διαδικασίες για εσωτερικούς ελέγχους και διαχειριστικές αναθεωρήσεις. (www.he-alert.org)

Όσο τα σύγχρονα σημερινά πλοία περιλαμβάνουν πολύπλοκα συστήματα, γίνονται όλο και πιο ευάλωτα σε κυβερνοεπιθέσεις, οπότε, είναι πολύ σημαντικό όλες οι ναυτιλιακές εταιρείες να συμπεριλάβουν τον κίνδυνο από τον κυβερνοχώρο στα SMS τους, ώστε να γνωρίζουν πως να αντιμετωπίζουν και να προσεγγίζουν τέτοια συμβάντα. Η «ένταξη» του κινδύνου από τον κυβερνοχώρο στο SMS είναι μία δράση που πρέπει να γίνει και ο χρόνος που θα χρειαστεί για αυτό εξαρτάται από την πολυπλοκότητα των συστημάτων που είναι εγκατεστημένα στα πλοία.

Το SMS της κάθε ναυτιλιακής εταιρείας θα πρέπει να περιλαμβάνει οδηγίες και διαδικασίες για τη διασφάλιση της ασφαλούς λειτουργίας του πλοίου αλλά και την προστασία του περιβάλλοντος, σε συμμόρφωση με τις σχετικές διεθνείς απαιτήσεις και τις απαιτήσεις του κράτους σημαίας. Οι εν λόγω οδηγίες και διαδικασίες θα πρέπει να εξετάζουν τους κινδύνους που προκύπτουν από τη χρήση των Πληροφοριακών Τεχνολογικών Συστημάτων (IT Systems) αλλά και των Λειτουργικών Τεχνολογικών Συστημάτων (OT Systems) επί του πλοίου, λαμβάνοντας υπόψη τους ισχύοντες κώδικες, τις κατευθυντήριες γραμμές και τα απαιτούμενα πρότυπα.

3.3 Ο Κώδικας I.S.P.S (International Ship And Port Facility Security Code)

Οι κατευθυντήριες γραμμές για την πρόληψη εσκεμμένων επιθέσεων και γενικότερα έκνομων πράξεων σε πλοία και λιμενικές εγκαταστάσεις καθορίζονται στον διεθνή κώδικα ασφάλειας

πλοίων και λιμενικών εγκαταστάσεων ISPS που εγκρίθηκε από τον Διεθνή Ναυτιλιακό Οργανισμό του IMO το 2002.

Ο κώδικας ISPS εφαρμόζεται στα πλοία που εκτελούν διεθνή δρομολόγια, συμπεριλαμβανομένων των επιβατηγών πλοίων και των φορτηγών πλοίων χωρητικότητας άνω των 500 κόρων. Ο κώδικας δεν ισχύει για τα πολεμικά πλοία ή τα κυβερνητικά πλοία που χρησιμοποιούνται σε μη εμπορικές υπηρεσίες.

Ο κώδικας ISPS περιλαμβάνει ένα πρώτο μέρος (Α) υποχρεωτικών διατάξεων και ένα δεύτερο μέρος (Β) προαιρετικών διατάξεων κατά τη διακριτική ευχέρεια των εθνικών αρχών. Ο κώδικας αυτός εφαρμόστηκε στην Ευρωπαϊκή Ένωση με τον κανονισμό 725/2004 επιβεβαιώνοντας ως υποχρεωτικές τις διατάξεις του μέρους Α και ορισμένες διατάξεις του μέρους Β.

3.3.1 Στόχοι Του Κώδικα ISPS

Τα πεδία στα οποία προσβλέπει ο κώδικα ISPS είναι:

1. Η θέσπιση διεθνούς πλαισίου που περιλαμβάνει τη συνεργασία μεταξύ κυβερνήσεων, κυβερνητικών υπηρεσιών, τοπικών διοικήσεων, ναυτιλιακών και λιμενικών βιομηχανιών για να εντοπιστούν οι απειλές κατά της ασφάλειας και να ληφθούν προληπτικά μέτρα για την αντιμετώπιση περιστατικών που έχουν να κάνουν με την ασφάλεια των πλοίων ή των λιμενικών εγκαταστάσεων.
2. Ο καθορισμός των αντίστοιχων αρμοδιοτήτων των κυβερνήσεων, των κυβερνητικών υπηρεσιών, των τοπικών διοικήσεων και των ναυτιλιακών και λιμενικών βιομηχανιών, σε εθνικό και διεθνές επίπεδο για τη διασφάλιση της θαλάσσιας ασφάλειας.
3. Η εξασφάλιση αποτελεσματικής συλλογής και ανταλλαγής δεδομένων σχετικών με την ασφάλεια των πλοίων.
4. Η παροχή μεθοδολογίας για τις αξιολογήσεις ασφαλείας, ώστε να υπάρχουν σχέδια και διαδικασίες για την αντίδραση στις μεταβαλλόμενες βαθμίδες ασφαλείας.
5. Η διασφάλιση της βεβαιότητας ότι εφαρμόζονται επαρκή και αναλογικά μέτρα θαλάσσιας ασφάλειας

3.3.2 Επίπεδα Ασφάλειας ISPS

Οι απειλές που εξετάζονται στον κώδικα ISPS είναι κυρίως φυσικού τύπου. Απειλές δηλαδή όπως πειρατεία, τρομοκρατία και γενικότερα απειλές που έχουν να κάνουν με την φυσική ασφάλεια των

πλοίων, των πληρωμάτων τους αλλά και των λιμενικών εγκαταστάσεων. Τα πλοία υποχρεούνται να εφαρμόζουν σταδιακά προστατευτικά μέτρα ασφαλείας σύμφωνα με τα ακόλουθα επίπεδα:

- Επίπεδο ασφάλειας 1: επίπεδο στο οποίο τα ελάχιστα κατάλληλα προστατευτικά μέτρα ασφαλείας εφαρμόζονται.
- Επίπεδο ασφάλειας 2: επίπεδο κατά το οποίο εφαρμόζονται κατάλληλα πρόσθετα προστατευτικά μέτρα ασφαλείας ως αποτέλεσμα αυξημένου κινδύνου περιστατικού ασφαλείας για ορισμένο χρονικό διάστημα.
- Επίπεδο ασφάλειας 3: επίπεδο κατά το οποίο μπαίνουν σε ισχύ περαιτέρω ειδικά μέτρα ασφαλείας για περιορισμένο χρονικό διάστημα όταν ένα περιστατικό είναι πιθανό ή άμεσο, αν και ενδέχεται να μην είναι δυνατός ο προσδιορισμός του συγκεκριμένου στόχου.

Με βάση τα παραπάνω, λοιπόν, οι συμβαλλόμενες εθνικές κυβερνήσεις του ISPS είναι υπεύθυνες για τα ακόλουθα:

1. Καθορισμός του ισχύοντος επιπέδου ασφάλειας.
2. Έγκριση αξιολόγησης ασφάλειας λιμενικής εγκατάστασης και μεταγενέστερων τροποποιήσεων εγκεκριμένης αξιολόγησης.
3. Καθορισμός των λιμενικών εγκαταστάσεων που θα απαιτείται για τον ορισμό υπεύθυνου ασφάλειας λιμενικής εγκατάστασης.
4. Έγκριση σχεδίου ασφάλειας λιμενικής εγκατάστασης και μεταγενέστερων τροποποιήσεων εγκεκριμένου σχεδίου.
5. Άσκηση μέτρων ελέγχου και συμμόρφωσης.
6. Καθορισμός των απαιτήσεων για δήλωση ασφάλειας. (www.he-alert.org)

3.3.3 Ρόλοι Στον ISPS

Ο Υπεύθυνος Ασφάλειας Εταιρείας (Company Security Officer – CSO) είναι το πρόσωπο που ορίζεται από την εταιρεία για να εξασφαλίζει τη διενέργεια Αξιολόγησης της Ασφάλειας του Πλοίου, την ανάπτυξη Σχεδίου Ασφάλειας Πλοίου, την υποβολή προς έγκριση και, στη συνέχεια, την εφαρμογή και τη συντήρηση, καθώς και για τη σύνδεση με τον Υπεύθυνο Ασφάλειας Πλοίου και τον Υπεύθυνο Ασφάλειας Λιμενικής Εγκατάστασης.

Ο Υπεύθυνος Ασφάλειας Πλοίου (Ship Security Officer – SSO) είναι το άτομο επί του πλοίου, το οποίο λογοδοτεί στον πλοίαρχο. Ορίζεται από την εταιρεία ως υπεύθυνος για την ασφάλεια του πλοίου, συμπεριλαμβανομένης της εφαρμογής και της συντήρησης του Σχεδίου Ασφάλειας του Πλοίου, και για τη σύνδεση και συνεργασία με τον Υπεύθυνο Ασφάλειας Εταιρείας και τον Υπεύθυνο Ασφάλειας Λιμενικής Εγκατάστασης.

Ο Υπεύθυνος Ασφάλειας Λιμενικής Εγκατάστασης (Port Facility Security Officer – PFSO) είναι εντεταλμένος υπάλληλος για τις λιμενικές εγκαταστάσεις. Είναι υπεύθυνος για την ανάπτυξη, την εφαρμογή, την αναθεώρηση και τη επικαιροποίηση του Σχεδίου Ασφάλειας Λιμενικής Εγκατάστασης και για τη σύνδεση και συνεργασία με τον Υπεύθυνο Ασφάλειας Εταιρείας και τον Υπεύθυνο Ασφάλειας Πλοίου.

3.3.4 Σχέδιο Ασφάλειας Πλοίου (Ship Security Plan – SSP)

Σύμφωνα με τον κώδικα ISPS, πρέπει να δημιουργηθεί ένα Σχέδιο Ασφάλειας Πλοίου (Ship Security Plan - SSP).

Το SSP επικεντρώνεται σαφώς στη φυσική ασφάλεια. Για παράδειγμα, το περιεχόμενό του θα περιλαμβάνει αναφορές στις ευθύνες των ανθρώπων στο πλοίο και στην ξηρά, φυσικούς ελέγχους πρόσβασης στο πλοίο, φρουρούς και περιπολίες, επιτήρηση CCTV και δράση κατά πιθανών πειρατικών επιθέσεων.

Η Εκτίμηση Κινδύνου Πλοίου (Ship Security Assessment – SSA) αποτελεί ουσιώδες και αναπόσπαστο μέρος της ανάπτυξης και της επικαιροποίησης του σχεδίου ασφάλειας πλοίων (SSP). Ο Υπεύθυνος Ασφάλειας Εταιρείας (Company Security Officer – CSO) θα διασφαλίζει ότι τα άτομα με τις κατάλληλες δεξιότητες που λαμβάνουν τις κατευθυντήριες γραμμές που παρέχονται στο μέρος Β του κώδικα ISPS εκπονούν την Εκτίμηση Κινδύνου Πλοίου. Ο Υπεύθυνος Ασφάλειας της Εταιρείας είναι υπεύθυνος για την εκτίμηση κινδύνου και οφείλει επίσης να την εγκρίνει.

Η Εκτίμηση Κινδύνου Πλοίου θα περιλαμβάνει επιτόπια έρευνα ασφάλειας έχοντας όψη τα ακόλουθα στοιχεία:

1. Τον προσδιορισμό των υφιστάμενων μέτρων, διαδικασιών και πράξεων ασφαλείας.
2. Τον προσδιορισμό και αξιολόγηση των βασικών λειτουργιών επί του πλοίου που είναι σημαντικό να προστατευθούν.
3. Τον εντοπισμό πιθανών απειλών και την πιθανότητα εμφάνισής τους και
4. Τον προσδιορισμό της αδυναμίας, συμπεριλαμβανομένων των ανθρώπινων παραγόντων.

Σημειώνεται, όσον αφορά την Εκτίμηση Κινδύνου Πλοίου πως τεκμηριώνεται, αναθεωρείται, γίνεται αποδεκτή και διατηρείται από την εταιρεία.

3.3.5 Σχέδιο Ασφάλειας Λιμενικής Εγκατάστασης (Port Facility Security Plan – PFSP)

Το Σχέδιο Ασφάλειας Λιμενικής Εγκατάστασης (PFSP) αναπτύσσεται και συντηρείται με βάση την Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης (Port Facility Security Assessment – PFSA) για κάθε Λιμενική Εγκατάσταση. Η Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης (PFSA), κατά τον κώδικα ISPS, αποτελεί ουσιώδες και αναπόσπαστο μέρος της διαδικασίας ανάπτυξης ή επικαιροποίησης του Σχεδίου Ασφάλειας Λιμενικής Εγκατάστασης.

Η Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης (Port Facility Security Assessment – PFSA) αποτελεί ουσιώδες και αναπόσπαστο μέρος της ανάπτυξης και της επικαιροποίησης του Σχέδιου Ασφάλειας Λιμενικής Εγκατάστασης. Το συμβαλλόμενο, με τον κώδικα, κράτος ή ο Αναγνωρισμένος Οργανισμός Ασφαλείας, οι οποίοι πρέπει να διαθέτουν τις κατάλληλες δεξιότητες, διενεργούν την Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης. Πρέπει να επανεξετάζεται και να ενημερώνεται περιοδικά λαμβάνοντας υπόψη τυχόν νέες απειλές ή αλλαγές στην ασφάλεια των λιμενικών εγκαταστάσεων.

Η Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης θα πρέπει να διευθετεί τα ακόλουθα:

1. Τον εντοπισμό και την αξιολόγηση σημαντικών περιουσιακών στοιχείων και υποδομών που χρήζουν προστασίας.
2. Τον εντοπισμό πιθανών απειλών και τη συχνότητα εμφάνισης του επί των περιουσιακών στοιχείων και των υποδομών.
3. Τον προσδιορισμό των διαδικαστικών αλλαγών για τη μείωση της ευπάθειας και των τρωτών σημείων.
4. Τον εντοπισμό αδυναμιών, συμπεριλαμβανομένων των ανθρώπινων παραγόντων.

Η Αξιολόγηση Ασφάλειας Λιμενικής Εγκατάστασης μπορεί να εφαρμοστεί σε περισσότερες από μία Λιμενικές Εγκαταστάσεις, εάν γίνει αποδεκτή από το συμβαλλόμενο, με τον κώδικα, κράτος.

Θα πρέπει να καταγράφεται η μεθοδολογία που χρησιμοποιείται για την πραγματοποίηση της Αξιολόγησης Ασφάλειας Λιμενικής Εγκατάστασης. Η αξιολόγηση και το σχέδιο ασφάλειας λιμενικής εγκατάστασης θα πρέπει να πληρούν τις διεθνείς απαιτήσεις του κώδικα ISPS και των τοπικών εθνικών αρχών.

3.4 Εγκύκλιος Του I.M.O. Για Την Κυβερνοασφάλεια (MSC-Fal.1-Circ.3)

Η επιτροπή διευκόλυνσης, κατά την 41η σύνοδό της (4 έως 7 Απριλίου 2017), και η Επιτροπή για την Ασφάλεια στη Θάλασσα, κατά την 98η σύνοδό της (7 έως 16 Ιουνίου 2017), έχοντας εξετάσει την επείγουσα ανάγκη ευαισθητοποίησης σχετικά με τις απειλές και τα τρωτά σημεία του κυβερνοχώρου, ενέκριναν τις κατευθυντήριες γραμμές για τη διαχείριση των θαλάσσιων κινδύνων στον κυβερνοχώρο, όπως ορίζονται στο παράρτημα. Στην παράγραφο αυτή θα περιγράψουμε την εγκύκλιο του ΙΜΟ που σχετίζεται με την κυβερνοασφάλεια.

3.4.1 Γενικό Πλαίσιο

Οι παρούσες κατευθυντήριες γραμμές που δίνονται παρέχουν συστάσεις για τη διαχείριση περιστατικών επίθεσης στον διαδίκτυο. Ο θαλάσσιος κίνδυνος στον κυβερνοχώρο ορίζεται ως όταν ένα τεχνολογικό περιουσιακό στοιχείο απειλείται από πιθανή περίσταση ή γεγονός, το οποίο μπορεί να οδηγήσει σε βλάβες που σχετίζονται με τη ναυτιλία σε λειτουργία, ασφάλεια ή ασφάλεια ως συνέπεια της καταστροφής, απώλειας ή παραβίασης πληροφοριών ή συστημάτων.

Τα ενδιαφερόμενα μέρη θα πρέπει να λάβουν τα αναγκαία μέτρα για να προστατεύσουν τη ναυτιλία από πιθανές απειλές και ευάλωτα σημεία που σχετίζονται με την ψηφιοποίηση, την ολοκλήρωση και την αυτοματοποίηση των διαδικασιών και των συστημάτων στη ναυτιλία.

Για λεπτομέρειες και καθοδήγηση σχετικά με την ανάπτυξη και την εφαρμογή οι διαδικασίες διαχείρισης κινδύνων, οι χρήστες των παρουσών κατευθυντήριων γραμμών θα πρέπει να ανατρέχουν στις απαιτήσεις των συγκεκριμένων κυβερνήσεων ή διοικήσεων σημαίας, καθώς και στα διεθνή και βιομηχανικά πρότυπα όπως αυτά έχουν καθοριστεί, αλλά και στις και βέλτιστες πρακτικές.

Η διαχείριση κινδύνου είναι θεμελιώδης για ασφαλείς ναυτιλιακές δραστηριότητες. Η διαχείριση κίνδυνου ως επί των πλείστων, επικεντρώνεται σε φυσικά προβλήματα κυρίως οικονομοτεχνικής φύσεως αλλά προκύπτει πλέον η ανάγκη διαχείρισης κινδύνου στην ψηφιοποίηση δεδομένων, την

αυτοματοποίηση και τα συστήματα όπου οι λειτουργίες τους και η αλληλεπίδρασή τους, βασίζεται στο δίκτυο.

Με βάση το στόχο της στήριξης της ασφαλούς ναυτιλίας, η οποία είναι λειτουργικά ανθεκτική στους κινδύνους στον κυβερνοχώρο, οι κατευθυντήριες γραμμές παρέχουν προτάσεις οι οποίες μπορούν να ενσωματωθούν στις τρέχουσες διαδικασίες διαχείρισης και αξιολόγησης κινδύνων. Εν προκειμένω, οι κατευθυντήριες γραμμές είναι συμπληρωματικές προς τις πρακτικές διαχείρισης της ασφάλειας και της προστασίας που έχουν καθοριστεί από τον IMO.

3.4.2 Υπόβαθρο

Οι τεχνολογίες του κυβερνοχώρου αποτελούν θεμελιώδη λίθο για τη λειτουργία και διαχείριση ενός μεγάλου μέρους συστημάτων που είναι κρίσιμα όσον αφορά την ασφάλεια της ναυτιλίας καθώς και την προστασία του περιβάλλοντος. Σε μερικές περιπτώσεις αυτά τα συστήματα πρέπει να συμμορφώνονται με διεθνή πρότυπα και με απαιτήσεις σημαίας (Flag Administration). Προκύπτουν, όμως, μέσω της προσπέλασης των συστημάτων αυτών αδύνατα σημεία (Vulnerabilities) που μπορεί να γίνουν εκμεταλλεύσιμα από "φορείς" του κυβερνοχώρου οπότε προκύπτουν θέματα κυβερνοασφάλειας. Τα συστήματα αυτά θα μπορούσαν να είναι, ανάμεσα σε άλλα, τα εξής παρακάτω:

1. Συστήματα Γέφυρας.
2. Συστήματα διαχείρισης και χειρισμού του φορτίου που μπαίνει σε ένα πλοίο.
3. Συστήματα διαχείρισης πρόωσης, μηχανημάτων και ελέγχου ισχύος.
4. Συστήματα ελέγχου προσπέλασης (Access Control Systems)
5. Συστήματα διαχείρισης και εξυπηρέτησης επιβατών.
6. Δημόσια δίκτυα (Public Networks) με τα οποία συνδέονται οι επιβάτες.
7. Συστήματα Επικοινωνίας

Η διάκριση μεταξύ Λειτουργικών και Πληροφοριακών Τεχνολογικών Συστημάτων (Information Technology Systems – IT Systems, Operation Technology Systems – OT Systems) πρέπει να ληφθούν υπόψη. Τα Πληροφοριακά Τεχνολογικά Συστήματα μπορεί να θεωρηθούν ότι επικεντρώνονται στη χρήση των δεδομένων ως πληροφοριών. Τα Λειτουργικά Τεχνολογικά Συστήματα μπορεί να θεωρούνται ότι επικεντρώνονται στη χρήση δεδομένων για τον έλεγχο ή την παρακολούθηση των φυσικών διεργασιών. Επιπλέον, θα πρέπει επίσης να εξεταστεί το ενδεχόμενο προστασίας των πληροφοριών και της ανταλλαγής δεδομένων στο πλαίσιο αυτών των συστημάτων.

Ενώ οι νέες τεχνολογίες παρέχουν σημαντικά κέρδη στη ναυτιλιακή βιομηχανία, παρουσιάζουν επίσης κινδύνους για τα ηλεκτρονικά συστήματα και τις διαδικασίες που εκτελούν. Οι κίνδυνοι αυτοί μπορεί να προκύψουν από τρωτά σημεία που οφείλονται σε ανεπαρκή λειτουργία, στη συντήρηση και το σχεδιασμό συστημάτων που σχετίζονται με τον κυβερνοχώρο, καθώς και από εσκεμμένες και ακούσιες απειλές στον κυβερνοχώρο.

Οι απειλές προέρχονται από κακόβουλες ενέργειες (π.χ. πειρατεία ή εισαγωγή κακόβουλου λογισμικού) ή ακούσιες ενέργειες (π.χ. συντήρηση λογισμικού). Γενικά, αυτές οι ενέργειες εκθέτουν τα τρωτά σημεία (π.χ. ξεπερασμένο λογισμικό ή αναποτελεσματικά τείχη προστασίας) ή εκμεταλλεύονται μια αδυναμία των IT και OT συστημάτων. Η αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο θα πρέπει να λαμβάνει υπόψη και τα δύο είδη απειλών.

Τα τρωτά σημεία μπορεί να προκύψουν από ανεπάρκειες στο σχεδιασμό, την ολοκλήρωση ή/και τη συντήρηση συστημάτων, καθώς και των ελλείψεων στην κυβερνο-απειθαρχία. Γενικά, όταν εκτίθενται ή αξιοποιούνται τρωτά σημεία στην επιχειρησιακή ή/και την τεχνολογία των πληροφοριών, είτε άμεσα (π.χ. αδύναμοι κωδικοί πρόσβασης) είτε έμμεσα (π.χ. απουσία διαχωρισμού δικτύου), μπορεί να υπάρξουν συνέπειες για την ασφάλεια και την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών. Επιπλέον, όταν εκτίθενται ή αξιοποιούνται τα τρωτά σημεία της λειτουργικής ή/και της πληροφοριακής τεχνολογίας, μπορεί να υπάρξουν επιπτώσεις στην ασφάλεια, ιδίως όταν τα κρίσιμα συστήματα (π.χ. πλοήγηση γέφυρας ή κύρια συστήματα πρόωσης) τίθενται σε κίνδυνο.

Η αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο θα πρέπει επίσης να λαμβάνει υπόψη τις επιπτώσεις στην ασφάλεια και την προστασία που προκύπτουν από την έκθεση ή την εκμετάλλευση τρωτών σημείων σε συστήματα πληροφορικής. Αυτό θα μπορούσε να προκύψει από ακατάλληλη σύνδεση με Λειτουργικά Τεχνολογικά Συστήματα ή από διαδικαστικές παραλείψεις από επιχειρησιακό προσωπικό ή τρίτους, οι οποίες ενδέχεται να θέσουν σε κίνδυνο τα συστήματα αυτά (π.χ. ακατάλληλη χρήση αφαιρούμενων μέσων, όπως ένα memory stick).

Αυτές οι ταχέως μεταβαλλόμενες τεχνολογίες και απειλές καθιστούν δύσκολη την αντιμετώπιση κινδύνων μόνο μέσω τεχνικών προτύπων. Ως εκ τούτου, κατευθυντήριες γραμμές συνιστούν μια προσέγγιση της διαχείρισης των κινδύνων στον κυβερνοχώρο που είναι ανθεκτικοί και εξελίσσεται ως φυσική επέκταση των υφιστάμενων πρακτικών διαχείρισης της ασφάλειας και της ασφάλειας.

Κατά την εξέταση πιθανών πηγών απειλών και τρωτών σημείων και στρατηγικών μετριασμού, θα πρέπει επίσης να ληφθούν υπόψη ορισμένες πιθανές επιλογές ελέγχου για τη διαχείριση των κινδύνων στον κυβερνοχώρο, συμπεριλαμβανομένων, μεταξύ άλλων, των διαχειριστικών, επιχειρησιακών ή διαδικαστικών και των τεχνικών ελέγχων.

3.4.3 Εφαρμογή

Αναγνωρίζοντας ότι δεν υπάρχουν δύο οργανισμοί στον ναυτιλιακό κλάδο που να είναι οι ίδιοι, οι κατευθυντήριες γραμμές εκφράζονται σε γενικές γραμμές προκειμένου να υπάρχει ευρεία εφαρμογή. Τα πλοία με περιορισμένα συστήματα που σχετίζονται με τον κυβερνοχώρο μπορούν να θεωρήσουν επαρκή την απλή εφαρμογή των παρουσών κατευθυντήριων γραμμών·

Ωστόσο, τα πλοία με πολύπλοκα συστήματα που σχετίζονται με τον κυβερνοχώρο μπορεί να απαιτούν μεγαλύτερο επίπεδο προστασίας και θα πρέπει να αναζητούν πρόσθετους πόρους μέσω αξιόπιστων βιομηχανικών και κυβερνητικών εταίρων.

3.4.4 Στοιχεία Της Διαχείρισης Κινδύνου Στον Κυβερνοχώρο

Η διαχείριση κινδύνων στον κυβερνοχώρο σημαίνει ότι εντοπίζεται, αξιολογείται και αναλύεται ένας πιθανός κίνδυνος που σχετίζεται με τον κυβερνοχώρο και στην συνέχεια γίνεται προσπάθεια αποφυγής, μεταφοράς η ακόμα και μετριασμού του σε ένα κοινώς αποδεκτό επίπεδο, λαμβάνοντας υπόψη το κόστος και τα οφέλη των δράσεων που αναλαμβάνονται από τους ενδιαφερόμενους. Στόχος της θαλάσσιας διαχείρισης κινδύνων στον κυβερνοχώρο είναι η υποστήριξη της ασφάλειας ναυσιπλοΐας που είναι λειτουργικά ανθεκτική στους κινδύνους του κυβερνοχώρου.

Η αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο θα πρέπει να ξεκινήσει από τα ανώτερα διοικητικά στελέχη. Η ανώτερη διαχείριση θα πρέπει να ενσωματώνει μια νοοτροπία ευαισθητοποίησης σχετικά με τους κινδύνους στον κυβερνοχώρο σε όλα τα επίπεδα ενός οργανισμού και να διασφαλίζει ένα ολιστικό και ευέλικτο καθεστώς διαχείρισης κινδύνων στον κυβερνοχώρο, το οποίο να βρίσκεται σε συνεχή λειτουργία και να αξιολογείται συνεχώς μέσω αποτελεσματικών μηχανισμών ανατροφοδότησης.

Μια αποδεκτή προσέγγιση για την επίτευξη των ανωτέρω είναι η ολοκληρωμένη αξιολόγηση και σύγκριση των αποτελεσμάτων της με τα επιθυμητά επίπεδα που έχει ορίσει μια εταιρία. Μια τέτοια σύγκριση μπορεί να αποκαλύψει κενά που μπορούν να αντιμετωπιστούν για την επίτευξη των στόχων διαχείρισης κινδύνων μέσω ενός σχεδίου διαχείρισης κινδύνων στον κυβερνοχώρο με προτεραιότητα. Αυτή η προσέγγιση που βασίζεται στον κίνδυνο θα επιτρέψει σε έναν οργανισμό

να εφαρμόσει καλύτερα τους πόρους του με τον πιο αποτελεσματικό τρόπο. Οι παρούσες κατευθυντήριες γραμμές παρουσιάζουν τα λειτουργικά στοιχεία που υποστηρίζουν την αποτελεσματική διαχείριση κίνδυνου στον κυβερνοχώρο. Αυτά τα λειτουργικά στοιχεία δεν είναι διαδοχικά – όλα θα πρέπει να είναι ταυτόχρονα και συνεχή στην πράξη και θα πρέπει να ενσωματώνονται κατάλληλα σε μια διαχείριση κινδύνου

- **Καθορισμός (Identify)***:* Καθορισμός ρόλων προσωπικού και ευθυνών για τη διαχείριση κίνδυνου από τον κυβερνοχώρο. Αναγνώριση συστημάτων, περιουσιακών στοιχείων, δεδομένων και ικανοτήτων που, όταν διαβάλλονται, εμφανίζουν κινδύνους στις λειτουργίες ενός πλοίου.

- **Προστασία (Protect)***:* Εφαρμογή διαδικασιών και μέτρων για τον έλεγχο κινδύνου. Σχεδιασμός έκτακτης ανάγκης για την προστασία από συμβάντα προερχόμενα από τον κυβερνοχώρο και τη διασφάλιση της συνέχειας των ναυτιλιακών λειτουργιών.

- **Εντοπισμός (Detect)***:* Ανάπτυξη και εφαρμογή δραστηριοτήτων που είναι απαραίτητες για τον έγκαιρο εντοπισμό ενός γεγονότος από τον κυβερνοχώρο.

- **Αντίδραση (Respond)***:* Ανάπτυξη και εφαρμογή δραστηριοτήτων και σχεδίων που παρέχουν ανθεκτικότητα και ανάκτηση συστημάτων που είναι απαραίτητα για τις ναυτιλιακές λειτουργίες ή υπηρεσίες που υφίστανται βλάβη από συμβάν του κυβερνοχώρου.

- **Ανάκτηση (Recover)***:* Προσδιορισμός των μέτρων εκείνων για την υποστήριξη και την αποκατάσταση των συστημάτων στον κυβερνοχώρο που είναι απαραίτητα για τις ναυτιλιακές επιχειρήσεις που επηρεάζονται από γεγονότα του κυβερνοχώρου.

Αυτά τα λειτουργικά στοιχεία περιλαμβάνουν όλες τις δραστηριότητες και τα επιθυμητά αποτελέσματα από μία αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο σε κρίσιμα συστήματα που επηρεάζουν τις θαλάσσιες επιχειρήσεις και την ανταλλαγή πληροφοριών, και αποτελούν μια συνεχή διαδικασία με αποτελεσματικούς μηχανισμούς ανάδρασης.

Η αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο, θα πρέπει να διασφαλίζει κατάλληλο επίπεδο ευαισθητοποίησης των κινδύνων σε όλα τα επίπεδα ενός οργανισμού. Το

επίπεδο ευαισθητοποίησης και ετοιμότητας θα πρέπει να είναι κατάλληλο για τους ρόλους και τις ευθύνες στο σύστημα διαχείρισης.

3.4.5 Βέλτιστες Πρακτικές Εφαρμογής

Οι προτεινόμενες κατευθυντήριες γραμμές παρέχουν τα θεμέλια για την καλύτερη κατανόηση και διαχείριση των απειλών από το διαδίκτυο, επιτρέποντας έτσι μια προσέγγιση διαχείρισης κινδύνων για την αντιμετώπιση τους και των τρωτών τους σημείων. Για λεπτομερείς οδηγίες σχετικά με τη διαχείριση των κινδύνων αυτών, οι χρήστες των κατευθυντήριων γραμμών θα πρέπει επίσης να αναφέρονται στις απαιτήσεις που έχουν θεσπίσει οι εκάστοτε κυβερνήσεις και τα κράτη-μέλη , καθώς και στα σχετικά διεθνή και βιομηχανικά πρότυπα και βέλτιστες πρακτικές.

Πρόσθετες οδηγίες και πρότυπα μπορεί να περιλαμβάνουν, χωρίς να περιορίζονται:

1. Οι κατευθυντήριες γραμμές για την ασφάλεια στον διαδίκτυο επί των πλοίων που παράγονται και υποστηρίζονται από τους οργανισμούς: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCOMF και IOMI
2. Πρότυπο ISO/IEC 27001 για την τεχνολογία των πληροφοριών – Τεχνικές ασφαλείας – Συστήματα διαχείρισης ασφάλειας πληροφοριών – Απαιτήσεις. Δημοσιεύθηκε από κοινού από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) και την Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission - IEC).
3. Πλαίσιο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών για τη βελτίωση της ασφάλειας στον κυβερνοχώρο στον κυβερνοχώρο για τις υποδομές ζωτικής σημασίας (National Institute of Standards and Technology’s Framework – NIST Framework).

3.5 Ψήφισμα MSC 428(98) (Resolution)

Με βάση την εγκύκλιο MSC-FAL.1-Circ.3, που εξέδωσαν οι επιτροπές MSC και FAL του IMO, η επιτροπή MSC εξέδωσε κατευθυντήρια οδηγία (Resolution), την MSC.428(98), στις 16-7-2017. Εντός αυτής, τονίζοντας τους στόχους του κώδικα ISM που, μεταξύ άλλων είναι, η παροχή ασφαλών πρακτικών κατά τη λειτουργία ενός πλοίου αλλά και για ένα ασφαλές περιβάλλον εργασίας, η εκτίμηση όλων των ανιχνευμένων κινδύνων σε πλοίο, προσωπικό και περιβάλλον, η θέσπιση κατάλληλων μέτρων προστασίας και η συνεχής βελτίωση των δεξιοτήτων που αφορούν τη διαχείριση ασφάλειας για το προσωπικό στο πλοίο και στη στεριά :

- *ΔΙΑΒΕΒΑΙΩΝΕΙ* ότι ένα εγκεκριμένο Σύστημα Ασφαλούς Διαχείρισης (Safety Management System – SMS) πρέπει να λαμβάνει υπόψη τη διαχείριση κινδύνου από τον κυβερνοχώρο και να είναι εναρμονισμένο με τους στόχους και λειτουργικές απαιτήσεις του κώδικα ISM.
- *ΕΝΘΑΡΡΥΝΕΙ* τις κυβερνήσεις να διασφαλίσουν πως οι κίνδυνοι από τον διαδίκτυο είναι κατάλληλα διευθετημένοι στα Συστήματα Ασφαλούς Διαχείρισης όχι αργότερα από την πρώτη επικύρωση του Κειμένου Συμμόρφωσης (Document of Compliance – DoC) μετά την 1η Ιανουαρίου του έτους 2021.
- *ΑΝΑΓΝΩΡΙΖΕΙ* τα σημαντικά μέτρα πρόληψης που μπορεί να χρειαστούν για τη διατήρηση της εμπιστευτικότητας ορισμένων πτυχών της διαχείρισης κινδύνου από τον κυβερνοχώρο.
- *ΑΠΑΙΤΕΙ* από τα Κράτη-Μέλη, του IMO, να θέσουν υπόψιν των ενδιαφερόμενων πλευρών την κατευθυντήρια γραμμή που εκδίδει.

4 ΕΥΡΩΠΑΪΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

4.1 Ο Κανονισμός 725/2004

Στον τομέα της ναυτιλίας, η Ευρωπαϊκή Ένωση έχοντας υπόψη τον κώδικα ISPS, που υιοθετήθηκε από τον ΙΜΟ το έτος 2002, ανέπτυξε τον Κανονισμό (EC) 725/2004 του Ευρωπαϊκού Κοινοβουλίου και Επιτροπής στις 31 Μαρτίου του έτους 2004 (Regulation (EC) 725/2004) για τη βελτίωση και ανάδειξη της ασφάλειας από έκνομες πράξεις των πλοίων αλλά και των λιμένων και των λιμενικών εγκαταστάσεων. Το βασικό αντικείμενο και στόχος του κανονισμού αυτού είναι η παρουσίαση και η εφαρμογή μέτρων της Ευρωπαϊκής Κοινότητας που στοχεύουν στη βελτίωση της ασφάλειας από έκνομες πράξεις όσον αφορά τα πλοία αλλά και τις σχετικές λιμενικές εγκαταστάσεις που μετέχουν στο εμπόριο τόσο σε διεθνές όσο και σε εθνικό επίπεδο. Τα μέτρα αυτά συνδέονται, πάντα, με την αντιμετώπιση των απειλών από σκόπιμες παράνομες δραστηριότητες.

Αφού υιοθετήθηκε ο κανονισμός 725/2004, κάποιες από τις προτάσεις και συμβουλές του Μέρους Β του ISPS κώδικα έγιναν υποχρεωτικές (αντί να είναι προτεινόμενες) για τα κράτη-μέλη της Ευρωπαϊκής Ένωσης. Αυτά τα υποχρεωτικά στοιχεία αφορούν:

- την Αξιολόγηση Κινδύνου Πλοίου (Ship Security Assessment)
- το Σχέδιο Κινδύνου Πλοίου (Ship Security Plan)
- την Αξιολόγηση Κινδύνου Λιμενικής Εγκατάστασης (Port Facility Security Assessment)
- το Σχέδιο Κινδύνου Λιμενικής Εγκατάστασης (Port Facility Security Plan)

και στις πιο κάτω παραγράφους αναλύονται εκτενέστερα.

4.1.1 Αξιολόγηση Κινδύνου Πλοίου

Η Αξιολόγηση Κινδύνου Πλοίου θα πρέπει να εκτιμήσει και λάβει υπόψη τα άτομα, τις δραστηριότητες, τις υπηρεσίες και τις λειτουργίες που είναι σημαντικές να προστατευθούν, περιλαμβανομένης της ικανότητας διατήρησης ασφαλούς πλοήγησης, της αντιμετώπισης καταστάσεων έκτακτης ανάγκης, τον εξοπλισμό και τα συστήματα επικοινωνίας για την ασφάλεια του πλοίου, και τον εξοπλισμό και συστήματα παρακολούθησης για την ασφάλεια του πλοίου.

Η Αξιολόγηση Κινδύνου Πλοίου θα πρέπει να εκτιμήσει και λάβει υπόψη όλες τις πιθανές απειλές που ενδέχεται περιλαμβάνει την αλλοίωση φορτίου, βασικού εξοπλισμού πλοίου ή συστημάτων αποθήκευσης του πλοίου.

Η Αξιολόγηση Κινδύνου Πλοίου θα πρέπει να εκτιμήσει πιθανές ευπάθειες και τρωτά σημεία που μπορεί να περιλαμβάνουν τον εξοπλισμό και τα συστήματα ασφαλείας μέσα στα οποία ενυπάρχουν και τα συστήματα επικοινωνιών.

4.1.2 Σχέδιο Κινδύνου Πλοίου

Το Σχέδιο Κινδύνου Πλοίου θα πρέπει να περιγράφει λεπτομερώς τα συστήματα επικοινωνίας για να επιτραπεί η αποτελεσματική αλλά και συνεχής, συνάμα, επικοινωνία εντός του πλοίου αλλά και μεταξύ πλοίου και άλλων, περιλαμβανομένων και των λιμενικών εγκαταστάσεων.

4.1.3 Αξιολόγηση Κινδύνου Λιμενικής Εγκατάστασης

Η Αξιολόγηση Κινδύνου Λιμενικής Εγκατάστασης θα πρέπει να αντιμετωπίζει τα ραδιοσυστήματα και τα συστήματα τηλεπικοινωνιών περιλαμβανομένων των συστημάτων ηλεκτρονικών υπολογιστών και δικτύων.

Εκείνοι που εμπλέκονται στην Αξιολόγηση Κινδύνου Λιμενικής Εγκατάστασης θα πρέπει να μπορούν να υποστηρίζονται από εμπειρογνώμονες σχετικούς με τα ραδιοσυστήματα και τα συστήματα τηλεπικοινωνιών περιλαμβανομένων των συστημάτων ηλεκτρονικών υπολογιστών και δικτύων.

4.1.4 Σχέδιο Κινδύνου Λιμενικής Εγκατάστασης

Το Σχέδιο Κινδύνου Λιμενικής Εγκατάστασης πρέπει να προσδιορίζει λεπτομερώς τους αρμόδιους επικοινωνίας του λιμένα με τις υπόλοιπες αρχές καθώς και να είναι αποτελεσματικό σε οποιαδήποτέ ανάγκη μπορεί να προκύψει

Το Σχέδιο Κινδύνου Λιμενικής Εγκατάστασης πρέπει να καθορίζει τα συστήματα επικοινωνίας που παρέχονται για να επιτρέπεται η αποτελεσματική και συνεχής επικοινωνία μεταξύ του προσωπικού της λιμενικής εγκατάστασης, των πλοίων μέσα στο λιμένα και, κατά περίπτωση, με τις εθνικές ή τοπικές αρχές που έχουν επιφορτιστεί με ευθύνες ασφάλειας από έκνομες πράξεις.

4.2 Ο Κανονισμός 336/2004

Στον τομέα της ναυτιλίας, η Ευρωπαϊκή Ένωση έχοντας υπόψη τον κώδικα ISM, που υιοθετήθηκε από τον IMO το έτος 1994, ανέπτυξε τον Κανονισμό (EC) 336/2006 του Ευρωπαϊκού Κοινοβουλίου και Επιτροπής στις 15 Φεβρουαρίου του έτους 2006 (Regulation (EC) 336/2006). Στον κανονισμό αυτό δεν έχουν συμπεριληφθεί στοιχεία σχετικά με την κυβερνοασφάλεια. Οι ναυτιλιακές εταιρείες θα οφείλουν να αξιολογήσουν κινδύνους που αφορούν το πλοίο, το προσωπικό και το περιβάλλον και να καθιερώσουν τα κατάλληλα μέτρα ασφαλείας.

4.3 Η Στρατηγική Της Ε.Ε. Για Την Ασφαλεια Στη Θάλασσα

Η Ευρωπαϊκή Ένωση για να μπορέσει να ανταπεξέλθει στα προβλήματα από τον κυβερνοχώρο, μερίμνησε ώστε να γίνει μία πλατφόρμα, πάνω σε κοινά θέματα κυβερνοασφάλειας, για τα Κράτη-Μέλη της. Αρχικά, η Ευρωπαϊκή Ένωση είχε παραγκωνίσει και βάλει σε δεύτερη μοίρα την κυβερνοασφάλεια ως ζήτημα που σχετίζεται με την ολοένα και αυξανόμενη εξάρτηση από την τεχνολογία της πληροφορικής και των επικοινωνιών. Ωστόσο αυτή η κατάσταση άλλαξε άρδην μετά από μία μεγάλη, σε έκταση βλάβης, κυβερνοεπίθεση στην Εσθονία το έτος 2007.

Το 2013 η Στρατηγική Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης με το σύνθημα: «Ένας ανοικτός και ασφαλής Κυβερνοχώρος» επιχείρησε να εξηγήσει και να αποσαφηνίσει τις αρχές που καθοδηγούν την πολιτική κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Οι αρχές αυτές είναι πέντε (5) και εκφράζονται σε αντίστοιχα πέντε (5) στρατηγικές προτεραιότητες.

1. Επίτευξη ανθεκτικότητας στον κυβερνοχώρο
2. Μείωση του εγκλήματος στο διαδίκτυο
3. Ανάπτυξη πολιτικής άμυνας στον κυβερνοχώρο και δυνατότητες που σχετίζονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας (Common Security and Defense Policy – CSDP).
4. Ανάπτυξη των βιομηχανικών και τεχνολογικών πηγών για την κυβερνοασφάλειας.
5. Εγκαθίδρυση και παγίωση μιας συνεκτικής διεθνούς πολιτικής κυβερνοχώρου από την Ευρωπαϊκή Ένωση και προώθηση βασικών αξιών.

Μερικές από αυτές τις στρατηγικές προτεραιότητες συνοδεύονται με νομοθετικά εργαλεία.

Μερικά παραδείγματα για το πώς οι πέντε (5) προτεραιότητες μετατράπηκαν σε κανόνες ή σε προτάσεις κανόνων είναι τα παρακάτω:

- **Ανθεκτικότητα Δικτύου**
  - Κανονισμός 526/2013 που κατήργησε τον Κανονισμό (EC) No 260/2004.

- Οδηγία (EU) 2016/1148, Μέτρα για ένα κοινό υψηλό επίπεδο ασφάλειας στα δίκτυα και τα συστήματα πληροφοριών εντός της Ένωσης (NIS Directive).
- Το 2017, η Ευρωπαϊκή Επιτροπή (Europe Commission) πρότεινε τη δημιουργία ενός πλαισίου πιστοποίησης για τα προϊόντα τεχνολογιών πληροφορίας και επικοινωνιών. Ένα σχήμα πιστοποίησης κυβερνοασφάλειας θα αναγνωριστεί στην Ευρωπαϊκή Ένωση.

❖ **Έγκλημα στον Κυβερνοχώρο**
- Οδηγία 2011/92/EU, καταπολέμηση της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών και παιδική πορνογραφία και αντικατάσταση της Απόφασης Πλαίσιο του Συμβουλίου 2004/68/JHA.
- Οδηγία 2013/40/EU, Επιθέσεις εναντίον συστημάτων πληροφοριών και αντικατάσταση της Απόφασης Πλαίσιο του Συμβουλίου 2005/222/JHA.
- Οδηγία για την πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση απάτης και πλαστογραφία μη ταμειακών μέσων πληρωμής και αντικατάσταση της Απόφασης Πλαίσιο του Συμβουλίου 2001/413/JHA.

❖ **Προστασία Δεδομένων**
- Κανονισμός (EC) No 45/2001, Προστασία ατόμων σχετικά με την επεξεργασία προσωπικών δεδομένων από τα Κοινοτικά Ιδρύματα και Φορείς για ελεύθερη διακίνηση τέτοιων δεδομένων.
- Οδηγία 2002/58/EC, Επεξεργασία προσωπικών δεδομένων και προστασία του απορρήτου στον τομέα των ηλεκτρονικών επικοινωνιών.
- Κανονισμός (EU) 2016/679, Προστασία φυσικών προσώπων σχετικά με την επεξεργασία προσωπικών δεδομένων και για ελεύθερη διακίνηση τέτοιων δεδομένων, και κατάργηση της Οδηγίας 95/46/EC. (GDPR)

❖ **Εξωτερικές Σχέσεις**
- Η Ευρωπαϊκή Ένωση προωθεί έντονα τη θέση ότι η διεθνής νομοθεσία και ειδικότερα ο χάρτης των Ηνωμένων Εθνών ισχύει στον Κυβερνοχώρο. Η προσέγγιση είναι η αντιμετώπιση του εγκλήματος από τον Κυβερνοχώρο μέσω της Σύμβασης της Βουδαπέστης, που είναι ένα εργαλείο ανοικτό για υιοθέτηση από τρίτους.

4.4 Κυβερνοασφάλεια Στο Πλαίσιο Της Ε.Ε.

Το πρόβλημα της Κυβερνοασφάλειας στη θάλασσα είναι πολυσύνθετο και εμπλέκει πολλά ενδιαφερόμενα μέρη ανεξαρτήτως συνόρων και τομέα καθώς και το έργο και την προσπάθεια διαφορετικών διευθύνσεων, φορέων, γραφείων και υπηρεσιών εντός της Ευρωπαϊκής Ένωσης, και αυτό για να μειώσει και να μετριάσει τους κινδύνους από Κυβερνοεπιθέσεις. Επιπλέον, οι στρατηγικές για να αντιμετωπισθεί το ζήτημα είναι διασυνδεδεμένες μεταξύ τους. Για παράδειγμα η Στρατηγική για την Κυβερνοασφάλεια της Ευρωπαϊκής Ένωσης, η Στρατηγική της Ευρωπαϊκής Ένωσης για την Ασφάλεια ή η Εσωτερική Στρατηγική Ασφαλείας έχουν ληφθεί υπόψη κατά την ανάπτυξη της Ευρωπαϊκής Στρατηγικής Ασφαλείας για τη Θάλασσα (European Union Maritime Security Strategy - EUMSS).

Έχοντας αυτά υπόψη θα δούμε κάποιες λεπτομέρειες για την Ευρωπαϊκή Στρατηγική για την Ασφάλεια στη Ναυτιλία και για το σχέδιο δράσης της. Η αρχή έχει γίνει πιο πάνω με τον Κανονισμό 725/2004 και πιο κάτω θα προσθέσουμε την Ευρωπαϊκή Στρατηγική Ασφαλείας για τη Θάλασσα (European Union Maritime Security Strategy - EUMSS) και για το σχέδιο δράσης της.

Η Ευρωπαϊκή Στρατηγική Ασφαλείας για τη Θάλασσα (European Union Maritime Security Strategy - EUMSS) παρέχει το πολιτικό και στρατηγικό πλαίσιο για την αντιμετώπιση προκλήσεων ασφαλείας στη θάλασσα κάνοντας χρήση όλων των σχετικών εργαλείων σε διεθνές, Ευρωπαϊκής Ένωσης αλλά και εθνικό επίπεδο. Το αντικείμενο της στρατηγικής είναι η προστασία των συμφερόντων θαλάσσιας ασφάλειας της Ευρωπαϊκής Ένωσης και των κρατών μελών της εναντίον κινδύνων και απειλών στο παγκόσμιο ναυτιλιακό πεδίο.

Οι πέντε (5) βασικές περιοχές εφαρμογής είναι:

1. Εξωτερική Δράση.
2. Θαλάσσια ευαισθητοποίηση, αντίληψη, παρακολούθηση και διαμοιρασμός πληροφορίας.
3. Ανάπτυξη Δυνατοτήτων.
4. Διαχείριση Κινδύνου, Προστασία κρίσιμων θαλάσσιων υποδομών και αντιμετώπιση κρίσεων.
5. Θαλάσσια Έρευνα και Νεωτερισμός, Εκπαίδευση και Κατάρτιση.

Επίσης, η στρατηγική περιλαμβάνει μια περιγραφή των κινδύνων και των απειλών που έχουν ανιχνευθεί στη θάλασσα, περιλαμβανομένων μεταξύ άλλων, της τρομοκρατίας και άλλες σχετικές παράνομες δραστηριότητες στη θάλασσα και στους λιμένες εναντίον πλοίων, φορτίου, προσωπικού και επιβαινόντων, λιμένων και λιμενικών εγκαταστάσεων, κρίσιμων θαλάσσιων και ενεργειακών υποδομών. Μέσα στις απειλές και τους κινδύνους αυτούς εμπεριέχονται οι επιθέσεις από τον Κυβερνοχώρο.

Το Σχέδιο Δράσης της Στρατηγικής της Ευρωπαϊκής Ένωσης για την Ασφάλεια στη Θάλασσα είναι η εφαρμογή της στρατηγικής στην πράξη. Αυτό περιέχει έναν αριθμό δράσεων που σχετίζονται με κάθε ένα από τις πέντε (5) περιοχές ενδιαφέροντος της στρατηγικής και ειδικότερα στις ακόλουθες δραστηριότητες που αναφέρονται στην Κυβερνοασφάλεια:

1. Ικανότητα,
2. Διαχείριση Κινδύνου,

3. Προστασία κρίσιμων θαλάσσιων υποδομών και αντιμετώπιση κρίσεων,
4. Έρευνα θαλάσσιας ασφάλειας και νεοτερισμός,
5. Εκπαίδευση και Κατάρτιση.

5 ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ (BEST PRACTICES)

5.1 Οι Βέλτιστες Πρακτικές Της Bimco

Η BIMCO σε συνεργασία με τους ICS, INTERCARGO, INTERMANAGER, INTERTANGO, IUMI, OCIMF, WORLD SHIPPING COUNCIL, εξέδωσε σύνολο βέλτιστων πρακτικών για την Κυβερνοασφάλεια οι οποίες θα αναλυθούν παρακάτω.

5.1.1 Αναγνώριση Απειλών

Ο κίνδυνος στον κυβερνοχώρο αφορά την εταιρεία, το πλοίο, τη λειτουργία ή/και το εμπόριο. Κατά την αξιολόγηση του κινδύνου, οι εταιρείες θα πρέπει να εξετάζουν συγκεκριμένες πτυχές των δραστηριοτήτων τους που θα μπορούσαν να αυξήσουν την τρωτότητά τους σε περιστατικά κυβερνοεπίθεσης. Οι εμπειρίες στον ναυτιλιακό κλάδο και από άλλους επιχειρηματικούς τομείς, όπως τα χρηματοπιστωτικά ιδρύματα, η δημόσια διοίκηση και οι αεροπορικές μεταφορές, έχουν δείξει ότι οι επιτυχείς επιθέσεις στον κυβερνοχώρο ενδέχεται να οδηγήσουν σε σημαντική απώλεια υπηρεσιών. Τα ακόλουθα ενδεικτικά παραδείγματα παρέχουν ενδείξεις για τις απειλές και τις πιθανές συνέπειες για τις εταιρείες και τα πλοία που διαχειρίζονται:

Πίνακας 5.1 Κίνητρα και στόχοι ομάδων απειλών. Πηγή: https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

Ομάδες απειλών	Κίνητρο	Στόχος
Ακτιβιστές	• Ζημία στην φήμη της εταιρίας • Διακοπή των εργασιών	• Καταστροφή δεδομένων • Δημοσίευση ευαίσθητων δεδομένων • Προσοχή των ΜΜΕ • Άρνηση πρόσβασης στην υπηρεσία ή στο σύστημα στο οποίο απευθύνεται
Εγκληματίες	• Οικονομικό κέρδος • Εμπορική κατασκοπεία • Βιομηχανική κατασκοπεία	• Πώληση κλεμμένων δεδομένων • Λύτρα για τα κλεμμένα δεδομένα • Λύτρα για την επαναλειτουργία του συστήματος • Οργάνωση παράνομης μεταφοράς φορτίου • Συλλογή πληροφοριών για πιο εξελιγμένο έγκλημα, ακριβή θέση φορτίου, μεταφορά πλοίων και σχέδια χειρισμού κ.λπ.

Καιροσκόποι	• Η πρόκληση	• «Σπάσιμο» της διαδικτυακής άμυνας • Οικονομικό όφελος
Κρατικοί Οργανισμοί - Τρομοκράτες	• Πολιτικό όφελος • Κατασκοπεία	• Απόκτηση της τεχνογνωσίας • Διαταραχή της οικονομίας και κρίσιμων εθνικών υποδομών

Οι παραπάνω ομάδες απειλών είναι ικανές να απειλήσουν την ασφάλεια των πλοίων και την επιχειρηματικότητα μιας εταιρείας. Επιπλέον, υπάρχει η πιθανότητα το προσωπικό της εταιρείας, επί του πλοίου και στην ξηρά, να θέσει σε κίνδυνο τα συστήματα και τα δεδομένα του κυβερνοχώρου. Γενικά, η εταιρεία θα πρέπει να αντιλαμβάνεται ότι αυτό μπορεί να είναι ακούσιο και να προκαλείται από ανθρώπινο σφάλμα κατά τη λειτουργία και τη διαχείριση Πληροφοριακών Τεχνολογικών Συστημάτων και των Λειτουργικών Τεχνολογικών Συστημάτων ή από μη τήρηση των τεχνικών και διαδικαστικών μέτρων προστασίας. Υπάρχει, ωστόσο, η πιθανότητα οι ενέργειες να είναι κακόβουλες και να είναι μια σκόπιμη προσπάθεια από έναν δυσαρεστημένο εργαζόμενο που θέλει να βλάψει την εταιρεία και το πλοίο.

5.1.2 Τύποι Κυβερνοεπιθέσεων

Γενικά υπάρχουν δύο (2) κατηγορίες κυβερνοεπιθέσεων που μπορεί να επηρεάσουν τόσο τις εταιρίες όσο και το ίδιο το πλοίο:

- *Γενικές επιθέσεις*, όπου στόχος είναι τα συστήματα και τα δεδομένα μιας εταιρείας ή ενός πλοίου (Untargeted attacks).
- *Στοχευμένες επιθέσεις*, όταν τα συστήματα και τα δεδομένα μιας εταιρείας ή ενός πλοίου είναι ο επιδιωκόμενος στόχος (Targeted attacks).

Οι **μη στοχευμένες επιθέσεις** είναι πιθανό να χρησιμοποιήσουν εργαλεία και τεχνικές που είναι διαθέσιμες στο διαδίκτυο, τα οποία μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την εκμετάλλευση εκτεταμένων τρωτών σημείων που μπορεί να υπάρχουν σε μια εταιρεία και στο πλοίο. Παραδείγματα ορισμένων εργαλείων και τεχνικών που μπορούν να χρησιμοποιηθούν σε αυτές τις περιπτώσεις περιλαμβάνουν:

- *Malware (Malicious software)*: Κακόβουλο λογισμικό που έχει σχεδιαστεί για να έχει πρόσβαση χωρίς να έχει γνώση ο ιδιοκτήτης. Υπάρχουν διάφοροι τύποι κακόβουλου λογισμικού, συμπεριλαμβανομένων trojans, ransomware, spyware, ιούς, και worms. Το ransomware για παράδειγμα, κρυπτογραφεί τα δεδομένα για τα συστήματα μέχρι να καταβληθούν τα ζητούμενα λύτρα.

- Ο όρος *"εκμετάλλευση" (exploitation)* συνήθως αναφέρεται στη χρήση ενός λογισμικού ή κώδικα, ο οποίος έχει σχεδιαστεί για να εκμεταλλευτεί και να χειριστεί ένα πρόβλημα σε ένα άλλο λογισμικό ή υλικό κάποιου υπολογιστή. Αυτό μπορεί, για παράδειγμα, να είναι ένα σφάλμα κώδικα, ευπάθεια συστήματος, ακατάλληλη σχεδίαση, δυσλειτουργία υλικού ή/και σφάλμα στην υλοποίηση πρωτοκόλλου. Αυτά τα θέματα ευπάθειας ενδέχεται να αξιοποιηθούν απομακρυσμένα ή να ενεργοποιηθούν τοπικά.
- *Phishing (Ηλεκτρονικό «ψάρεμα»)*: Είναι η αποστολή e-mail σε μεγάλο αριθμό παραληπτών που ζητούν συγκεκριμένες πληροφορίες για ευαίσθητες ή εμπιστευτικές πληροφορίες. Ένα τέτοιο μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί επίσης να ζητήσει από ένα άτομο να επισκεφθεί έναν ψεύτικο ιστότοπο χρησιμοποιώντας έναν υπερσύνδεσμο (hyperlink) που περιλαμβάνεται σε μήνυμα ηλεκτρονικού ταχυδρομείου.
- *Water holing*: Το να δημιουργεί κάποιος ένα πλαστό δικτυακό τόπο ή να θέσει σε κίνδυνο μια πραγματική ιστοσελίδα για την εκμετάλλευση των επισκεπτών.
- *Scanning*: Επίθεση σε μεγάλα τμήματα-ομάδες του διαδικτύου τυχαία.

Οι **στοχευμένες επιθέσεις** μπορεί να είναι πιο εξελιγμένες και να χρησιμοποιούν εργαλεία και τεχνικές που δημιουργούνται ειδικά για τη στόχευση μιας εταιρείας ή ενός πλοίου. Παραδείγματα εργαλείων και τεχνικών, τα οποία μπορούν να χρησιμοποιηθούν σε αυτές τις περιπτώσεις, περιλαμβάνουν:

- *Social engineering (Κοινωνική μηχανική)* Μια τεχνική που χρησιμοποιείται από εισβολείς στον κυβερνοχώρο για να αντλήσουν εμπιστευτικές πληροφορίες και να σπάσουν τις διαδικασίες ασφαλείας. Συνήθως γίνεται μέσω των μέσων κοινωνικής δικτύωσης.
- *Brute force (Ωμή βία)* Μια επίθεση η οποία, μέσω επαναλαμβανόμενης διαδικασίας, ο εισβολέας δοκιμάζει πολλούς κωδικούς πρόσβασης ελπίζοντας να πετύχει τον σωστό. Ο εισβολέας ελέγχει συστηματικά όλους τους πιθανούς κωδικούς πρόσβασης μέχρι να βρεθεί ο σωστός.
- *Denial of service (DoS) (Άρνηση υπηρεσίας)* Γίνεται άρνηση εισόδου σε όλους τους νόμιμους και εξουσιοδοτημένους χρήστες, έτσι ώστε να μην μπορούν να έχουν πρόσβαση σε πληροφορίες, συνήθως «πλημμυρίζοντας» ένα δίκτυο με δεδομένα. Μια επίθεση κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service - DDoS)

αναλαμβάνει τον έλεγχο πολλών υπολογιστών ή/και διακομιστών (servers) για πραγματοποιηθεί DoS επίθεση.

- *Spear-phishing* Είναι όπως το ηλεκτρονικό ψάρεμα (phishing), αλλά στα θύματα στέλνονται προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία συχνά περιέχουν κακόβουλο λογισμικό ή συνδέσεις που κάνουν αυτόματη λήψη κακόβουλου λογισμικού.
- *Subverting the supply chain (Ανατροπή της εφοδιαστικής αλυσίδας)* Επίθεση σε μια εταιρεία ή πλοίο με ψευδή υπόσχεση παράδοσης εξοπλισμού, λογισμικού ή υποστηρικτικών υπηρεσιών στην εταιρεία ή το πλοίο.

Τα παραπάνω παραδείγματα δεν περιγράφουν όλες τις μεθόδους κυβερνοεπίθεσης. Καινούργιες μέθοδοι εξελίσσονται, όπως η απομίμηση ενός νόμιμου υπαλλήλου με έδρα την ξηρά σε μια ναυτιλιακή εταιρεία για να λάβει πολύτιμες πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν για μια περαιτέρω επίθεση. Ο δυνητικός αριθμός και η πολυπλοκότητα των εργαλείων και των τεχνικών που χρησιμοποιούνται στις επιθέσεις στον κυβερνοχώρο εξακολουθούν να εξελίσσονται και περιορίζονται μόνο από την εφευρετικότητα των οργανισμών και των ατόμων που τις αναπτύσσουν.

5.1.3 Στάδια Κυβερνοεπίθεσης

Η εισβολή μπορεί να περάσει απαρατήρητη ακόμα και για χρόνια. Ο αριθμός αυτός ήταν κάτω από 205 ημέρες το 2015 και συνεχίζει να μειώνεται, επειδή η ανίχνευση τεχνολογικά βελτιώνεται. Το 2018, χρειάστηκαν κατά μέσο όρο 140 ημέρες μεταξύ της στιγμής που μολύνθηκε το δίκτυο ενός θύματος και της ανακάλυψης της κυβερνοεπίθεσης. Το χρονικό διάστημα για την προετοιμασία μιας κυβερνοεπίθεσης μπορεί να καθοριστεί από τα κίνητρα και τους στόχους του επιτιθέμενου, καθώς και από την ανθεκτικότητα των τεχνικών και των διαδικαστικών ελέγχων στον κυβερνοχώρο που εφαρμόζει η εταιρεία, συμπεριλαμβανομένων και εκείνων που εφαρμόζονται στα πλοία της. Κατά την εξέταση στοχευμένων επιθέσεων στον κυβερνοχώρο, τα γενικά στάδια μιας επίθεσης είναι:

- *Survey-reconnaissance (Έρευνα-αναγνώριση)* Οι ανοικτές/δημόσιες πηγές χρησιμοποιούνται για να αποκτήσουν πληροφορίες σχετικά με μια εταιρεία, ένα πλοίο ή έναν ναυτικό στο πλαίσιο της προετοιμασίας μιας κυβερνοεπίθεσης. Τα μέσα κοινωνικής δικτύωσης, τα τεχνικά φόρουμ και οι κρυφές ιδιότητες σε ιστοσελίδες, έγγραφα και

δημοσιεύσεις μπορούν να χρησιμοποιηθούν για τον εντοπισμό τεχνικών, διαδικασιών και φυσικών τρωτών σημείων. Η χρήση ανοικτών/δημόσιων πηγών μπορεί να συμπληρωθεί με την παρακολούθηση (sniffing) των πραγματικών δεδομένων που προέρχονται από και προς μια εταιρεία ή ένα πλοίο.

- *Delivery (Παράδοση)* Οι επιτιθέμενοι ενδέχεται να προσπαθήσουν να αποκτήσουν πρόσβαση στα συστήματα και τα δεδομένα της εταιρείας και του πλοίου. Αυτό μπορεί να γίνει είτε εντός της εταιρείας ή του πλοίου ή εξ αποστάσεως μέσω της σύνδεσης με το διαδίκτυο. Παραδείγματα μεθόδων που χρησιμοποιούνται για την πρόσβαση περιλαμβάνουν:
    - Ηλεκτρονικές υπηρεσίες on-line της εταιρείας, συμπεριλαμβανομένων των συστημάτων παρακολούθησης φορτίου ή εμπορευματοκιβωτίων.
    - Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν κακόβουλα αρχεία ή συνδέσεις σε κακόβουλους ιστότοπους στο προσωπικό της εταιρίας ή του πλοίου.
    - Παροχή μολυσμένων αφαιρούμενων μέσων (π.χ. usb stick), ως μέρος μιας ενημερωμένης έκδοσης λογισμικού σε λογισμικό ενός συστήματος στο πλοίο.
    - Δημιουργία ψευδών ή παραπλανητικών ιστότοπων, οι οποίοι αποσκοπούν στην αποκάλυψη των πληροφοριών του λογαριασμού του χρήστη.

- *Breach (Παραβίαση)* Το κατά πόσο ο επιτιθέμενος μπορεί να παραβιάσει το σύστημα μιας εταιρείας ή του πλοίου θα εξαρτηθεί από τη σημασία της ευπάθειας που εντόπισε, και τη μέθοδο που έχει επιλεγεί για την "παράδοση" μιας απειλής. Θα πρέπει να σημειωθεί ότι μια παραβίαση μπορεί να μην οδηγήσει σε προφανείς αλλαγές στο καθεστώς του εξοπλισμού. Ανάλογα με τη σημασία της παραβίασης, ο επιτιθέμενος μπορεί να είναι σε θέση να:
    - Κάνει αλλαγές που επηρεάζουν τη λειτουργία του συστήματος, για παράδειγμα, να διακόπτει ή να χειρίζεται πληροφορίες που χρησιμοποιούνται από εξοπλισμό πλοήγησης ή να τροποποιήσει σημαντικές πληροφορίες, όπως τις λίστες φόρτωσης.

- Αποκτήσει πρόσβαση σε εμπορικά ευαίσθητα δεδομένα, όπως δηλωτικά φορτίου ή/και λίστες πληρώματος και επιβατών/επισκεπτών.
- Να αποκτήσει τον πλήρη έλεγχο ενός συστήματος, για παράδειγμα ενός συστήματος διαχείρισης μηχανημάτων.

- *Pivot / Pivoting* είναι η τεχνική της χρήσης ενός ήδη εγκατεστημένου ιού που έχει ήδη εγκατασταθεί στο σύστημα με σκοπό να "κινηθεί" και να εκτελέσει και άλλες δραστηριότητες. Κατά τη διάρκεια αυτής της επίθεσης, ένας εισβολέας χρησιμοποιεί το πρώτο σύστημα που έχει παραβιαστεί για να επιτεθεί σε συστήματα που δεν είναι προσβάσιμα. Ένας εισβολέας θα στοχεύει συνήθως το πιο ευάλωτο μέρος του συστήματος του θύματος με το χαμηλότερο επίπεδο ασφάλειας. Μόλις αποκτηθεί η πρόσβαση, τότε ο εισβολέας θα προσπαθήσει να εκμεταλλευτεί το υπόλοιπο σύστημα. Συνήθως, στη φάση του pivoting, ο εισβολέας μπορεί να προσπαθήσει να:
  - ανεβάσει εργαλεία ή λογισμικά στο υπό επίθεση σύστημα, τα οποία υποστηρίζουν τον εισβολέα στη νέα επίθεση (pivot),
  - ανακαλύψει «γειτονικά» συστήματα χρησιμοποιώντας εργαλεία σάρωσης ή χαρτογράφησης δικτύου για να αποκτήσει πρόσβαση σε αυτά,
  - να εγκαταστήσει μόνιμα εργαλεία ή μια κλειδοθήκη κωδικών πρόσβασης (key logger) , για να διατηρήσει πρόσβαση στο σύστημα,
  - εκτελέσει εκ νέου επίθεση στο σύστημα.

Τα κίνητρα και οι στόχοι του επιτιθέμενου θα καθορίσουν την επίδραση που θα έχουν στην εταιρεία ή στο σύστημα και στα δεδομένα του πλοίου. Ο επιτιθέμενος μπορεί να:

- Αποκτήσει πρόσβαση σε εμπορικά ευαίσθητα ή εμπιστευτικά δεδομένα σχετικά με το φορτίο, το πλήρωμα, τους επισκέπτες και τους επιβάτες
- Παραποιήσει τους καταλόγους πληρώματος ή επιβατών/επισκεπτών, δηλωτικά φορτίου ή πίνακες φόρτωσης. Αυτό μπορεί στη συνέχεια να χρησιμοποιηθεί για να επιτραπεί η παράνομη μεταφορά φορτίου ή η κλοπή φορτίου,
- Προκαλέσει την αδυναμία μιας υπηρεσίας,

- Υποβοηθήσει πειρατείες ή ναυταπάτες
- Διαταράξει την κανονική λειτουργία της εταιρείας και των συστημάτων των πλοίων, για παράδειγμα διαγράφοντας πληροφορίες άφιξης του πλοίου σε ένα λιμάνι ή υπερφορτώνοντας τα συστήματα της εταιρείας με αποτέλεσμα να πέσει το δίκτυο της.

5.1.4 Αναγνώριση Αδυναμιών

Συνιστάται μια ναυτιλιακή εταιρεία να διενεργεί αρχικά αξιολόγηση των πιθανών απειλών που μπορεί να αντιμετωπιστούν. Αυτή θα πρέπει να ακολουθείται από αξιολόγηση των συστημάτων και των διαδικασιών επί του πλοίου για τη χαρτογράφηση της ευρωστίας και τους για την αντιμετώπιση του τρέχοντος επιπέδου απειλής. Μπορεί να γίνει είτε από εσωτερικούς εμπειρογνώμονες ή να υποστηρίζεται από εξωτερικούς εμπειρογνώμονες με γνώση της ναυτιλιακής βιομηχανίας και των βασικών διαδικασιών της. Το αποτέλεσμα θα πρέπει να είναι μια στρατηγική που θα επικεντρώνεται στους βασικούς κινδύνους.

Τα αυτόνομα συστήματα θα είναι λιγότερο ευάλωτα σε εξωτερικές κυβερνοεπιθέσεις σε σύγκριση με εκείνα που συνδέονται με τοπικά δίκτυα ή απευθείας στο διαδίκτυο. Θα πρέπει να λαμβάνεται μέριμνα για την κατανόηση του τρόπου με τον οποίο τα κρίσιμα συστήματα επί του πλοίου ενδέχεται να συνδέονται σε μη ελεγχόμενα δίκτυα. Κατά τον τρόπο αυτό, θα πρέπει να λαμβάνεται υπόψη το ανθρώπινο στοιχείο, καθώς πολλά περιστατικά προκαλούνται από τις ενέργειες του προσωπικού. Τα συστήματα επί του πλοίου θα μπορούσαν να περιλαμβάνουν:

- ***Συστήματα διαχείρισης φορτίου***. Τα ψηφιακά συστήματα που χρησιμοποιούνται για τη φόρτωση, τη διαχείριση και τον έλεγχο του φορτίου, συμπεριλαμβανομένου του επικίνδυνου φορτίου, μπορούν να διασυνδέονται με διάφορα συστήματα στην ξηρά, συμπεριλαμβανομένων των λιμένων και των θαλάσσιων τερματικών σταθμών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν εργαλεία παρακολούθησης αποστολών που διατίθενται στους αποστολείς μέσω του διαδικτύου. Ωστόσο, η παρακολούθηση γίνεται συνήθως μέσω των συστημάτων της εταιρείας που συνδέονται με το πλοίο και όχι απευθείας μεταξύ του αποστολέα και του πλοίου. Οι διεπαφές αυτές καθιστούν ευάλωτα τα συστήματα διαχείρισης φορτίου και τα δεδομένα σε δηλωτικά φορτίου και πίνακες φόρτωσης σε επιθέσεις στον κυβερνοχώρο.
- ***Συστήματα γέφυρας***. Η αυξανόμενη χρήση ψηφιακών συστημάτων πλοήγησης δικτύου, με διασυνδέσεις σε δίκτυα εδάφους για την ενημέρωση και την παροχή υπηρεσιών,

καθιστά τα συστήματα αυτά ευάλωτα σε επιθέσεις στον κυβερνοχώρο. Τα συστήματα γέφυρας που δεν είναι συνδεδεμένα σε άλλα δίκτυα ενδέχεται να είναι εξίσου ευάλωτα, καθώς τα αφαιρούμενα μέσα χρησιμοποιούνται συχνά για την ενημέρωση τέτοιων συστημάτων από άλλα ελεγχόμενα ή μη ελεγχόμενα δίκτυα. Ένα περιστατικό στον κυβερνοχώρο μπορεί να επεκταθεί σε άρνηση ή χειραγώγηση υπηρεσίας και, ως εκ τούτου, μπορεί να επηρεάσει όλα τα ηλεκτρονικά συστήματα που σχετίζονται με την πλοήγηση.

- ***Σύστημα διαχείρισης πρόωσης και ελέγχου ισχύος***. Η χρήση των ψηφιακών συστημάτων τα οποία χρησιμεύουν για την παρακολούθηση και τον έλεγχο των επί του πλοίου μηχανημάτων τα οποία είναι υπεύθυνα για την πρόωση και την πλοήγηση, τα καθιστά ευάλωτα σε επιθέσεις. Η ευπάθεια αυτών των συστημάτων μπορεί να αυξηθεί όταν χρησιμοποιούνται σε συνδυασμό με απομακρυσμένη παρακολούθηση (Remote access).

- ***Συστήματα ελέγχου πρόσβασης***. Τα συστήματα τα οποία χρησιμοποιούνται για την υποστήριξη του ελέγχου πρόσβασης και τη εξασφάλιση της ασφάλειας ενός πλοίου και του φορτίου του, συμπεριλαμβανομένης την παρακολούθηση του (CCTV), του συστήματος ασφαλείας των μηχανών και των βοηθητικών αλλά και των ηλεκτρονικών συστημάτων είναι ευάλωτα σε επιθέσεις στον κυβερνοχώρο.
- ***Συστήματα εξυπηρέτησης και διαχείρισης επιβατών***. Τα ψηφιακά συστήματα που χρησιμοποιούνται για τη διαχείριση του πλοίου, την επιβίβαση επιβατών και τον έλεγχο πρόσβασης ενδέχεται να διαθέτουν πολύτιμα δεδομένα που σχετίζονται με τους επιβάτες. Οι έξυπνες συσκευές (tablets, φορητοί σαρωτές κ.λπ.) μπορεί να καταστούν, εν αγνοία των χρηστών τους, μέσο για να αποκτήσει πρόσβαση ο επιτιθέμενος, καθώς τελικά τα δεδομένα που συλλέγονται διαβιβάζονται σε άλλα συστήματα.
- ***Τα δημόσια δίκτυα που συνδέονται οι επιβάτες***. Τα σταθερά ή ασύρματα δίκτυα που είναι εγκατεστημένα επί του πλοίου προς όφελος των επιβατών, θα πρέπει να θεωρούνται ανασφαλή και δεν θα πρέπει να συνδέονται με κανένα σύστημα ζωτικής σημασίας για την ασφάλεια επί του πλοίου.
- ***Διοικητικά συστήματα και συστήματα ευημερίας του πληρώματος***. Τα δίκτυα υπολογιστών επί του πλοίου που χρησιμοποιούνται για τη διαχείριση του πλοίου είναι ιδιαίτερα ευάλωτα όταν οι χρήστες είναι στο διαδίκτυο ή κάνουν σύνδεση στο ηλεκτρονικό τους ταχυδρομείο. Αυτό μπορεί να αξιοποιηθεί από τους εισβολείς στον κυβερνοχώρο για

να αποκτήσουν πρόσβαση σε συστήματα και δεδομένα επί του πλοίου. Τα συστήματα αυτά θα πρέπει επίσης να θεωρούνται ανασφαλή και δεν θα πρέπει να συνδέονται με κανένα σύστημα ζωτικής σημασίας για την ασφάλεια επί του πλοίου. Το λογισμικό που παρέχεται από εταιρείες διαχείρισης πλοίων ή ιδιοκτήτες περιλαμβάνεται επίσης σε αυτή την κατηγορία.

- ***Συστήματα επικοινωνίας***. Η διαθεσιμότητα σύνδεσης στο διαδίκτυο μέσω δορυφορικής ή/και άλλης ασύρματης επικοινωνίας μπορεί να αυξήσει την ευπάθεια των πλοίων. Ο πάροχος των δορυφορικών επικοινωνιών, παρέχει προγράμματα (antivirus, malware) τα οποία εξασφαλίζουν την ασφάλεια στο διαδίκτυο, αλλά δεν θα πρέπει να εξαρτώνται μόνο από αυτά όσον αφορά τη διασφάλιση των συστημάτων και δεδομένων επί του πλοίου. Στα συστήματα αυτά περιλαμβάνονται συνδέσεις επικοινωνίας με δημόσιες αρχές για τη διαβίβαση των απαιτούμενων πληροφοριών υποβολής εκθέσεων πλοίων. Οι εν λόγω αρχές θα πρέπει να τηρούν αυστηρά τις ισχύουσες απαιτήσεις ελέγχου ταυτότητας και διαχείρισης ελέγχου πρόσβασης.

5.1.5 Διασύνδεση Πλοίου – Ξηράς

Τα πλοία ενσωματώνονται και συγχρονίζονται όλο και περισσότερο με τις λειτουργίες στην ξηρά, επειδή η επικοινωνία χρησιμοποιείται για τη διεξαγωγή επιχειρηματικών δραστηριοτήτων, αλλά και για τη διαχείριση των λειτουργιών και τη διατήρηση επαφής με τα κεντρικά γραφεία. Ακόμα, τα συστήματα πλοίων που είναι απαραίτητα για την ασφάλεια της ναυσιπλοΐας, και της διαχείρισης του φορτίου έχουν ψηφιοποιηθεί και συνδέονται στο διαδίκτυο για την εκτέλεση ενός μεγάλου εύρους λειτουργιών, όπως:

- Παρακολούθηση της απόδοσης του κινητήρα.
- Διαχείριση των ανταλλακτικών και των αναλωσίμων.
- Φορτίο, φορτοεκφόρτωση, λειτουργία των γερανών και των αντλιών αλλά και τον σχεδιασμό στοιβασίας.
- Την παρακολούθηση των επιδόσεων του ταξιδιού.

Τα παραπάνω συστήματα παρέχουν δεδομένα, τα οποία μπορεί να ενδιαφέρουν τους εγκληματίες του κυβερνοχώρου και οι καινούργιες τεχνολογίες μπορούν να βρουν τρωτά σημεία στην ασφάλεια των πλοίων, ιδίως εάν υπάρχουν ανασφαλή σχέδια δικτύων και ανεξέλεγκτη πρόσβαση στο διαδίκτυο. Επιπλέον, το προσωπικό στην ξηρά και επί του πλοίου ενδέχεται να μην γνωρίζει

τον τρόπο με τον οποίο ορισμένοι κατασκευαστές διατηρούν απομακρυσμένη πρόσβαση στον εξοπλισμό επί του πλοίου και στο σύστημα δικτύου του. Ως σημαντικό μέρος της εκτίμησης κινδύνου θα πρέπει να λαμβάνεται υπόψη η άγνωστη και ασυντόνιστη απομακρυσμένη πρόσβαση σε ένα πλοίο.

Συνιστάται στις εταιρείες να κατανοούν πλήρως τα Λειτουργικά και Πληροφοριακά Τεχνολογικά Συστήματα του πλοίου και τον τρόπο με τον οποίο τα συστήματα αυτά συνδέονται και ενσωματώνονται με την πλευρά της ξηράς, συμπεριλαμβανομένων των δημόσιων αρχών και των τερματικών σταθμών. Αυτό απαιτεί την κατανόηση όλων των συστημάτων που βασίζονται σε υπολογιστή επί του πλοίου και πώς η ασφάλεια, οι λειτουργίες και οι επιχειρήσεις μπορούν να τεθούν σε κίνδυνο από ένα περιστατικό στον κυβερνοχώρο. Όσον αφορά τους κατασκευαστές, τους αναδόχους εργασιών και των παρόχων υπηρεσιών, θα πρέπει να εξετάζονται τα ακόλουθα:

- Ευαισθητοποίηση και διαδικασίες διαχείρισης κινδύνων στον κυβερνοχώρο του κατασκευαστή και του παρόχου υπηρεσιών: Οι εταιρείες αυτές ενδέχεται να μην διαθέτουν εκπαίδευση στον κυβερνοχώρο στους δικούς τους οργανισμούς και αυτό μπορεί να αντιπροσωπεύει περισσότερες πηγές ευπάθειας, οι οποίες θα μπορούσαν να οδηγήσουν σε κυβερνοεπιθέσεις. Οι εταιρείες αυτές, επίσης, θα πρέπει να διαθέτουν επικαιροποιημένη πολιτική της εταιρείας διαχείρισης κινδύνων στον κυβερνοχώρο, η οποία θα περιλαμβάνει διαδικασίες κατάρτισης και διακυβέρνησης για προσβάσιμα Λειτουργικά και Πληροφοριακά Τεχνολογικά Συστήματα.
- Την ωριμότητα των διαδικασιών διαχείρισης κινδύνων στον κυβερνοχώρο: Ο πλοιοκτήτης θα πρέπει να υποβάλει ερωτήματα για την εσωτερική διακυβέρνηση της ασφάλειας του δικτύου στον κυβερνοχώρο και να επιδιώξει να λάβει διασφάλιση διαχείρισης κινδύνου στον κυβερνοχώρο κατά την εξέταση μελλοντικών συμβάσεων και υπηρεσιών. Αυτό είναι ιδιαίτερα σημαντικό όταν καλύπτεται η ασφάλεια του δικτύου, εάν το πλοίο πρόκειται να διασυνδεθεί με το τρίτο μέρος, όπως ένα τερματικό σταθμό.

5.1.6 Κοινά Τρωτά Σημεία

Τα παρακάτω σημεία, τα οποία υπάρχουν σε παλαιότερα πλοία, αλλά και σε ορισμένα νεότευκτα είναι εξίσου ευάλωτα σε διαδικτυακές επιθέσεις:

- Απαρχαιωμένα και μη υποστηριζόμενα λειτουργικά συστήματα.

- Απαρχαιωμένο λογισμικό ή έλλειψη λογισμικού προστασίας από ιούς και προστασία από κακόβουλο λογισμικό.
- Ανεπαρκείς ρυθμίσεις παραμέτρων και βέλτιστων πρακτικών ασφαλείας, συμπεριλαμβανομένης της αναποτελεσματικής διαχείρισης δικτύου και της χρήσης προεπιλεγμένων κωδικών πρόσβασης.
- Δίκτυο υπολογιστών επί του πλοίου το οποίο δεν διαθέτει μέτρα προστασίας και κατανομής του δικτύου.
- Εξοπλισμός ασφαλείας ή συστήματα μονίμως συνδεδεμένα με την ξηρά.
- Ελλιπείς έλεγχοι πρόσβασης, συμπεριλαμβανομένων των κατασκευαστών και των παρόχων υπηρεσιών.

5.1.7 Αξιολόγηση Έκθεσης Κινδύνου

Η Αξιολόγηση Κινδύνου από τον Κυβερνοχώρο πρέπει να ξεκινήσει από ανώτερο διοικητικό επίπεδο μιας εταιρείας, αντί να ανατεθεί αμέσως στον αξιωματικό ασφάλειας του πλοίου ή στον προϊστάμενο του Τμήματος Πληροφορικής. Υπάρχουν διάφοροι λόγοι για αυτό όπως:

1. Πρωτοβουλίες για την ενίσχυση της ασφάλειας και της ασφάλειας από έκνομες πράξεις στον κυβερνοχώρο μπορεί ταυτόχρονα να επηρεάσουν τις συνήθεις επιχειρηματικές διαδικασίες και λειτουργίες, καθιστώντας τις πιο χρονοβόρες ή/και δαπανηρές. Ως εκ τούτου, είναι απόφαση ανώτερου διοικητικού επιπέδου να αξιολογεί και να αποφασίζει για τον μετριασμό των κινδύνων.
2. Ορισμένες πρωτοβουλίες, οι οποίες θα βελτιώσουν τη διαχείριση των κινδύνων στον κυβερνοχώρο, σχετίζονται με τις επιχειρηματικές διαδικασίες, την κατάρτιση, την ασφάλεια του πλοίου και του περιβάλλοντος και όχι με τα συστήματα πληροφορικής και, ως εκ τούτου, πρέπει να βασιστούν οργανωτικά εκτός του Τμήματος Πληροφορικής.
3. Πρωτοβουλίες που αυξάνουν την ευαισθητοποίηση στον κυβερνοχώρο μπορεί να αλλάξουν τον τρόπο με τον οποίο η εταιρεία αλληλοεπιδρά με τους πελάτες, τους προμηθευτές και τις αρχές, και να επιβάλουν νέες απαιτήσεις για τη συνεργασία μεταξύ των μερών. Είναι μια απόφαση ανώτερου επιπέδου διοίκησης εάν και πώς να οδηγήσει αυτές τις αλλαγές στις σχέσεις.

Οι ακόλουθες ερωτήσεις μπορούν να χρησιμοποιηθούν ως βάση για την αξιολόγηση κινδύνου κατά την αντιμετώπιση των κινδύνων στον κυβερνοχώρο επί των πλοίων:

- Ποια περιουσιακά στοιχεία είναι σε κίνδυνο;
- Ποιος είναι ο πιθανός αντίκτυπος και επίπτωση ενός περιστατικού του Κυβερνοχώρου;
- Ποιος έχει την τελική ευθύνη για τη διαχείριση των κινδύνων στον κυβερνοχώρο;
- Τα Λειτουργικά Τεχνολογικά Συστήματα (OT Systems) και το περιβάλλον εργασίας τους προστατεύονται από το διαδίκτυο;
- Υπάρχει απομακρυσμένη πρόσβαση στα Λειτουργικά Τεχνολογικά Συστήματα (OT Systems), και αν ναι πώς παρακολουθείται και προστατεύεται;
- Τα Πληροφοριακά Τεχνολογικά Συστήματα (IT Systems) προστατεύονται και η απομακρυσμένη πρόσβαση διαχειρίζεται και παρακολουθείται;
- Ποιες βέλτιστες πρακτικές διαχείρισης κινδύνων στον κυβερνοχώρο χρησιμοποιούνται;
- Ποιο είναι το επίπεδο εκπαίδευσης του προσωπικού που χειρίζεται τα Πληροφοριακά Τεχνολογικά Συστήματα (IT Systems) και τα Λειτουργικά Τεχνολογικά Συστήματα (OT Systems);

Βασιζόμενοι στις απαντήσεις, των παραπάνω ερωτημάτων, η εταιρεία πρέπει να αναθέσει την αρμοδιότητα και να διαθέσει τον προϋπολογισμό που απαιτείται για τη διενέργεια πλήρους εκτίμησης κινδύνου και την ανάπτυξη λύσεων που είναι καταλληλότερες για την εταιρεία και τη λειτουργία των πλοίων τους. Θα πρέπει να αντιμετωπιστούν τα ακόλουθα:

- Ανίχνευση συστημάτων που είναι σημαντικά για τη λειτουργία, την ασφάλεια και την προστασία του περιβάλλοντος.
- Αντιστοίχιση των προσώπων που είναι υπεύθυνα να θέσουν πολιτικές Κυβερνοχώρου, διαδικασίες και επιβολή για παρακολούθηση.
- Καθορισμός για το πού θα πρέπει να χρησιμοποιεί η ασφαλής απομακρυσμένη πρόσβαση πολλαπλά επίπεδα άμυνας και πού θα πρέπει να αποσυνδεθεί η προστασία των δικτύων από το Διαδίκτυο.

Το επίπεδο του κινδύνου από τον Κυβερνοχώρο θα αντικατοπτρίζει τις συνθήκες της εταιρείας, του πλοίου (της λειτουργίας και του εμπορίου που φέρει), των Λειτουργικών αλλά και των Πληροφοριακών Τεχνολογικών Συστημάτων που χρησιμοποιούνται, καθώς και των πληροφοριών ή/και των αποθηκευμένων δεδομένων. Ο ναυτιλιακός κλάδος διαθέτει μια σειρά χαρακτηριστικών, τα οποία επηρεάζουν την ευπάθειά του σε περιστατικά από τον Κυβερνοχώρο μερικά από τα οποία είναι:

- Οι έλεγχοι στον κυβερνοχώρο που έχουν ήδη εφαρμοστεί από την εταιρεία επί των πλοίων της.
- Πλήθος ενδιαφερομένων εμπλέκεται συχνά στη λειτουργία και τη ναύλωση ενός πλοίου με πιθανό αποτέλεσμα την έλλειψη ανάληψης ευθυνών για την υποδομή πληροφορικής.
- Το πλοίο που είναι σε απευθείας σύνδεση και πώς διασυνδέεται με άλλα μέρη της παγκόσμιας εφοδιαστικής αλυσίδας.
- Εξοπλισμός πλοίων που παρακολουθείται εξ αποστάσεως, π.χ. από τους κατασκευαστές.
- Πληροφορία κρίσιμη για τις επιχειρήσεις, ευαίσθητη σε δεδομένα και ευαίσθητη εμπορικά που διαμοιράζεται και κοινοποιείται σε προμηθευτές υπηρεσιών ξηράς περιλαμβανομένων των θαλάσσιων τερματικών σταθμών και επίσης, κατά περίπτωση, των δημόσιων αρχών.
- Η διαθεσιμότητα και η χρήση κρίσιμων συστημάτων που ελέγχονται από υπολογιστή για την ασφάλεια του πλοίου και για την προστασία του περιβάλλοντος

Τα στοιχεία αυτά θα πρέπει να λαμβάνονται υπόψη και τα σχετικά μέρη να ενσωματώνονται στις πολιτικές της εταιρείας για την ασφάλεια στον κυβερνοχώρο, στα συστήματα διαχείρισης της ασφάλειας και στα σχέδια ασφάλειας των πλοίων. Οι χρήστες των παρουσών κατευθυντήριων γραμμών θα πρέπει να αναφέρονται σε ειδικούς εθνικούς, διεθνείς κανονισμούς και κανονισμούς του κράτους σημαίας, καθώς και σε σχετικά διεθνή και βιομηχανικά πρότυπα και βέλτιστες πρακτικές κατά την ανάπτυξη και εφαρμογή διαδικασιών διαχείρισης κινδύνων στον κυβερνοχώρο. Τα Πληροφοριακά και τα Λειτουργικά Τεχνολογικά Συστήματα, το λογισμικό και η συντήρηση μπορούν να ανατεθούν σε τρίτους προμηθευτές υπηρεσιών και η ίδια η εταιρεία ενδέχεται να μην διαθέτει τρόπο επαλήθευσης του επιπέδου ασφάλειας που παρέχεται από αυτούς (τους προμηθευτές). Ορισμένες εταιρείες χρησιμοποιούν διαφορετικούς προμηθευτές που είναι υπεύθυνοι για τους ελέγχους λογισμικού και ασφάλειας στον κυβερνοχώρο. Η αυξανόμενη χρήση των μαζικών δεδομένων, των έξυπνων πλοίων και του «διαδικτύου των πραγμάτων» (Internet of Things – IoT) θα αυξήσει την ποσότητα των πληροφοριών που είναι διαθέσιμες στους εισβολείς στον κυβερνοχώρο και το πιθανό εύρος επίθεσης σε αυτούς. Αυτό καθιστά σημαντική την ανάγκη για ισχυρές προσεγγίσεις για τη διαχείριση των κινδύνων στον κυβερνοχώρο τόσο τώρα όσο και στο μέλλον.

5.1.8 Πρόσβαση Από Τρίτους

Οι επισκέψεις σε πλοία από τρίτους που απαιτούν σύνδεση με έναν ή περισσότερους υπολογιστές επί του πλοίου μπορούν επίσης να οδηγήσουν στη σύνδεση του πλοίου με την ξηρά. Είναι σύνηθες για τεχνικούς, πωλητές, υπαλλήλους λιμένων, εκπροσώπους θαλάσσιων τερματικών σταθμών, πράκτορες, πιλότους, τελωνειακούς υπάλληλους ή αξιωματικοί ελέγχου του κράτους του λιμένα, να επιβιβάζονται στο πλοίο και να συνδέουν συσκευές, όπως φορητούς υπολογιστές και tablet για διάφορες εργασίες ή ακόμη και για εκτύπωση εγγράφων. Ορισμένοι τεχνικοί ενδέχεται να απαιτούν τη χρήση αφαιρούμενων μέσων αποθήκευσης (Removable Data Units) για την ενημέρωση υπολογιστών, τη λήψη δεδομένων ή/και την εκτέλεση άλλων εργασιών.

Μερικές φορές δεν υπάρχει κανένας έλεγχος ως προς το ποιος έχει πρόσβαση στα συστήματα επί του πλοίου, π.χ. κατά την ανάληψη ενός νέου ή υπάρχοντος πλοίου. Σε αυτές τις περιπτώσεις, είναι δύσκολο να γνωρίζουμε αν κακόβουλο λογισμικό έχει αφεθεί στα συστήματα επί του πλοίου. Συνιστάται η αφαίρεση ευαίσθητων δεδομένων από το πλοίο και η επανεγκατάσταση κατά την επιστροφή τους στο πλοίο. Όπου είναι δυνατόν, τα συστήματα θα πρέπει να σαρώνονται για κακόβουλο λογισμικό πριν από τη χρήση. Τα Λειτουργικά Τεχνολογικά Συστήματα θα πρέπει να δοκιμάζονται για να ελέγχεται ότι λειτουργούν σωστά.

Ορισμένα Λειτουργικά και Πληροφοριακά Τεχνολογικά Συστήματα είναι απομακρυσμένα προσβάσιμα και ενδέχεται να λειτουργούν με συνεχή σύνδεση στο διαδίκτυο για απομακρυσμένη παρακολούθηση, συλλογή δεδομένων, λειτουργίες συντήρησης, ασφάλεια και προστασία. Τα συστήματα αυτά μπορούν να είναι "συστήματα τρίτων", μέσω των οποίων ο εξωτερικός συνεργάτης τεχνικός παρακολουθεί και συντηρεί τα συστήματα από απομακρυσμένα. Τα συστήματα αυτά θα μπορούσαν να περιλαμβάνουν τόσο αμφίδρομη ροή δεδομένων όσο και αποστολή μόνο. Τα συστήματα και οι σταθμοί εργασίας με λειτουργίες τηλεχειρισμού, πρόσβασης ή διαμόρφωσης θα μπορούσαν, για παράδειγμα, να είναι:

- Ηλεκτρονικοί Υπολογιστές στη Γέφυρα και στο Μηχανοστάσιο και σταθμοί εργασίας στο δίκτυο διαχείρισης του πλοίου.
- Φορτίο, όπως εμπορευματοκιβώτια με συστήματα ελέγχου θερμοκρασίας ή εξειδικευμένα φορτία που παρακολουθούνται εξ αποστάσεως.
- Συστήματα ευστάθειας.
- Συστήματα παρακολούθησης καταπόνησης γάστρας.

- Συστήματα πλοήγησης, συμπεριλαμβανομένου του Ηλεκτρονικού Χάρτη Πλοήγησης (Electronic Navigation Chart - ENC), του Κατάγραφέα Δεδομένων Ταξιδιού (Voyage Data Recorder - VDR), και της Δυναμικής Τοποθέτησης (Dynamic Positioning - DP).
- Διακίνηση και στοιβασία φορτίου, διαχείριση κινητήρων και φορτίου και συστήματα σχεδιασμού φόρτωσης.
- Δίκτυα ασφάλειας και προστασίας, όπως CCTV (Closed Circuit Television).
- Εξειδικευμένα συστήματα όπως εργασίες γεώτρησης, συστήματα υποθαλάσσιας εγκατάστασης, επείγουσα διακοπή λειτουργίας (Emergency Shutdown - ESD) για δεξαμενόπλοια αερίου, εγκατάσταση και επισκευή υποβρυχίων καλωδίων.

Η έκταση και η φύση της συνδεσιμότητας του εξοπλισμού θα πρέπει να είναι γνωστές από τον πλοιοκτήτη ή τον φορέα εκμετάλλευσης και να θεωρούνται σημαντικό μέρος της εκτίμησης κινδύνου.

5.1.9 Αξιολόγηση Επιπτώσεων

Η Εμπιστευτικότητα (Confidentiality), Ακεραιότητα (Integrity) και Διαθεσιμότητα (Availability) παρέχουν ένα πλαίσιο αξιολόγησης της επίπτωσης:

- Μη εξουσιοδοτημένης πρόσβασης και αποκάλυψης πληροφοριών ή δεδομένων σχετικά με το πλοίο, το πλήρωμα, το φορτίο και τους επιβάτες
- Απώλειας ακεραιότητας, η οποία θα τροποποιούσε ή θα κατέστρεφε πληροφορίες και δεδομένα σχετικά με την ασφαλή και αποτελεσματική λειτουργία και διαχείριση του πλοίου
- Απώλειας διαθεσιμότητας λόγω της καταστροφής των πληροφοριών και των δεδομένων ή/και της διακοπής των υπηρεσιών/ λειτουργίας των συστημάτων πλοίων.

Η σχετική σημασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας εξαρτάται από τη χρήση των πληροφοριών ή των δεδομένων. Για παράδειγμα, η αξιολόγηση της ευπάθειας των Πληροφοριακών Τεχνολογικών Συστημάτων που σχετίζονται με εμπορικές δραστηριότητες μπορεί να επικεντρωθεί στην εμπιστευτικότητα και την ακεραιότητα αντί για τη διαθεσιμότητα. Αντιστρόφως, η αξιολόγηση της ευπάθειας των Λειτουργικών Τεχνολογικών Συστημάτων επί των πλοίων, ιδίως των συστημάτων ζωτικής σημασίας για την ασφάλεια, μπορεί να επικεντρωθεί στη διαθεσιμότητα ή/και την ακεραιότητα αντί της εμπιστευτικότητας.

Οι δυνητικές επιπτώσεις μπορεί να είναι σχετικές με την ασφάλεια , τη λειτουργία, το περιβάλλον, την οικονομία , τη φήμη και τη συμμόρφωση. Αρκετές μεθοδολογίες αξιολόγησης παρέχουν κριτήρια και τεχνικές που βοηθούν να αποσαφηνίσουν την σπουδαιότητα μιας επίπτωσης από επίθεση στον Κυβερνοχώρο

Πίνακας 5.2. Επίπεδα πιθανών επιπτώσεων με χρήση του μοντέλου CIA.

Πηγή: Bimco's Guidelines Version 3.

Πιθανή Επίπτωση	Ορισμός - Αποσαφήνιση	Πρακτική
Χαμηλή (Low)	Η απώλεια εμπιστευτικότητας, πληρότητας ή διαθεσιμότητας μπορεί να αναμένεται να έχει ένα περιορισμένο αρνητικό αντίκτυπο στην εταιρεία και το πλοίο, στα περιουσιακά στοιχεία της εταιρείας ή στο προσωπικό.	Περιορισμένα αρνητική σημαίνει ότι μια παραβίαση ασφάλειας μπορεί: (1) να προκαλέσει υποβάθμιση λειτουργιών του πλοίου σε βαθμό και διάρκεια που ο οργανισμός να μπορεί να εφαρμόσει τις βασικές λειτουργίες του αλλά η αποτελεσματικότητά είναι μειωμένες (2) να έχει ως αποτέλεσμα ασήμαντες βλάβες στα περιουσιακά στοιχεία του οργανισμού (3) να έχει ως αποτέλεσμα ασήμαντη οικονομική απώλεια (4) να έχει ως αποτέλεσμα ασήμαντη βλάβη σε άτομα.
Μέτρια (Moderate)	Η απώλεια εμπιστευτικότητας, πληρότητας ή διαθεσιμότητας μπορεί να αναμένεται να έχει ουσιαστικά αρνητική επίπτωση στην εταιρεία, το πλοίο τα περιουσιακά στοιχεία και στο προσωπικό.	Ουσιαστικά αρνητική σημαίνει ότι μια παραβίαση ασφάλειας μπορεί: (1) να προκαλέσει σημαντική υποβάθμιση λειτουργιών του πλοίου σε βαθμό και διάρκεια που ο οργανισμός να μπορεί να εφαρμόσει τις βασικές λειτουργίες του αλλά η αποτελεσματικότητά είναι μειωμένες σημαντικά (2) να έχει ως αποτέλεσμα σημαντικές βλάβες στα περιουσιακά στοιχεία του οργανισμού (3) να έχει ως αποτέλεσμα σημαντική οικονομική απώλεια (4) να έχει ως αποτέλεσμα σημαντική βλάβη σε άτομα.
Υψηλή (High)	Η απώλεια εμπιστευτικότητας, πληρότητας ή διαθεσιμότητας μπορεί να αναμένεται να έχει σοβαρή αρνητική επίπτωση στην εταιρεία, το πλοίο τα περιουσιακά στοιχεία και στο προσωπικό.	Σοβαρή αρνητική σημαίνει ότι μια παραβίαση ασφάλειας μπορεί: (1) να προκαλέσει σοβαρή υποβάθμιση λειτουργιών του πλοίου σε βαθμό και διάρκεια που ο οργανισμός να μπορεί να εφαρμόσει τις βασικές λειτουργίες του αλλά η αποτελεσματικότητά είναι μειωμένες σοβαρά (2) να έχει ως αποτέλεσμα σοβαρές βλάβες στα περιουσιακά στοιχεία του οργανισμού (3) να έχει ως αποτέλεσμα σοβαρή οικονομική απώλεια (4) να έχει ως αποτέλεσμα σοβαρή βλάβη σε άτομα.

Η Αξιολόγηση Κινδύνου για Λειτουργικά Τεχνολογικά Συστήματα, βασίζεται σε μία επισκόπηση των αποθεμάτων εξοπλισμού, στα ηλεκτρονικά συστήματα τα οποία λειτουργούν μέσω Η/Υ και σε ένα χάρτη που αποτυπώνει τις συνδέσεις δικτύου επί του πλοίου ή της εταιρίας κατά περίπτωση. Επιπλέον, σημεία πρόσβασης και συσκευές επικοινωνίας πρέπει να είναι μέρη της επισκόπησης αυτής. Δεδομένου πως η επίπτωση ενός περιστατικού του Κυβερνοχώρου σε Λειτουργικά Τεχνολογικά Συστήματα επί του πλοίου μπορεί να περιλαμβάνει φυσικές συνέπειες και επιδράσεις, οι αξιολογήσεις κινδύνου πρέπει να συμπεριλαμβάνουν:

- Επιπτώσεις στην ασφάλεια του προσωπικού του πλοίου, στο ίδιο το πλοίο και στο φορτίο.
- Τις συνέπειες που μπορεί να προκληθούν σε ένα Λειτουργικό Τεχνολογικό Σύστημα, αλλά και στα περιβάλλοντα συστήματα τα οποία είναι διασυνδεμένα με αυτό.
- Τα επακόλουθα για τις Αξιολογήσεις Κινδύνου των μη ψηφιακών στοιχείων ελέγχου στο πλαίσιο Λειτουργικού Τεχνολογικού Συστήματος.

Η εφαρμογή μέτρων προστασίας που βασίζονται σε εκτιμήσεις κινδύνου είναι καθιερωμένη σε όλα τα πλοία μέσω του κώδικα ISM και του Safety Management Systems (SMS) του πλοίου. Οι αξιολογήσεις ασφάλειας αφορούν κυρίως τον φυσικό κόσμο, λαμβάνοντας υπόψη ότι ο φυσικός και ο ψηφιακός κόσμος είναι πλέον αλληλένδετοι. Η αξιολόγηση της πιθανής σωματικής βλάβης από ένα περιστατικό στον κυβερνοχώρο θα πρέπει να περιλαμβάνει:

1. Το πώς ένα περιστατικό θα μπορεί να χειριστεί τη λειτουργία αισθητήρων και συσκευών ενεργοποίησης που έχουν επίπτωση στο φυσικό περιβάλλον.
2. Τι περιττά στοιχεία ελέγχου και χειροκίνητες δυνατότητες παράκαμψης υπάρχουν στο Λειτουργικό Τεχνολογικό Σύστημα για την πρόληψη ενός συμβάντος.
3. Πως θα μπορούσε να προκύψει ένα φυσικό περιστατικό.
4. Πώς να αποτιμηθούν πιθανές συνέπειες στη φυσική διαδικασία που εκτελέστηκε από το Λειτουργικό Τεχνολογικό Σύστημα.

5.1.10 Φέρε Τη Δική Σου Συσκευή (Bring Your Own Device - BYOD)

Αναγνωρίζεται ότι το προσωπικό μπορεί να έχει τη δυνατότητα να μεταφέρει τις δικές του συσκευές (BYOD) επί του πλοίου για να έχει πρόσβαση στο σύστημα ή το δίκτυο του πλοίου. Αν και αυτό μπορεί να είναι τόσο ευεργετικό όσο και οικονομικό για τα πλοία, αυξάνει σημαντικά το επίπεδο ευπάθειας, επειδή αυτές οι συσκευές μπορεί να μην είναι διαχειριζόμενες. Οι πολιτικές και οι διαδικασίες θα πρέπει να εξετάζουν τον έλεγχο και τη χρήση των BYOD, καθώς και τον τρόπο προστασίας των ευάλωτων δεδομένων, χρησιμοποιώντας, για παράδειγμα, τον διαχωρισμό δικτύου.

5.1.11 Αξιολόγηση Κινδύνου Από Την Εταιρεία

Όπως αναφέρθηκε παραπάνω, η Αξιολόγηση Κινδύνου ως διαδικασία ξεκινά εκτιμώντας τα συστήματα επί του πλοίου προκειμένου να χαρτογραφηθεί η στιβαρότητά τους για την αντιμετώπιση του τρέχοντος επιπέδου απειλών από τον Κυβερνοχώρο. Η αξιολόγηση πρέπει να εκτιμά τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα επί του πλοίου. Όταν διενεργείται η αξιολόγηση, η εταιρεία πρέπει να εκτιμήσει τα αποτελέσματα της Αξιολόγησης Κινδύνου για το πλοίο καθώς και τα ακόλουθα:

1. Αναγνώριση υπαρχόντων τεχνικών και διαδικαστικών ελέγχων για να προστατευθούν τα επί του πλοίου Λειτουργικά και Πληροφοριακά Τεχνολογικά Συστήματα.
2. Αναγνώριση των Λειτουργικών και Πληροφοριακών Τεχνολογικών Συστημάτων που είναι ευάλωτα εμπεριεχομένου του ανθρώπινου παράγοντα και πολιτικές και διαδικασίες που ελέγχουν τη χρήση αυτών των συστημάτων.
3. Αναγνώριση και εκτίμηση κρίσιμων λειτουργιών του πλοίου που είναι ευπαθείς σε επιθέσεις από τον Κυβερνοχώρο.
4. Αναγνώριση των πιθανών περιστατικών από τον Κυβερνοχώρο και οι επιπτώσεις τους σε κρίσιμες λειτουργίες του πλοίου. Επίσης και η πιθανότητα της εμφάνισής τους για τη θέσπιση και απόδοση προτεραιοτήτων σε κατάλληλα μέτρα.

Οι εταιρείες μπορούν να διαβουλεύονται με τους κατασκευαστές και τους προμηθευτές υπηρεσιών εξοπλισμού και συστημάτων επί του πλοίου για να κατανοήσουν τους τεχνικούς και διαδικαστικούς ελέγχους που ενδέχεται να έχουν ήδη τεθεί σε εφαρμογή για την αντιμετώπιση της διαχείρισης κινδύνων στον κυβερνοχώρο. Επιπλέον, οποιαδήποτε προσδιορισμένη ευπάθεια στον κυβερνοχώρο στην τυποποιημένη διαμόρφωση για ένα κρίσιμο σύστημα ή κατασκευαστικό στοιχείο θα πρέπει να γνωστοποιείται για τη διευκόλυνση της καλύτερης προστασίας του εξοπλισμού στο μέλλον.

5.1.12 Αξιολογήσεις Κινδύνου Από Τρίτους

Οι αυτό-αξιολογήσεις μπορούν να χρησιμεύσουν ως μια καλή αρχή, αλλά μπορούν να συμπληρωθούν από αξιολογήσεις κινδύνου από τρίτους να εμβαθύνουν και να προσδιορίσουν τους κινδύνους και τα κενά που μπορεί να μην βρεθούν κατά τη διάρκεια της αυτο-αξιολόγησης. Μπορούν επίσης να πραγματοποιηθούν δοκιμές διείσδυσης κρίσιμων υποδομών Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων για να προσδιοριστεί κατά πόσον το πραγματικό αμυντικό επίπεδο ταιριάζει στο επιθυμητό επίπεδο που καθορίζεται στη στρατηγική ασφάλειας στον κυβερνοχώρο για την εταιρεία. Τέτοιες δοκιμές μπορούν να εκτελεστούν από εξωτερικούς εμπειρογνώμονες που προσομοιώνουν επιθέσεις χρησιμοποιώντας Πληροφοριακά Τεχνολογικά

Συστήματα, κοινωνική μηχανική και, εάν είναι επιθυμητό, ακόμη και φυσική διείσδυση της περιμέτρου ασφαλείας μιας εγκατάστασης. Αυτές οι δοκιμές αναφέρονται ως ενεργές δοκιμές, επειδή περιλαμβάνουν την πρόσβαση και την εισαγωγή λογισμικού σε ένα σύστημα. Αυτό μπορεί να είναι κατάλληλο μόνο για Πληροφοριακά Τεχνολογικά Συστήματα. Όταν ο κίνδυνος για τα Λειτουργικά Τεχνολογικά Συστήματα κατά τη διάρκεια των δοκιμών διείσδυσης είναι απαράδεκτος, θα πρέπει να εξετάζονται παθητικές προσεγγίσεις δοκιμών. Οι παθητικές μέθοδοι βασίζονται στη σάρωση δεδομένων που μεταδίδονται από ένα σύστημα για τον εντοπισμό ευπαθειών. Γενικά, δεν γίνεται καμία προσπάθεια ενεργού πρόσβασης ή εισαγωγής λογισμικού στο σύστημα.

5.1.13 Διαδικασία Αξιολόγησης Κινδύνου

Φάση 1: Ενέργειες πριν την αξιολόγηση

Πριν να αρχίσει η Αξιολόγηση Κινδύνου από τον Κυβερνοχώρο στο πλοίο, θα πρέπει να εκτελεστούν οι ακόλουθες δραστηριότητες:

- Χαρτογράφηση των κρίσιμων λειτουργιών του πλοίου καθώς και των συστημάτων και του επιπέδου πιθανών επιπτώσεών τους.
- Προσδιορισμός βασικών διαδικασιών κρίσιμου εξοπλισμού των Λειτουργικών και Πληροφοριακών Τεχνολογικών Συστημάτων .
- Επανεξέταση λεπτομερούς τεκμηρίωσης των κρίσιμων Πληροφοριακών και Λειτουργικών Συστημάτων, συμπεριλαμβανομένης της αρχιτεκτονικής του δικτύου τους, των διεπαφών και των διασυνδέσεων.
- Προσδιορισμός των σημείων επαφής ασφάλειας από τον Κυβερνοχώρο με καθέναν από τους κατασκευαστές και δημιουργία σχέσεων εργασίας μαζί τους.
- Λεπτομερής τεκμηρίωση σχετικά με τη συντήρηση και την υποστήριξη των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων του πλοίου.
- Θέσπιση συμβατικών απαιτήσεων και υποχρεώσεων που μπορεί να έχει ο πλοιοκτήτης/εφοπλιστής για τη συντήρηση και την υποστήριξη δικτύων και εξοπλισμού επί του πλοίου.
- Υποστήριξη, εάν είναι απαραίτητο, της αξιολόγησης κινδύνου με εξωτερικό εμπειρογνώμονα για την ανάπτυξη λεπτομερών σχεδίων και τη συμπερίληψη παραγωγών και προμηθευτών υπηρεσιών.

Φάση 2: Αξιολόγηση Πλοίου

Στόχος της αξιολόγησης του δικτύου ενός πλοίου και των συστημάτων και συσκευών του είναι ο εντοπισμός τυχόν τρωτών σημείων που θα μπορούσαν να θέσουν σε κίνδυνο ή να οδηγήσουν είτε σε απώλεια της εμπιστευτικότητας, είτε σε απώλεια της ακεραιότητας είτε σε απώλεια της

λειτουργίας του εξοπλισμού, του συστήματος, του δικτύου, ή ακόμη και του πλοίου. Αυτά τα τρωτά σημεία και αδυναμίες θα μπορούσαν να εμπίπτουν σε μία από τις ακόλουθες κατηγορίες:

- Τεχνικές, όπως ελαττώματα λογισμικού ή απαρχαιωμένα ή συστήματα που δεν περιέχουν λογισμικό επιδιόρθωσης.
- Σφάλματα εφαρμογής όπως ελλιπώς εγκατεστημένα τείχη προστασίας (firewalls).
- Διαδικαστικά ή άλλα λάθη από το χρήστη.

Οι δραστηριότητες που εκτελούνται κατά τη διάρκεια μιας αξιολόγησης θα μπορούσαν να περιλαμβάνουν την αναθεώρηση της ρύθμισης παραμέτρων όλων των υπολογιστών, διακομιστών, δρομολογητών και τεχνολογιών ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των τειχών προστασίας. Θα μπορούσε επίσης να περιλαμβάνει αναθεωρήσεις όλων των διαθέσιμων εγγράφων και διαδικασιών ασφάλειας στον κυβερνοχώρο για συνδεδεμένα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα και συσκευές.

Μια πτυχή της επιτόπιας αξιολόγησης είναι η συμμετοχή του πληρώματος όλων των επιπέδων· ιδιαίτερα του πλοιάρχου, του αρχιμηχανικού και του πρώτου μηχανικού. Αυτή η διαδικασία βοηθά στην κατανόηση της εφαρμογής των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων επί του πλοίου, και πώς αυτά μπορεί να διαφέρουν από την δηλωμένη τεκμηρίωση του σχεδιασμού, καθώς και στην κατανόηση του επιπέδου της εκπαίδευσης στον κυβερνοχώρο που παρέχεται στο πλήρωμα του πλοίου.

Φάση 3: Ενημέρωση και ανασκόπηση/υποβολή εκθέσεων ευπάθειας

Μετά την αξιολόγηση, κάθε διαπιστωθείσα ευπάθεια θα πρέπει να αξιολογείται για τον πιθανό αντίκτυπό της και την πιθανότητα εκμετάλλευσής της. Θα πρέπει να προσδιορίζονται τα συνιστάμενα τεχνικά ή/και διαδικαστικά διορθωτικά μέτρα για κάθε ευπάθεια.

Ιδανικά, η Αξιολόγηση Κινδύνου από τον Κυβερνοχώρο θα πρέπει να περιέχει:

- Συνοπτική παρουσίαση – περίληψη υψηλού επιπέδου - των αποτελεσμάτων, των συστάσεων και του συνολικού προφίλ ασφάλειας του.
- Τεχνικά ευρήματα – ανάλυση των ανακαλυφθέντων ευπαθειών, την πιθανότητα εκμετάλλευσής τους, τις επιπτώσεις που προκύπτουν και κατάλληλες τεχνικές συμβουλές επιδιόρθωσης και μετριασμού.
- Κατά προτεραιότητα κατάλογος δράσεων – οι προτεραιότητες που έχουν διατεθεί θα πρέπει να αντικατοπτρίζουν την αποτελεσματικότητα του μέτρου, το κόστος, τη δυνατότητα εφαρμογής κ.λπ. Είναι σημαντικό ο κατάλογος αυτός να είναι ένας πλήρης

κατάλογος διαθέσιμων επιλογών και να μην αντιπροσωπεύει κατάλογο υπηρεσιών και προϊόντων που ο τρίτος αξιολογητής κινδύνου, κατά περίπτωση, θα ήθελε να πωλήσει.

- Συμπληρωματικά στοιχεία – ένα συμπλήρωμα που περιέχει τις τεχνικές λεπτομέρειες όλων των βασικών ευρημάτων και ολοκληρωμένη ανάλυση κρίσιμων ελαττωμάτων. Η ενότητα αυτή θα πρέπει επίσης να περιλαμβάνει δείγματα δεδομένων που ανακτώνται κατά τη διάρκεια της δοκιμής διείσδυσης, εάν υπάρχουν, κρίσιμων τρωτών σημείων ή ευπαθειών υψηλού κινδύνου.
- Παραρτήματα – αρχεία των δραστηριοτήτων που διεξάγονται από την ομάδα αξιολόγησης κινδύνου στον κυβερνοχώρο και τα εργαλεία που χρησιμοποιήθηκαν κατά τη διάρκεια της δέσμευσης

Θα πρέπει να εξεταστεί ακόμη κατά πόσον τμήματα της αξιολόγησης κινδύνου στον κυβερνοχώρο θα πρέπει να αντιμετωπίζονται ως εμπιστευτικά.

Ενώ οι πολιτικές και οι διαδικασίες διαχείρισης κινδύνων στον κυβερνοχώρο θα πρέπει να περιλαμβάνονται στο σύστημα διαχείρισης της ασφάλειας της εταιρείας, αυτές δεν θα πρέπει να περιέχουν πληροφορίες, οι οποίες, εάν καταστούν διαθέσιμες εκτός της εταιρείας, θα μπορούσαν να καταστούν τρωτά σημεία.

Φάση 4: Ενημέρωση κατασκευαστή

Μόλις ο πλοιοκτήτης έχει την ευκαιρία να επανεξετάσει, να συζητήσει και να αξιολογήσει τα πορίσματα, ενδέχεται να χρειαστεί να σταλεί ένα υποσύνολο των πορισμάτων στους κατασκευαστές των επηρεαζόμενων συστημάτων. Τυχόν ευρήματα, τα οποία εγκρίνονται από τον πλοιοκτήτη για γνωστοποίηση στους κατασκευαστές, θα μπορούσαν να αναλυθούν περαιτέρω με την υποστήριξη εξωτερικών εμπειρογνωμόνων, οι οποίοι θα πρέπει να συνεργάζονται με το σημείο επαφής του παραγωγού για την ασφάλεια στον κυβερνοχώρο, ώστε να εξασφαλίζεται ότι επιτυγχάνεται η τεχνική κατανόηση του προβλήματος. Αυτή η υποστηρικτική δραστηριότητα έχει ως στόχο να εξασφαλίσει ότι κάθε σχέδιο αποκατάστασης που καταρτίζει ο παραγωγός είναι περιεκτικό και προσδιορίζει τη σωστή λύση για την εξάλειψη των τρωτών σημείων.

5.1.14 Ανάπτυξη Προστασίας Και Ανακάλυψη Μέτρων

Το αποτέλεσμα της Αξιολόγησης Κινδύνου της εταιρείας και της επακόλουθης στρατηγικής ασφάλειας από τον Κυβερνοχώρο πρέπει να είναι η μείωση στο χαμηλότερο δυνατό επίπεδο. Σε τεχνικό επίπεδο, αυτό θα περιλαμβάνει τις απαραίτητες δράσεις που πρέπει να αναπτυχθούν για την καθιέρωση και συντήρηση ενός συμφωνημένου επιπέδου ασφαλείας από τον Κυβερνοχώρο.

Είναι σημαντικό να προσδιοριστεί ο τρόπος με τον οποίο θα εφαρμόζεται το μέτρο της ασφάλειας στον Κυβερνοχώρο, επί του πλοίου, και να ανατεθούν αρμοδιότητες στον Πλοίαρχο, και στους υπεύθυνους αξιωματικούς.

5.1.15 Άμυνα Σε Βάθος Και Σε Εύρος

Είναι σημαντικό να προστατεύονται τα κρίσιμα συστήματα και τα δεδομένα με μέτρα πολλαπλών επιπέδων τα οποία λαμβάνουν υπόψη τον ρόλο του προσωπικού, διαδικασίες και τεχνολογία για να:

- Αυξηθεί η πιθανότητα ανίχνευσης ενός περιστατικού Κυβερνοχώρου.
- Αυξηθεί η προσπάθεια και οι πηγές που απαιτούνται για την προστασία της πληροφορίας των δεδομένων. Επίσης, να αυξηθεί η διαθεσιμότητα των Πληροφοριακών και των Λειτουργικών Τεχνολογικών Συστημάτων.

Τα Λειτουργικά Τεχνολογικά Συστήματα που είναι συνδεδεμένα επί του πλοίου, απαιτούν πάνω από ένα τεχνικό ή/και διαδικαστικό μέτρο προστασίας. Περιμετρικές άμυνες όπως τείχη προστασίας είναι σημαντικά εργαλεία για την αποτροπή ανεπιθύμητης εισόδου στα συστήματα.

Αυτή η σε βάθος προσέγγιση άμυνας ενισχύει ένα συνδυασμό από:

- Φυσικής προστασίας του πλοίου σε συμφωνία με το Σχέδιο Κινδύνου Πλοίου (Ship Security Plan – SSP).
- Προστασία των δικτύων, περιλαμβανομένης μίας αποτελεσματικής κατάτμησης (Segmentation).
- Ανίχνευση εισβολής.
- Περιοδική σάρωση και δοκιμασία των ευπαθειών.
- Πρόσβαση και στοιχεία ελέγχου χρήστη.
- Κατάλληλες διαδικασίες σχετικά με τη χρήση αφαιρούμενων μέσων αποθήκευσης και πολιτικές συνθηματικών.
- Αντίληψη του προσωπικού περί κινδύνου και οικειότητα με κατάλληλες διαδικασίες.

Οι πολιτικές και οι διαδικασίες της εταιρείας θα πρέπει να συμβάλλουν στη διασφάλιση ότι η ασφάλεια στον κυβερνοχώρο λαμβάνεται υπόψη στο πλαίσιο της συνολικής προσέγγισης για τη διαχείριση κινδύνων για την ασφάλεια γενικά. Η πολυπλοκότητα των απειλών στον κυβερνοχώρο σημαίνει ότι θα πρέπει να εξεταστεί το ενδεχόμενο μιας προσέγγισης "**άμυνας σε βάθος**". Ο εξοπλισμός και τα δεδομένα που προστατεύονται από επίπεδα μέτρων προστασίας είναι πιο ανθεκτικά στις επιθέσεις στον κυβερνοχώρο.

Κατά την ανάπτυξη της ενοποίησης μεταξύ συστημάτων, θα πρέπει να λαμβάνεται υπόψη ένα μοντέλο ορίου εμπιστοσύνης, σύμφωνα με το οποίο τα συστήματα ομαδοποιούνται σε εκείνα μεταξύ των οποίων η εμπιστοσύνη είναι σιωπηρή (για παράδειγμα οι σταθμοί εργασίας χρήστη) και εκείνα μεταξύ των οποίων η εμπιστοσύνη θα πρέπει να είναι σαφής (μεταξύ των υπολογιστών γέφυρας και των εταιρικών δικτύων). Για μεγάλα ή σύνθετα δίκτυα, η μοντελοποίηση των απειλών θα πρέπει να θεωρείται ως μια δραστηριότητα για να καταλάβουμε που θα αναπτυχθούν οι τεχνικοί έλεγχοι μεταξύ συστημάτων προκειμένου να εφαρμοστεί "**άμυνα σε εύρος**".

Ωστόσο, επί των πλοίων στα οποία τα επίπεδα ολοκλήρωσης μεταξύ των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων μπορεί να είναι υψηλά, η «άμυνα σε βάθος» λειτουργεί μόνο εάν εφαρμόζονται τεχνικά και διαδικαστικά μέτρα προστασίας σε επίπεδα σε όλα τα ευάλωτα και ολοκληρωμένα συστήματα. Πρόκειται για «άμυνα σε εύρος» και χρησιμοποιείται για την πρόληψη τυχόν τρωτών σημείων σε ένα σύστημα που χρησιμοποιούνται για την καταστρατήγηση των μέτρων προστασίας ενός άλλου συστήματος.

Τα μέτρα προστασίας από τον κυβερνοχώρο μπορούν να έχουν τεχνικό ή διαδικαστικό χαρακτήρα, με τεχνικούς ελέγχους που εφαρμόζονται για την επιβολή διαδικαστικών ελέγχων. Μια συνδυασμένη προσέγγιση με τη χρήση κατάλληλων μέτρων παρέχει το πλέον αποτελεσματικό επίπεδο προστασίας.

Η **άμυνα σε βάθος** και η **άμυνα σε εύρος** είναι συμπληρωματικές προσεγγίσεις, οι οποίες, όταν εφαρμόζονται από κοινού, παρέχουν τη βάση μιας ολιστικής απάντησης στη διαχείριση των κινδύνων στον κυβερνοχώρο.

Τα μέτρα προστασίας από τον κίνδυνο στον κυβερνοχώρο μπορεί να είναι τεχνικά και να επικεντρώνονται στη διασφάλιση ότι τα συστήματα επί του πλοίου σχεδιάζονται και έχουν ρυθμιστεί ώστε να είναι ανθεκτικά στις επιθέσεις στον κυβερνοχώρο. Τα μέτρα προστασίας μπορούν επίσης να είναι διαδικαστικά και θα πρέπει να καλύπτονται από τις πολιτικές της εταιρείας, τις διαδικασίες διαχείρισης της ασφάλειας, τις διαδικασίες ασφαλείας από έκνομες πράξεις και τους ελέγχους πρόσβασης.

Πρέπει να εξεταστεί η εφαρμογή τεχνικών ελέγχων που είναι πρακτικοί και οικονομικά αποδοτικοί, ιδίως στα υπάρχοντα πλοία.

Θα πρέπει να δοθεί προτεραιότητα στην εφαρμογή των ελέγχων ασφάλειας στον κυβερνοχώρο, εστιάζοντας πρώτα στα μέτρα αυτά ή σε συνδυασμούς μέτρων, τα οποία προσφέρουν το μεγαλύτερο όφελος.

5.1.16 Τεχνικά Μέτρα Προστασίας

Το Κέντρο για την Ασφάλεια στο Διαδίκτυο (Center of Internet Security - CIS) παρέχει οδηγίες οι οποίες αφορούν τα μέτρα που μπορούν να ληφθούν για την αντιμετώπιση των ευπαθειών. Τα μέτρα αυτά είναι ουσιαστικά μια λίστα που αποτελείται από κρίσιμους ελέγχους ασφαλείας (Critical Security Controls - CSC) οι οποίοι ελέγχονται για να διασφαλίσουν ότι παρέχουν μια αποτελεσματική προσέγγιση στις εταιρείες για την αξιολόγηση και τη βελτίωση της άμυνας τους. Τα CSC περιλαμβάνουν τόσο τεχνικές όσο και διαδικαστικές πτυχές.

- **Οριοθέτηση και έλεγχος για θύρες δικτύων, πρωτοκόλλα και υπηρεσίες** Κατάλογοι πρόσβασης σε συστήματα δικτύων μπορεί να χρησιμοποιηθούν για την εφαρμογή της πολιτικής της εταιρείας για την ασφάλεια. Αυτό βοηθά στη διασφάλιση ότι μόνο κατάλληλη κυκλοφορία θα επιτρέπεται μέσω ενός ελεγχόμενου δικτύου ή υποδικτύου, που θα είναι βασισμένη στην πολιτική ελέγχου αυτού του δικτύου ή υποδικτύου.
  Συνιστάται οι δρομολογητές (routers) να είναι ασφαλείς έναντι επιθέσεων και οι θύρες που δεν χρησιμοποιούνται να είναι κλειστές για να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δεδομένα.
- **Ρύθμιση των συσκευών δικτύου όπως Τείχη Προστασίας, Δρομολογητές (Routers) και Διακόπτες (Switches).** Θα πρέπει να προσδιορίζεται ποια συστήματα θα πρέπει να συνδέονται με ελεγχόμενα ή ανεξέλεγκτα δίκτυα. Τα ελεγχόμενα δίκτυα έχουν σχεδιαστεί για να αποτρέπουν τυχόν κινδύνους ασφαλείας από συνδεδεμένες συσκευές με τη χρήση τείχους προστασίας, πυλών ασφαλείας, δρομολογητών και διακοπτών. Τα ανεξέλεγκτα δίκτυα ενδέχεται να ενέχουν κινδύνους λόγω έλλειψης ελέγχου της κυκλοφορίας δεδομένων και θα πρέπει να απομονωθούν από ελεγχόμενα δίκτυα, καθώς η απευθείας σύνδεση στο διαδίκτυο τα καθιστά ιδιαίτερα επιρρεπή σε διείσδυση από κακόβουλο λογισμικό. Για παράδειγμα:
  - ✓ Τα δίκτυα τα οποία είναι καίρια για την ομαλή λειτουργία του πλοίου, πρέπει να ελέγχονται. Είναι σημαντικό ότι αυτά τα συστήματα έχουν υψηλό επίπεδο ασφάλειας

- ✓ Θα πρέπει επίσης να ελέγχονται τα δίκτυα που παρέχουν στους προμηθευτές απομακρυσμένη πρόσβαση στην πλοήγηση και στο λογισμικό άλλων Λειτουργικών Τεχνολογικών Συστημάτων επί του πλοίου. Αυτά τα δίκτυα ενδέχεται να είναι απαραίτητα για να επιτραπεί στους προμηθευτές να αποστείλουν αναβαθμίσεις συστήματος ή να εκτελούν απομακρυσμένη συντήρηση. Τα εξωτερικά σημεία πρόσβασης των συνδέσεων αυτών στη ξηρά θα πρέπει να είναι ασφαλή ώστε να αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση
- ✓ Τα συστήματα στοιβασίας φορτίου, σχεδιασμού και διαχείρισης φόρτωσης πρέπει να ελέγχονται. Για αυτό θα πρέπει τα συστήματα αυτά να εφαρμόζουν υποχρεωτική αναφορά για το πλοίο σε δημόσιες αρχές
- ✓ Τα υπόλοιπα δίκτυα, όπως τα δίκτυα στα οποία έχουν πρόσβαση οι επισκέπτες του πλοίου. Οποιοδήποτε ασύρματο δίκτυο θα πρέπει να θεωρείται ως ανεξέλεγκτο.

Ο αποτελεσματικός διαχωρισμός των συστημάτων, με βάση τα απαραίτητα επίπεδα πρόσβασης και εμπιστοσύνης, είναι μία από τις πιο επιτυχημένες στρατηγικές για την πρόληψη συμβάντων στον κυβερνοχώρο. Τα αποτελεσματικά διαχωρισμένα δίκτυα μπορούν να εμποδίσουν σημαντικά την πρόσβαση ενός εισβολέα στα συστήματα ενός πλοίου και είναι μία από τις πιο αποτελεσματικές τεχνικές για την πρόληψη της εξάπλωσης κακόβουλου λογισμικού. Τα δίκτυα στο πλοίο θα πρέπει να είναι χωρισμένα σε διαμερίσματα από τείχη προστασίας για τη δημιουργία ασφαλών ζωνών. Όσο λιγότερες συνδέσεις επικοινωνιών και συσκευές σε μια ζώνη, τόσο πιο ασφαλή είναι τα συστήματα και τα δεδομένα σε αυτή τη ζώνη. Τα εμπιστευτικά και κρίσιμα για την ασφάλεια συστήματα θα πρέπει να είναι στην πλέον προστατευμένη ζώνη.

- **Φυσική ασφάλεια από έκνομες πράξεις.** Η φυσική ασφάλεια αποτελεί κεντρική πτυχή της διαχείρισης των κινδύνων στον κυβερνοχώρο και μια αποτελεσματική στρατηγική για την άμυνα σε βάθος βασίζεται στη διασφάλιση ότι οι τεχνικοί έλεγχοι δεν μπορούν να καταστρατηγηθούν με ασήμαντα τεχνικά μέσα. Οι περιοχές που περιέχουν ευαίσθητα Λειτουργικά ή Πληροφοριακά Τεχνολογικά κατασκευαστικά στοιχεία ελέγχου πληροφορικής θα πρέπει να είναι ασφαλώς κλειδωμένες. Ο κρίσιμος εξοπλισμός για την ασφάλεια και την ασφάλεια από έκνομες πράξεις και οι διαδρομές καλωδίων θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και η

φυσική πρόσβαση σε ευαίσθητο εξοπλισμό χρήστη (όπως οι εκτεθειμένες θύρες USB σε συστήματα γέφυρας) θα πρέπει να είναι ασφαλής

- **Εντοπισμός, αποκλεισμός και συναγερμοί.** Ο εντοπισμός εισβολών και μολύνσεων αποτελεί κεντρικό μέρος των διαδικασιών ελέγχου. Θα πρέπει να καθοριστεί και να διαχειρίζεται μια γραμμή βάσης των λειτουργιών του δικτύου και των αναμενόμενων ροών δεδομένων για τους χρήστες και τα συστήματα, έτσι ώστε να είναι δυνατή η θέσπιση ορίων προειδοποίησης για συμβάντα στον Κυβερνοχώρο. Το κλειδί σε αυτό θα είναι ο καθορισμός των ρόλων και των ευθυνών για τον εντοπισμό, ώστε να διασφαλιστεί η ανάληψη ευθυνών. Επιπλέον, μια εταιρεία μπορεί να επιλέξει να ενσωματώσει ένα σύστημα ανίχνευσης εισβολών (Intrusion Detection System - IDS) ή ένα σύστημα πρόληψης εισβολών (Intrusion Prevention System - IPS) στο δίκτυο ή ως μέρος του τείχους προστασίας. Ορισμένες από τις κύριες λειτουργίες των συστημάτων αυτών περιλαμβάνουν τον εντοπισμό απειλών/κακόβουλων δραστηριοτήτων και κώδικα και, στη συνέχεια, καταγραφή, αναφορά και προσπάθεια αποκλεισμού της δραστηριότητας. Αυτό βοηθά να εξασφαλιστεί ότι το αφοσιωμένο προσωπικό επί του πλοίου μπορεί να κατανοήσει τις ειδοποιήσεις και τις επιπτώσεις τους. Τα συμβάντα που εντοπίζονται θα πρέπει να απευθύνονται σε άτομο ή πάροχο υπηρεσιών, ο οποίος είναι υπεύθυνος για την ανάληψη δράσης σε αυτό το είδος καταχώρισης.
- **Δορυφόρος και Ράδιο Επικοινωνία.** Η Κυβερνοασφάλεια για τη δορυφορική και ράδιο σύνδεση πρέπει να λαμβάνεται υπόψη σε συνεργασία με τον πάροχο υπηρεσιών. Στο πλαίσιο αυτό, η προδιαγραφή της δορυφορικής σύνδεσης πρέπει να λαμβάνεται υπόψη κατά τον καθορισμό των απαιτήσεων προστασίας δικτύου επί του πλοίου. Κατά τη δημιουργία σύνδεσης ανερχόμενης ζεύξης (uplink) για τα συστήματα πλοήγησης και ελέγχου ενός πλοίου σε παρόχους υπηρεσιών ξηράς, θα πρέπει να εξετάζεται ο τρόπος με τον οποίο θα αποφεύγεται η πρόσβαση των παράνομων συνδέσεων στα συστήματα επί του πλοίου. Η διασύνδεση πρόσβασης είναι ευθύνη του εταίρου διανομής. Η τελική δρομολόγηση της κυκλοφορίας των χρηστών από το σημείο πρόσβασης στο διαδίκτυο στον τελικό προορισμό του επί του πλοίου (“Last Mile”) είναι ευθύνη του πλοιοκτήτη. Η κυκλοφορία των χρηστών δρομολογείται μέσω του εξοπλισμού επικοινωνίας για περαιτέρω μετάδοση επί του πλοίου. Στο σημείο

πρόσβασης για αυτήν την κυκλοφορία, είναι απαραίτητο να παρέχεται ασφάλεια δεδομένων, τείχος προστασίας και μια αποκλειστική σύνδεση "Last-Mile". Όταν χρησιμοποιείται ένα εικονικό ιδιωτικό δίκτυο (Virtual Private Network - VPN), η κυκλοφορία δεδομένων θα πρέπει να κρυπτογραφηθεί σε ένα αποδεκτό διεθνές πρότυπο. Επιπλέον, θα πρέπει να αναπτυχθεί ένα τείχος προστασίας μπροστά από τους διακομιστές και τους υπολογιστές που είναι συνδεδεμένοι με τα δίκτυα (στην ξηρά ή επί του πλοίου). Ο συνεργάτης διανομής θα πρέπει να παρέχει συμβουλές σχετικά με τη δρομολόγηση και τον τύπο της σύνδεσης που είναι καταλληλότερα για συγκεκριμένη κυκλοφορία. Το φιλτράρισμα στην ξηρά (επιθεώρηση/αποκλεισμός) της κυκλοφορίας είναι επίσης θέμα μεταξύ ενός πλοιοκτήτη και του εταίρου διανομής. Τόσο το χερσαίο φιλτράρισμα της κυκλοφορίας όσο και των τειχών προστασίας της επιθεώρησης των πυλών αποκλεισμού στο πλοίο είναι απαραίτητα και αλληλοσυμπληρώνονται για την επίτευξη επαρκούς επιπέδου προστασίας. Οι κατασκευαστές τερματικών δορυφορικών επικοινωνιών και άλλου εξοπλισμού επικοινωνίας μπορούν να παρέχουν διασυνδέσεις διαχείρισης με λογισμικό ελέγχου ασφαλείας προσβάσιμο μέσω του διαδικτύου. Αυτό παρέχεται κυρίως με τη μορφή διεπαφών χρήστη που βασίζονται στο διαδίκτυο (Web-Based user interfaces). Κατά την αξιολόγηση της ασφάλειας της εγκατάστασης ενός πλοίου θα πρέπει να λαμβάνεται υπόψη η προστασία των εν λόγω διεπαφών.

- **Ασύρματη πρόσβαση ελέγχου.** Η ασύρματη πρόσβαση σε δίκτυα επί του πλοίου πρέπει να περιοριστεί σε κατάλληλα εξουσιοδοτημένες συσκευές και να ασφαλιστεί με χρήση ισχυρής κρυπτογράφησης, που θα αλλάζει τακτικά. Τα παρακάτω μπορεί να λαμβάνονται υπόψη για τον έλεγχο ασύρματης πρόσβασης:
  - ✓ Η χρήση εταιρικών συστημάτων ελέγχου ταυτοποίησης που χρησιμοποιούν ασύμμετρη κρυπτογράφηση και απομονώνουν δίκτυα με κατάλληλα ασύρματα ειδικά σημεία πρόσβασης (π.χ. δίκτυα επισκεπτών απομονωμένα από διοικητικά δίκτυα)
  - ✓ Η υιοθέτηση συστημάτων, όπως το ασύρματο IPS, που μπορεί να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση δικτύου σε τοπικά δίκτυα και άλλους πόρους πληροφοριών από ασύρματες συσκευές.

- ✓ Η προστασία της φυσικής διασύνδεσης μεταξύ των ασύρματων συσκευών πρόσβασης και του δικτύου (όπως βύσματα δικτύου, ράφια δικτύου κ.λπ.) για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση από παραπλανητικές συσκευές.

- **Εντοπισμός κακόβουλου λογισμικού (Malware).** Το λογισμικό σάρωσης που μπορεί να εντοπίσει και να αντιμετωπίσει αυτόματα την παρουσία κακόβουλου λογισμικού στα συστήματα επί του πλοίου θα πρέπει να ενημερώνεται τακτικά. Ως γενική κατευθυντήρια γραμμή, οι υπολογιστές επί του πλοίου θα πρέπει να προστατεύονται στο ίδιο επίπεδο με τους υπολογιστές γραφείου στην ξηρά. Το λογισμικό προστασίας από ιούς και λογισμικό κακόβουλης λειτουργίας θα πρέπει να εγκατασταθεί, να διατηρηθεί και να ενημερωθεί σε όλους τους προσωπικούς υπολογιστές που σχετίζονται με την εργασία επί του πλοίου. Αυτό θα μειώσει τον κίνδυνο αυτών των υπολογιστών που ενεργούν ως φορείς επίθεσης προς διακομιστές και άλλους υπολογιστές στο δίκτυο του πλοίου.
- **Ασφαλής Ρύθμιση για Υλικό και Λογισμικό.** Μόνο οι ανώτεροι υπάλληλοι θα πρέπει να έχουν προφίλ διαχειριστή, έτσι ώστε να μπορούν να ελέγχουν τη ρύθμιση και την απενεργοποίηση των κανονικών προφίλ χρηστών. Τα προφίλ χρηστών θα πρέπει να περιορίζονται ώστε να επιτρέπουν μόνο τη χρήση των υπολογιστών, των σταθμών εργασίας ή των διακομιστών για τους σκοπούς για τους οποίους απαιτούνται. Τα προφίλ χρηστών δεν πρέπει να επιτρέπουν στο χρήστη να τροποποιεί τα συστήματα ή να εγκαθιστά και να εκτελεί νέα προγράμματα.

- **Προστασία Ηλεκτρονικού Ταχυδρομείου (email) και Περιηγητή Δικτύου (web browser).** Η επικοινωνία μέσω email μεταξύ πλοίου και ξηράς είναι ζωτικής σημασίας για τη λειτουργία του πλοίου. Η κατάλληλη προστασία Ηλεκτρονικού Ταχυδρομείου (email) και Περιηγητή Δικτύου (web browser) εξυπηρετούν στην:
  - ✓ Αποτροπή το να χρησιμοποιηθεί το email για απόκτηση ευαίσθητων πληροφοριών.
  - ✓ Εξασφάλιση ότι η ανταλλαγή ευαίσθητων πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου ή φωνής προστατεύεται κατάλληλα για να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, π.χ. προστασία από κρυπτογράφηση.
  - ✓ Παρεμπόδιση των προγραμμάτων περιήγησης διαδικτύου και τα προγραμμάτων που είναι πελάτες ηλεκτρονικού ταχυδρομείου να εκτελούν κακόβουλες δέσμες ενεργειών.

Ορισμένες βέλτιστες πρακτικές για την ασφαλή μεταφορά ηλεκτρονικού ταχυδρομείου είναι: ηλεκτρονικό ταχυδρομείο ως zip ή κρυπτογραφημένο αρχείο όταν είναι απαραίτητο, απενεργοποίηση υπερ-συνδέσεων (hyperlinks) στο σύστημα ηλεκτρονικού ταχυδρομείου, αποφυγή της χρήσης γενικών διευθύνσεων ηλεκτρονικού ταχυδρομείου και επιβεβαίωση ότι το σύστημα έχει ρυθμίσει τους λογαριασμούς χρηστών.

- **Δυνατότητα ανάκτησης δεδομένων (Data Recovery Capability).** Ικανότητα ανάκτησης δεδομένων είναι η δυνατότητα επαναφοράς ενός συστήματος ή/και δεδομένων από ένα ασφαλές αντίγραφο ή εικόνα, επιτρέποντας έτσι την αποκατάσταση ενός "καθαρού" συστήματος. Οι βασικές πληροφορίες και οι κατάλληλες για λογισμικό εφεδρικές εγκαταστάσεις θα πρέπει να είναι διαθέσιμες για να διασφαλιστεί η αποκατάσταση μετά από ένα περιστατικό στον κυβερνοχώρο. Θα πρέπει να δημιουργηθούν περίοδοι διατήρησης και σενάρια αποκατάστασης για να δοθεί προτεραιότητα σε ποια κρίσιμα συστήματα χρειάζονται δυνατότητες γρήγορης επαναφοράς για να μειώσουν τον αντίκτυπο. Τα συστήματα που έχουν υψηλές απαιτήσεις διαθεσιμότητας δεδομένων θα πρέπει να καταστούν ανθεκτικά. Τα Λειτουργικά Τεχνολογικά Συστήματα, τα οποία είναι ζωτικής σημασίας για την ασφαλή ναυσιπλοΐα και τη λειτουργία του πλοίου, θα πρέπει να διαθέτουν εφεδρικά συστήματα που θα επιτρέπουν στο πλοίο να ανακτά γρήγορα και με ασφάλεια τις δυνατότητες πλοήγησης και λειτουργίας μετά από ένα περιστατικό στον κυβερνοχώρο.

- **Ασφάλεια λογισμικού εφαρμογών.** Οι ενημερώσεις ασφάλειας και προστασίας θα πρέπει να παρέχονται στα συστήματα επί του πλοίου. Οι συνήθεις ενημερωμένες εκδόσεις κώδικα ασφαλείας θα πρέπει να περιλαμβάνονται στον κύκλο περιοδικής συντήρησης Τα κρίσιμα αρχεία ενημερώσεων (patches) θα πρέπει να αξιολογούνται από την άποψη των λειτουργικών επιπτώσεων στα Λειτουργικά Τεχνολογικά Συστήματα. Αυτές οι ενημερώσεις ή ενημερωμένες εκδόσεις κώδικα θα πρέπει να εφαρμόζονται σωστά και εγκαίρως για να διασφαλιστεί ότι τυχόν ελαττώματα σε ένα σύστημα αντιμετωπίζονται πριν από την εκμετάλλευση τους από μια κυβερνοεπίθεση. Εάν δεν είναι δυνατή η εγκατάσταση μιας κρίσιμης ενημερωμένης έκδοσης κώδικα, θα πρέπει να αξιολογηθούν εναλλακτικά μέτρα για την εφαρμογή τεχνικών εικονικής ενημέρωσης κώδικα.

5.1.17 Διαδικαστικά Μέτρα Προστασίας

Οι διαδικαστικοί έλεγχοι επικεντρώνονται στον τρόπο με τον οποίο το προσωπικό χρησιμοποιεί τα συστήματα επί του πλοίου. Τα σχέδια και οι διαδικασίες που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να διατηρούνται εμπιστευτικά και να αντιμετωπίζονται σύμφωνα με τις πολιτικές της εταιρείας. Παραδείγματα για διαδικαστικές ενέργειες μπορεί να είναι:

- **Κατάρτιση και Ευαισθητοποίηση.** Η κατάρτιση και η ευαισθητοποίηση αποτελούν τα βασικά υποστηρικτικά στοιχεία για μια αποτελεσματική προσέγγιση της διαχείρισης των κινδύνων στον κυβερνοχώρο. Η εσωτερική απειλή στον κυβερνοχώρο θα πρέπει να ληφθεί υπόψη. Το προσωπικό έχει βασικό ρόλο στην προστασία των Λειτουργικών και Πληροφοριακών Τεχνολογικών Συστημάτων, αλλά μπορεί επίσης να είναι απρόσεκτο, για παράδειγμα με τη χρήση αφαιρούμενων μέσων αποθήκευσης για τη μεταφορά δεδομένων μεταξύ συστημάτων χωρίς να λαμβάνονται προφυλάξεις κατά της μεταφοράς κακόβουλου λογισμικού. Η κατάρτιση και η ευαισθητοποίηση θα πρέπει να προσαρμόζονται στα κατάλληλα επίπεδα για:
  - ✓ Το προσωπικό επί του πλοίου, συμπεριλαμβανομένου του πλοιάρχου, των αξιωματικών και του πληρώματος
  - ✓ Το προσωπικό στην ξηρά, το οποίο υποστηρίζει τη διαχείριση, τη φόρτωση και τη λειτουργία του πλοίου.

  Οι εν λόγω κατευθυντήριες γραμμές προϋποθέτουν ότι άλλοι σημαντικοί παράγοντες της αλυσίδας εφοδιασμού, όπως οι ναυλωτές, οι νηογνώμονες και οι πάροχοι υπηρεσιών, θα πραγματοποιήσουν τη δική τους βέλτιστη πρακτική για την προστασία και την κατάρτιση στον κυβερνοχώρο. Συνιστάται για τους ιδιοκτήτες και τους φορείς εκμετάλλευσης να εξακριβώσουν την κατάσταση της ετοιμότητας για την ασφάλεια στον κυβερνοχώρο των τρίτων παρόχων τους, συμπεριλαμβανομένων των θαλάσσιων τερματικών σταθμών και των λιμενεργατών, στο πλαίσιο των διαδικασιών προμήθειας για τις εν λόγω υπηρεσίες.

  Θα πρέπει να υπάρχει προγραμματισμός ευαισθητοποίησης για όλο το προσωπικό του πλοίου, το οποίο θα καλύπτει τουλάχιστον τα ακόλουθα:

  - ✓ Κίνδυνοι που σχετίζονται με τα μηνύματα ηλεκτρονικού ταχυδρομείου και τον τρόπο συμπεριφοράς με ασφαλή τρόπο. Παραδείγματα είναι επιθέσεις ηλεκτρονικού "ψαρέματος" (Phishing) όπου ο χρήστης κάνει κλικ σε μια σύνδεση προς μια κακόβουλη τοποθεσία.

- ✓ Κίνδυνοι που σχετίζονται με τη χρήση του διαδικτύου, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης, των φόρουμ συνομιλίας και της αποθήκευσης αρχείων που βασίζονται στο cloud, όπου η κίνηση των δεδομένων είναι λιγότερο ελεγχόμενη και παρακολουθείται.
- ✓ Κίνδυνοι που συνδέονται με τη χρήση ιδίων συσκευών. Αυτές οι συσκευές ενδέχεται να μη διαθέτουν ενημερωμένα σημεία κώδικα ασφαλείας και στοιχεία ελέγχου, όπως η προστασία από ιούς, και ενδέχεται να μεταφέρουν τον κίνδυνο στο περιβάλλον, στο οποίο είναι συνδεδεμένες.
- ✓ Κίνδυνοι που σχετίζονται με την εγκατάσταση και τη διατήρηση λογισμικού σε εταιρικό υλικό που χρησιμοποιεί μολυσμένο υλικό (αφαιρούμενο μέσο) ή λογισμικό (μολυσμένο πακέτο).
- ✓ Κίνδυνοι που σχετίζονται με κακές πρακτικές ασφάλειας λογισμικού και δεδομένων, όπου δεν διενεργούνται έλεγχοι κατά των ιών ή επαληθεύσεις γνησιότητας.
- ✓ Προστασία των πληροφοριών χρήστη, των κωδικών πρόσβασης και των ψηφιακών πιστοποιητικών.
- ✓ Κίνδυνοι στον κυβερνοχώρο σε σχέση με τη φυσική παρουσία μη εταιρικού προσωπικού, π.χ., όπου τρίτοι τεχνικοί αφήνονται να εργάζονται σε εξοπλισμό χωρίς επίβλεψη.
- ✓ Τον εντοπισμό ύποπτης δραστηριότητας ή συσκευών και τον τρόπο αναφοράς ενός πιθανού συμβάντος στον κυβερνοχώρο. Παραδείγματα αυτού είναι παράξενες συνδέσεις που συνήθως δεν εμφανίζονται ή κάποιος που συνδέει μια άγνωστη συσκευή στο δίκτυο της αποστολής.
- ✓ Ευαισθητοποίηση για τις συνέπειες και επιπτώσεις από περιστατικά Κυβερνοχώρου εναντίον της ασφάλειας και της λειτουργίας του πλοίου.
- ✓ Κατανόηση του τρόπου εφαρμογής προληπτικών διαδικασιών συντήρησης, όπως η προστασία από ιούς και λογισμικό κακόβουλης λειτουργίας, η επιδιόρθωση, η δημιουργία αντιγράφων ασφαλείας και ο σχεδιασμός και ο έλεγχος συμβάντων-απόκρισης.
- ✓ Διαδικασίες προστασίας από κινδύνους από τα αφαιρούμενα μέσα των παρόχων υπηρεσιών πριν από τη σύνδεση με τα συστήματα του πλοίου.

Επιπλέον, το προσωπικό πρέπει να γνωρίζει ότι η παρουσία λογισμικού προστασίας καταργεί την απαίτηση για ισχυρές διαδικασίες ασφαλείας, για παράδειγμα τον έλεγχο της χρήσης όλων των αφαιρούμενων μέσων.

Επιπλέον, το αρμόδιο προσωπικό θα πρέπει να γνωρίζει τα σημάδια που εμφανίζονται όταν ένας υπολογιστής έχει παραβιαστεί. Αυτό μπορεί να περιλαμβάνει τα ακόλουθα:

- Αργό και χωρίς αντιδράσεις σύστημα.

- Απρόσμενες αλλαγές συνθηματικών ή εξουσιοδοτημένοι χρήστες αποκλείονται από το σύστημα.
- Απρόσμενα λάθη σε προγράμματα, περιλαμβανομένου του σφάλματος σωστής εκτέλεσης ή προγράμματα που εκτελούνται δίχως να αναμένεται.
- Απρόσμενες ή ξαφνικές αλλαγές σε διαθέσιμο χώρο δίσκου ή μνήμης.
- Μηνύματα ηλεκτρονικού ταχυδρομείου που επιστρέφονται απροσδόκητα.
- Απροσδόκητες δυσκολίες στη συνδεσιμότητα με το δίκτυο.
- Συχνά κωλύματα (crash) συστήματος.
- Παράλογη δραστηριότητα δίσκου ή επεξεργαστή.
- Απροσδόκητες αλλαγές στον περιηγητή, στις ρυθμίσεις λογισμικού ή χρήστη, περιλαμβανομένων των αδειών εξουσιοδότησης (permissions).

Επιπρόσθετα, το καθορισμένο προσωπικό θα πρέπει να είναι σε θέση να κατανοήσει τις εκθέσεις από τα συστήματα IDS, εάν χρησιμοποιούνται. Ο κατάλογος αυτός που παρατέθηκε δεν είναι πλήρης και αποσκοπεί στην αύξηση της ευαισθητοποίησης σχετικά με πιθανά σημεία, τα οποία θα πρέπει να αντιμετωπίζονται ως πιθανά περιστατικά στον κυβερνοχώρο.

- **Πρόσβαση σε επισκέπτες.** Οι επισκέπτες, όπως οι αρχές, οι τεχνικοί, οι πράκτορες, οι υπάλληλοι λιμένων και τερματικών σταθμών, καθώς και οι εκπρόσωποι των ιδιοκτητών θα πρέπει να περιορίζονται όσον αφορά την πρόσβαση σε υπολογιστή κατά τη διάρκεια της επιβίβασης. Θα πρέπει να απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητους υπολογιστές δικτύου Λειτουργικών Τεχνολογικών Συστημάτων. Εάν απαιτείται και επιτρέπεται η πρόσβαση σε ένα δίκτυο από έναν επισκέπτη, τότε θα πρέπει να περιορίζεται από την άποψη των προνομίων του χρήστη. Η πρόσβαση σε ορισμένα δίκτυα για λόγους συντήρησης θα πρέπει να εγκρίνεται και να συντονίζεται σύμφωνα με τις κατάλληλες διαδικασίες που περιγράφονται από την εταιρεία/τον φορέα εκμετάλλευσης του πλοίου.

  Εάν ένας επισκέπτης απαιτεί πρόσβαση υπολογιστή και εκτυπωτή, θα πρέπει να χρησιμοποιείται ένας ανεξάρτητος υπολογιστής, που θα είναι «στεγανός» από όλα τα ελεγχόμενα δίκτυα. Για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση, θα πρέπει να αποτρέπεται η χρήση αφαιρούμενων μέσων σε όλους τους άλλους υπολογιστές και θύρες δικτύου με φυσική πρόσβαση.

- **Αναβαθμίσεις και Συντήρηση λογισμικού.** Το υλικό ή το λογισμικό που δεν υποστηρίζεται πλέον από τον παραγωγό ή τον προγραμματιστή λογισμικού δεν θα λαμβάνει ενημερώσεις για την αντιμετώπιση πιθανών ευπαθειών. Για το λόγο αυτό, η χρήση υλικού και λογισμικού, το

οποίο δεν υποστηρίζεται πλέον, θα πρέπει να αξιολογείται προσεκτικά από την εταιρεία στο πλαίσιο της αξιολόγησης κινδύνου στον κυβερνοχώρο. Οι σχετικές εγκαταστάσεις υλικού και λογισμικού επί του πλοίου θα πρέπει να επικαιροποιούνται ώστε να συμβάλλουν στη διατήρηση επαρκούς επιπέδου ασφάλειας. Ενδέχεται να χρειαστεί να θεσπιστούν διαδικασίες έγκαιρης ενημέρωσης του λογισμικού, λαμβάνοντας υπόψη τον τύπο του πλοίου, την ταχύτητα της σύνδεσης στο διαδίκτυο κ.λπ. Το λογισμικό περιλαμβάνει λειτουργικά συστήματα υπολογιστών, τα οποία θα πρέπει επίσης να ενημερώνονται. Επιπλέον, ένας αριθμός δρομολογητών, διακοπτών και τειχών προστασίας, καθώς και διάφορες Λειτουργικές Τεχνολογικές Συσκευές θα εκτελούν το δικό τους firmware, το οποίο μπορεί να απαιτεί τακτικές ενημερώσεις και θα πρέπει να λαμβάνονται υπόψιν στις διαδικαστικές απαιτήσεις. Η αποτελεσματική συντήρηση του λογισμικού εξαρτάται από τον εντοπισμό, τον σχεδιασμό και την εκτέλεση των μέτρων που απαιτούνται για την υποστήριξη των δραστηριοτήτων συντήρησης καθ' όλη τη διάρκεια του κύκλου ζωής του λογισμικού. Έχει αναπτυχθεί ένα βιομηχανικό πρότυπο από τις BIMCO και CIRM (Committee International Radio-Machine) για να διασφαλιστεί η ασφαλής συντήρηση λογισμικού. Αυτό το πρότυπο καθορίζει τις απαιτήσεις για όλους τους ενδιαφερόμενους που εμπλέκονται στη συντήρηση λογισμικού του εξοπλισμού επί του πλοίου και των συναφών ολοκληρωμένων συστημάτων. Το πρότυπο επίσης καλύπτει συντήρηση λογισμικού επί του πλοίου, στην ξηρά και απομακρυσμένα.

- **Ενημερώσεις εργαλείων Antivirus και Anti-malware.** Για τη σάρωση εργαλείων λογισμικού για τον εντοπισμό και την αντιμετώπιση κακόβουλου λογισμικού, αυτά θα πρέπει να ενημερώνονται συνεχώς. Θα πρέπει επίσης να θεσπιστούν διαδικαστικές απαιτήσεις για να εξασφαλίζεται η έγκαιρη διανομή των επικαιροποιήσεων στα πλοία και η έγκαιρη ενημέρωση όλων των σχετικών υπολογιστών επί του πλοίου.

- **Απομακρυσμένη πρόσβαση.** Θα πρέπει να θεσπιστούν πολιτικές και διαδικασίες για τον έλεγχο της απομακρυσμένης πρόσβασης (remote access) στα Λειτουργικά και Πληροφοριακά Τεχνολογικά Συστήματα (IT/OT) του πλοίου. Σαφείς οδηγίες θα πρέπει να καθορίζουν ποιος έχει δικαίωμα πρόσβασης, πότε μπορεί να έχει πρόσβαση και σε τι μπορεί να έχει πρόσβαση. Οι διαδικασίες απομακρυσμένης πρόσβασης (remote access) από τεχνικούς θα πρέπει να επιβλέπονται από τον καπετάνιο του πλοίου και το προσωπικό που έχει την κατάλληλη

εκπαίδευση σε θέματα κυβερνοασφάλειας του πλοίου. Όλες οι προσπάθειες απομακρυσμένης πρόσβασης θα πρέπει να καταγράφονται για επανεξέταση σε περίπτωση διαταραχής ενός Λειτουργικού ή ενός Πληροφοριακού Τεχνολογικού Συστήματος. Τα συστήματα, τα οποία απαιτούν απομακρυσμένη πρόσβαση, θα πρέπει να καθορίζονται, να παρακολουθούνται και να αναθεωρούνται περιοδικά.

- **Χρήση δικαιωμάτων διαχειριστή.** Τα δικαιώματα διαχειριστή επιτρέπουν πλήρη πρόσβαση στις ρυθμίσεις παραμέτρων του συστήματος και σε όλα τα δεδομένα. Οι χρήστες που συνδέονται σε συστήματα με δικαιώματα διαχειριστή ενδέχεται να επιτρέψουν την πιο εύκολη εκμετάλλευση των υπαρχόντων θεμάτων ευπάθειας. Τα προνόμια διαχειριστή θα πρέπει να παρέχονται μόνο σε κατάλληλα εκπαιδευμένο προσωπικό, το οποίο, στο πλαίσιο του ρόλου του στην εταιρεία ή επί του πλοίου, πρέπει να συνδεθεί σε συστήματα που χρησιμοποιούν αυτά τα προνόμια. Σε κάθε περίπτωση, η χρήση των δικαιωμάτων διαχειριστή θα πρέπει πάντα να περιορίζεται σε λειτουργίες που απαιτούν τέτοια πρόσβαση. Τα δικαιώματα των χρηστών θα πρέπει να καταργούνται όταν τα ενδιαφερόμενα άτομα δεν είναι πλέον επί του πλοίου. Οι λογαριασμοί χρηστών δεν πρέπει να μεταβιβάζονται από τον ένα χρήστη στον άλλο χρησιμοποιώντας γενικά ονόματα χρήστη. Παρόμοιοι κανόνες θα πρέπει να εφαρμόζονται στο προσωπικό ξηράς, το οποίο έχει απομακρυσμένη πρόσβαση σε συστήματα πλοίων, όταν αλλάζει ρόλο και δεν χρειάζεται πλέον πρόσβαση.

  Σε ένα επιχειρηματικό περιβάλλον, όπως η ναυτιλία, η πρόσβαση σε συστήματα επί του πλοίου παρέχεται σε διάφορους ενδιαφερόμενους φορείς. Οι προμηθευτές και οι ανάδοχοι αποτελούν κίνδυνο, διότι συχνά έχουν τόσο στενή γνώση των δραστηριοτήτων ενός πλοίου όσο και πλήρη πρόσβαση στα συστήματα. Για την προστασία της πρόσβασης σε εμπιστευτικά δεδομένα και των κρίσιμων για την ασφάλεια συστημάτων, θα πρέπει να αναπτυχθεί μια ισχυρή πολιτική για τους κωδικούς πρόσβασης. Οι κωδικοί πρόσβασης πρέπει να είναι ισχυροί και να αλλάζουν περιοδικά. Η πολιτική της εταιρείας θα πρέπει να αντιμετωπίζει το γεγονός ότι οι υπερβολικά περίπλοκοι κωδικοί πρόσβασης, οι οποίοι πρέπει να αλλάζουν πολύ συχνά, κινδυνεύουν να γραφτούν σε χαρτί και να διατηρηθούν κοντά στον υπολογιστή.

- **Έλεγχοι σε φυσικά και αφαιρούμενα μέσα.** Κατά τη μεταφορά δεδομένων από μη ελεγχόμενα συστήματα σε ελεγχόμενα συστήματα, υπάρχει κίνδυνος εισαγωγής κακόβουλου

λογισμικού. Τα αφαιρούμενα μέσα μπορούν να χρησιμοποιηθούν για την παράκαμψη επιπέδων άμυνας και συστημάτων επίθεσης που διαφορετικά δεν είναι συνδεδεμένα στο διαδίκτυο. Μια σαφής πολιτική για τη χρήση τέτοιων συσκευών μέσων είναι σημαντικό να υπάρχει και να εφαρμόζεται. Θα πρέπει να συμβάλλει στη διασφάλιση ότι οι συσκευές μέσων ενημέρωσης δεν χρησιμοποιούνται συνήθως για τη μεταφορά πληροφοριών μεταξύ μη ελεγχόμενων και ελεγχόμενων συστημάτων. Υπάρχουν, ωστόσο, περιπτώσεις όπου είναι αναπόφευκτο να χρησιμοποιηθούν αυτές οι συσκευές πολυμέσων, για παράδειγμα κατά τη συντήρηση λογισμικού. Σε αυτές τις περιπτώσεις, θα πρέπει να υπάρχει μια διαδικασία για τον έλεγχο των αφαιρούμενων μέσων για κακόβουλο λογισμικό ή/και την επικύρωση νόμιμου λογισμικού με ψηφιακές υπογραφές και υδατογραφήματα (Watermarks). Οι πολιτικές και οι διαδικασίες που σχετίζονται με τη χρήση αφαιρούμενων μέσων, θα πρέπει να περιλαμβάνουν την απαίτηση σάρωσης οποιασδήποτε αφαιρούμενης συσκευής μέσων, σε υπολογιστή που δεν είναι συνδεδεμένος στα ελεγχόμενα δίκτυα του πλοίου. Εάν δεν είναι δυνατόν να σαρωθεί το αφαιρούμενο μέσο επί του πλοίου, π.χ. το φορητό υπολογιστή ενός τεχνικού συντήρησης, τότε η σάρωση θα μπορούσε να γίνει πριν από την επιβίβαση. Οι εταιρείες θα πρέπει να εξετάσουν το ενδεχόμενο κοινοποίησης στους λιμένες και στους τερματικούς σταθμούς σχετικά με την απαίτηση σάρωσης αφαιρούμενων μέσων πριν επιτραπεί η αποστολή αρχείων στο σύστημα του πλοίου. Αυτή η σάρωση θα πρέπει να πραγματοποιείται κατά τη μεταφορά των ακόλουθων τύπων αρχείων:

- ✓ Αρχεία για το φορτίο και το σχέδιο φόρτωσης
- ✓ Εθνικά, τελωνειακά και λιμενικά έντυπα
- ✓ Έντυπα καυσίμων και λίπαντικών
- ✓ Κατάλογοι αποθηκών του πλοίου και κατάλογοι προμηθειών
- ✓ Αρχεία συντήρησης μηχανής

Ο κατάλογος παραπάνω περιέχει παραδείγματα και δεν πρέπει να θεωρείται εξαντλητικός. Όπου είναι δυνατόν, τα αρχεία και οι φόρμες θα πρέπει να μεταφέρονται ηλεκτρονικά ή να λαμβάνονται απευθείας από αξιόπιστη πηγή χωρίς τη χρήση αφαιρούμενων μέσων.

- **Διάθεση εξοπλισμού, περιλαμβανομένης της καταστροφής δεδομένων.** Ο απαρχαιωμένος εξοπλισμός μπορεί να περιέχει δεδομένα που είναι εμπορικά ευαίσθητα ή εμπιστευτικά. Πριν από τη διάθεση του εξοπλισμού, η εταιρεία θα πρέπει να διαθέτει διαδικασία για να διασφαλίζει ότι τα δεδομένα που περιέχονται σε απαρχαιωμένο εξοπλισμό καταστρέφονται σωστά και δεν μπορούν να ανακτηθούν.

- **Λήψη στήριξης από σχέδια ξηράς και σχέδια έκτακτης ανάγκης.** Τα πλοία θα πρέπει να έχουν πρόσβαση σε τεχνική υποστήριξη σε περίπτωση κυβερνοεπίθεσης. Λεπτομέρειες για την υποστήριξη αυτή και τις συναφείς διαδικασίες θα πρέπει να είναι διαθέσιμες επί του πλοίου.

5.1.18 Κατάρτιση Σχέδιων Έκτακτης Ανάγκης

Κατά την ανάπτυξη σχεδίων έκτακτης ανάγκης και για την εφαρμογή τους επί των πλοίων, είναι σημαντικό να κατανοήσουμε τη σημασία της κυβερνοεπίθεσης και να δώσουμε προτεραιότητα στην αντιμετώπισή της.

Κάθε περιστατικό στον κυβερνοχώρο θα πρέπει να αξιολογείται για την εκτίμηση των επιπτώσεων στις επιχειρήσεις, τα περιουσιακά στοιχεία κ.λπ. Στις περισσότερες περιπτώσεις, και με εξαίρεση τα συστήματα σχεδιασμού και διαχείρισης φορτίου, η απώλεια Πληροφοριακών Τεχνολογικών Συστημάτων επί του πλοίου, συμπεριλαμβανομένης της παραβίασης δεδομένων εμπιστευτικών πληροφοριών, θα αποτελεί ζήτημα επιχειρησιακής συνέπειας και δεν θα πρέπει να έχει αντίκτυπο στην ασφαλή λειτουργία του πλοίου. Σε περίπτωση κυβερνοεπίθεσης, προτεραιότητα είναι η άμεση εφαρμογή σχεδίου έρευνας και αποκατάστασης.

Η απώλεια Λειτουργικών Τεχνολογικών Συστημάτων μπορεί να έχει σημαντικό και άμεσο αντίκτυπο στην ασφαλή λειτουργία του πλοίου. Σε περίπτωση που ένα περιστατικό στον κυβερνοχώρο έχει ως αποτέλεσμα την απώλεια ή τη δυσλειτουργία των Λειτουργικών Τεχνολογικών Συστημάτων, θα είναι σημαντικό να ληφθούν αποτελεσματικά μέτρα για να διασφαλιστεί η άμεση ασφάλεια του πληρώματος, του πλοίου, του φορτίου και της προστασίας του θαλάσσιου περιβάλλοντος. Γενικά, τα κατάλληλα σχέδια έκτακτης ανάγκης για συμβάντα στον κυβερνοχώρο, συμπεριλαμβανομένης της απώλειας κρίσιμων συστημάτων και της ανάγκης χρήσης εναλλακτικών τρόπων λειτουργίας, θα πρέπει να αντιμετωπίζονται με τις σχετικές επιχειρησιακές διαδικασίες και διαδικασίες έκτακτης ανάγκης που περιλαμβάνονται στο σύστημα διαχείρισης της ασφάλειας.

Ορισμένες από τις υφιστάμενες διαδικασίες στο σύστημα διαχείρισης της ασφάλειας του πλοίου θα καλύπτουν ήδη τέτοια περιστατικά στον κυβερνοχώρο. Ωστόσο, τα περιστατικά στον κυβερνοχώρο μπορεί να οδηγήσουν σε «ντόμινο» και να προκαλέσουν τον τερματισμό περισσότερων συστημάτων ταυτόχρονα. Ο σχεδιασμός έκτακτης ανάγκης θα πρέπει να λαμβάνει υπόψη τα περιστατικά αυτά.

5.1.19 Αποσύνδεση Λειτουργικών Τεχνολογικών Συστημάτων (ΟΤ) Από Το Δίκτυο Ξηράς

Οι συνδέσεις μεταξύ ξηράς και Λειτουργικών Τεχνολογικών Συστημάτων μπορεί να είναι σχετικές με ένα ευρύ φάσμα εφαρμογών, όπως παρακολούθηση επιδόσεων και η προληπτική συντήρηση και απομακρυσμένη υποστήριξη. Βέβαια αυτά τα συστήματα δεν είναι απολύτως απαραίτητα για την ασφαλή λειτουργία του πλοίου. Ωστόσο, αντιπροσωπεύουν ένα πιθανό φορέα επίθεσης στα συστήματα που απαιτούνται για την ασφαλή λειτουργία του πλοίου. Ως εκ τούτου, είναι σημαντικό να εκτιμηθεί πότε επιτρέπονται αυτές οι συνδέσεις και υπό ποιες συνθήκες. Θα πρέπει να θεσπιστούν σχέδια που να προσδιορίζουν πότε τα εν λόγω Λειτουργικά Τεχνολογικά Συστήματα θα πρέπει να διαχωρίζονται προσωρινά από τη σύνδεση του δικτύου ξηράς για την προστασία της ασφαλούς λειτουργίας του πλοίου. Η αποσύνδεση θα βοηθήσει να αποτραπεί ο εισβολέας από το να είναι σε θέση να χειριστεί τα κρίσιμα συστήματα ασφαλείας ή να αναλάβει τον άμεσο έλεγχο του συστήματος. Η αποσύνδεση θα μπορούσε επίσης να πραγματοποιηθεί για να αποφευχθεί η εξάπλωση κακόβουλου λογισμικού μεταξύ τμημάτων δικτύου. Για να απομονωθούν αποτελεσματικά οι συνδέσεις μεταξύ ξηράς και πλοίου, είναι σημαντικό το δίκτυο και οι υπηρεσίες συνδεσιμότητας να έχουν σχεδιαστεί με τέτοιο τρόπο ώστε τα δίκτυα να μπορούν να διαχωριστούν, με την αφαίρεση π.χ. ενός καλωδίου δικτύου ή την απενεργοποίηση του τείχους προστασίας.

5.1.20 Σύστημα Διαχείρισης Ασφάλειας

Το σύστημα διαχείρισης ασφάλειας περιλαμβάνει διαδικασίες για την αναφορά ατυχημάτων ή επικίνδυνων καταστάσεων και καθορίζει επίπεδα επικοινωνίας και εξουσιοδότησης για τη λήψη αποφάσεων. Ακολουθούν μερικά παραδείγματα συμβάντων στον κυβερνοχώρο, τα οποία θα πρέπει να συμπεριλαμβάνονται σε σχέδια έκτακτης ανάγκης:

- Απώλεια ηλεκτρονικού εξοπλισμού πλοήγησης ή απώλεια ακεραιότητας δεδομένων που σχετίζονται με τη ναυσιπλοΐα.
- Απώλεια διαθεσιμότητας ή ακεραιότητας εξωτερικών πηγών δεδομένων, συμπεριλαμβανομένων του GNSS (Global Navigation Satellite System).

- Απώλεια ουσιαστικής συνδεσιμότητας με την ακτή, συμπεριλαμβανομένης της διαθεσιμότητας επικοινωνιών του Παγκόσμιου Ναυτιλιακού Συστήματος Κινδύνου και Ασφάλειας (Global Maritime Distress and Safety System - GMDSS).
- Απώλεια της διαθεσιμότητας βιομηχανικών συστημάτων ελέγχου, συμπεριλαμβανομένης της πρόωσης, των βοηθητικών συστημάτων και άλλων κρίσιμων συστημάτων, καθώς και απώλεια της δυνατότητας διαχείρισης και του ελέγχου δεδομένων.
- Κυβερνοεπίθεση με ransomware ή με λογισμικό το οποίο δεν θα επιτρέπει την διεκπεραίωση υπηρεσιών ή την είσοδο στο σύστημα.

Επιπλέον, είναι σημαντικό να διασφαλιστεί ότι η απώλεια εξοπλισμού ή αξιόπιστων πληροφοριών λόγω κυβερνοεπίθεσης δεν θα καθιστά αναποτελεσματικά τα υφιστάμενα σχέδια και διαδικασίες έκτακτης ανάγκης. Τα σχέδια έκτακτης ανάγκης και οι σχετικές πληροφορίες θα πρέπει να είναι διαθέσιμα σε μη ηλεκτρονική μορφή, δεδομένου ότι ορισμένοι τύποι κυβερνοεπιθέσεων μπορούν να περιλαμβάνουν τη διαγραφή δεδομένων και τη διακοπή λειτουργίας των συνδέσεων επικοινωνίας. Μπορεί να υπάρχουν περιπτώσεις στις οποίες η ανταπόκριση σε ένα περιστατικό στον κυβερνοχώρο, να είναι πέρα από τις ικανότητες των μελών του πληρώματος επί του πλοίου ή των απασχολούμενων στα γραφεία λόγω της πολυπλοκότητας ή της σοβαρότητας της επίθεσης. Σε αυτές τις περιπτώσεις, μπορεί να απαιτηθεί εξωτερική βοήθεια εμπειρογνωμόνων (για παράδειγμα, εγκληματολογική ανάλυση μετά το συμβάν και καθαρισμός του συστήματος).

5.1.21 Αποτελεσματική Ανταπόκριση

Θα πρέπει να συσταθεί ομάδα, η οποία μπορεί να περιλαμβάνει συνδυασμό προσωπικού επί του πλοίου και του προσωπικού ξηράς ή/και εξωτερικών εμπειρογνωμόνων, ώστε να λαμβάνονται τα κατάλληλα μέτρα για την αποκατάσταση των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων, και το πλοίο να μπορεί να συνεχίσει τις κανονικές λειτουργίες του. Η ομάδα θα πρέπει να είναι σε θέση να αποτρέψει και να αντιμετωπίσει την κυβερνοεπίθεση. Μια αποτελεσματική αντιμετώπιση θα πρέπει τουλάχιστον να αποτελείται από τα ακόλουθα βήματα:

1. ***Αρχική αξιολόγηση***. Για να εξασφαλιστεί η κατάλληλη απάντηση, η ομάδα απόκρισης θα πρέπει να ανακαλύψει:
    - πώς συνέβη το περιστατικό,
    - ποια συστήματα προσβλήθηκαν και πως,
    - τον βαθμό στον οποίο επηρεάζονται τα εμπορικά ή/και τα επιχειρησιακά δεδομένα,

- αν υπάρχουν υπολείμματα του ιού στο σύστημα.

2. ***Ανάκτηση συστημάτων και δεδομένων***. Μετά από μια αρχική αξιολόγηση της κυβερνοεπίθεσης, τα συστήματα και τα δεδομένα (Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα) θα πρέπει να καθαρίζονται, να ανακτώνται και να αποκαθίστανται, στο μέτρο του δυνατού, σε λειτουργική κατάσταση με την αφαίρεση απειλών από το σύστημα και την αποκατάσταση του λογισμικού.
3. ***Ανάλυση του περιστατικού***. Για να κατανοηθούν τα αίτια και οι συνέπειες ενός συμβάντος στον κυβερνοχώρο, η εταιρεία θα πρέπει να διεξάγει έρευνα, με την υποστήριξη εξωτερικού εμπειρογνώμονα. Οι πληροφορίες από την έρευνα θα διαδραματίσουν σημαντικό ρόλο στην πρόληψη μιας πιθανής επανάληψης.
4. ***Αποτροπή επανάληψης επίθεσης***. Λαμβάνοντας υπόψη το αποτέλεσμα της προαναφερόμενης έρευνας, θα πρέπει να εξεταστούν μέτρα για την αντιμετώπιση τυχόν ελλείψεων σε τεχνικά ή/και διαδικαστικά μέτρα προστασίας, σύμφωνα με τις διαδικασίες της εταιρείας για την εφαρμογή διορθωτικών μέτρων.

Όταν μια κυβερνοεπίθεση είναι σύνθετη, για παράδειγμα εάν τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα δεν μπορούν να επιστρέψουν στην κανονική λειτουργία, μπορεί να είναι απαραίτητο να ξεκινήσει το σχέδιο αποκατάστασης παράλληλα με τα σχέδια έκτακτης ανάγκης επί του πλοίου. Όταν συμβαίνει αυτό, η ομάδα αντίδρασης θα πρέπει να είναι σε θέση να παρέχει συμβουλές στο πλοίο σχετικά με:

- εάν τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα θα πρέπει να κλείσουν ή να διατηρηθούν σε λειτουργία για την προστασία των δεδομένων.
- κατά πόσον ορισμένες συνδέσεις επικοινωνίας πλοίων με την ξηρά θα πρέπει να κλείσουν.
- την κατάλληλη χρήση των προηγμένων εργαλείων που παρέχονται σε προ εγκατεστημένο λογισμικό ασφαλείας.
- το βαθμό στον οποίο το περιστατικό έχει θέσει σε κίνδυνο τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα πέραν των δυνατοτήτων των υφιστάμενων σχεδίων αποκατάστασης.

Είναι σημαντικό για το αρμόδιο προσωπικό να εκτελεί τακτικές ασκήσεις ασφάλειας στον κυβερνοχώρο, προκειμένου να διατηρήσει την ικανότητα απόκρισης αποτελεσματική. Οι ασκήσεις ασφάλειας στον κυβερνοχώρο θα μπορούσαν, όπου ενδείκνυται, να εμπνέονται από

γεγονότα της πραγματικής ζωής και να είναι προσομοιώσεις συμβάντων μεγάλης κλίμακας που κλιμακώνονται για να γίνουν κρίσεις στον κυβερνοχώρο. Αυτό προσφέρει την ευκαιρία να αναλυθούν προηγμένα τεχνικά περιστατικά ασφάλειας στον κυβερνοχώρο. Επίσης ,μπορεί να συμβάλει στην αντιμετώπιση της επιχειρησιακής συνέχειας και της διαχείρισης κρίσεων.

5.1.22 Σχέδιο Αποκατάστασης

Τα σχέδια αποκατάστασης θα πρέπει να είναι διαθέσιμα σε έντυπη μορφή επί του πλοίου και στην ξηρά. Σκοπός του σχεδίου είναι η υποστήριξη της ανάκτησης των συστημάτων και των δεδομένων που είναι απαραίτητα για την αποκατάσταση των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων σε λειτουργική κατάσταση. Για να εξασφαλιστεί η ασφάλεια του προσωπικού επί του πλοίου, θα πρέπει να δοθεί προτεραιότητα στη λειτουργία και τη ναυσιπλοΐα του πλοίου στο σχέδιο. Το σχέδιο αποκατάστασης θα πρέπει να γίνεται κατανοητό από το προσωπικό που είναι υπεύθυνο για την ασφάλεια στον κυβερνοχώρο. Η λεπτομέρεια και η πολυπλοκότητα ενός σχεδίου αποκατάστασης θα εξαρτηθεί από τον τύπο του πλοίου και τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα και άλλα συστήματα που είναι εγκατεστημένα επί του πλοίου.

Η ομάδα αντιμετώπισης περιστατικών θα πρέπει να εξετάσει προσεκτικά τις επιπτώσεις των ενεργειών ανάκτησης (όπως π.χ. η σάρωση των αφαιρούμενων δίσκων), οι οποίες μπορεί να οδηγήσουν στην καταστροφή αποδεικτικών στοιχείων που θα μπορούσαν να παράσχουν πολύτιμες πληροφορίες σχετικά με τα αίτια ενός συμβάντος. Όπου είναι δυνατόν, θα πρέπει να παρέχεται επαγγελματική υποστήριξη για την αντιμετώπιση συμβάντων στον κυβερνοχώρο, προκειμένου να βοηθηθεί η διατήρηση των αποδεικτικών στοιχείων, αποκαθιστώντας παράλληλα την επιχειρησιακή ικανότητα.

Η ικανότητα ανάκτησης δεδομένων αποτελεί πολύτιμο μέτρο τεχνικής προστασίας. Οι δυνατότητες ανάκτησης δεδομένων είναι συνήθως με τη μορφή δημιουργίας αντιγράφων ασφαλείας λογισμικού για Πληροφοριακά Τεχνολογικά Δεδομένα. Η διαθεσιμότητα αντιγράφου ασφαλείας λογισμικού, είτε επί του πλοίου είτε στην ξηρά, θα πρέπει να επιτρέπει την ανάκτηση των Πληροφοριακών Τεχνολογικών Συστημάτων σε λειτουργική κατάσταση μετά από κυβερνοεπίθεση.

Η ανάκτηση των Λειτουργικών Τεχνολογικών Συστημάτων μπορεί να είναι πιο περίπλοκη, ειδικά αν δεν υπάρχουν διαθέσιμα εφεδρικά συστήματα και μπορεί να απαιτήσει βοήθεια από την ξηρά.

Λεπτομέρειες σχετικά με το πού είναι διαθέσιμη η βοήθεια αυτή και από ποιον, θα πρέπει να αποτελεί μέρος του σχεδίου αποκατάστασης, για παράδειγμα με τη διαδικασία σε λιμένα για τη λήψη βοήθειας από εξειδικευμένο μηχανικό δικτύου. Εάν υπάρχει διαθέσιμο ειδικευμένο προσωπικό επί του πλοίου, μπορούν να πραγματοποιηθούν πιο εκτεταμένες διαγνωστικές ενέργειες και ενέργειες αποκατάστασης.

5.1.23 Διερεύνηση Περιστατικών Κυβερνοεπίθεσης

Η διερεύνηση μιας κυβερνοεπίθεσης μπορεί να παρέχει πολύτιμες πληροφορίες σχετικά με τον τρόπο με τον οποίο έγινε εκμετάλλευση μιας ευπάθειας του συστήματος. Οι εταιρείες θα πρέπει, όπου είναι δυνατόν, να διερευνούν κυβερνοεπιθέσεις που επηρεάζουν τα Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα επί του πλοίου, σύμφωνα με τις διαδικασίες της εταιρείας. Μια λεπτομερής έρευνα μπορεί να απαιτήσει την υποστήριξη εξωτερικών εμπειρογνωμόνων. Οι πληροφορίες από μια έρευνα μπορούν να χρησιμοποιηθούν για τη βελτίωση των τεχνικών και διαδικαστικών μέτρων προστασίας επί του πλοίου και την ξηρά. Μπορεί επίσης να βοηθήσει την ευρύτερη ναυτιλιακή βιομηχανία με την καλύτερη κατανόηση των θαλάσσιων κινδύνων στον κυβερνοχώρο. Κάθε έρευνα θα πρέπει να έχει ως αποτέλεσμα:

- Καλύτερη κατανόηση των δυνητικών κινδύνων στον κυβερνοχώρο που αντιμετωπίζει ο ναυτιλιακός κλάδος τόσο επί του πλοίου όσο και στην ξηρά.
- Διδάγματα που αντλήθηκαν από κυβερνοεπιθέσεις με σκοπό την βελτίωση της εκπαίδευσης του προσωπικού για αύξηση επαγρύπνησης.
- Επικαιροποιήσεις των τεχνικών και διαδικαστικών μέτρων προστασίας για την πρόληψη της επανάληψης μιας κυβερνοεπίθεσης.

5.1.24 Απώλειες Λόγω Κυβερνοεπίθεσης

Για τους ασφαλιστές, ο όρος "κυβερνοχώρος" περιλαμβάνει πολλές διαφορετικές πτυχές και είναι σημαντικό να γίνει διάκριση μεταξύ αυτών και των επιπτώσεών τους στην ασφαλιστική κάλυψη. Ορισμένοι ασφαλιστές πιστεύουν ότι δεν υπάρχει συστημικός κίνδυνος, για τα πλοία, που προκύπτει από ένα περιστατικό κυβερνοεπίθεσης και ο αντίκτυπος ενός συμβάντος πιθανότατα θα περιοριστεί σε ένα μόνο πλοίο. Οι εταιρείες γνωρίζουν ότι ενδέχεται να υπάρχει ειδική, μη θαλάσσια, ασφαλιστική κάλυψη για την κάλυψη της απώλειας δεδομένων και τυχόν πρόστιμα τα οποία προκύπτουν. Οι εταιρείες θα πρέπει να είναι σε θέση να αποδείξουν ότι ενεργούν με

προσοχή στην προσέγγισή τους για τη διαχείριση του κινδύνου στον κυβερνοχώρο και για την προστασία του πλοίου από οποιαδήποτε ζημία που μπορεί να προκύψει από μια κυβερνοεπίθεση.

5.1.25 Κάλυψη Για Υλικές Ζημίες

Γενικά, σε πολλές αγορές που προσφέρουν ασφάλεια περιουσιακών στοιχείων, το ασφαλιστήριο συμβόλαιο μπορεί να καλύπτει την απώλεια ή τη ζημία στο πλοίο και τον εξοπλισμό του που προκαλούνται από ένα περιστατικό ναυτιλίας, όπως προσάραξη, σύγκρουση, πυρκαγιά ή εισροή υδάτων, ακόμη και όταν η αιτία του συμβάντος είναι κυβερνοεπίθεση. Πρέπει να σημειωθεί ότι επί του παρόντος σε ορισμένες αγορές υπάρχουν ρήτρες αποκλεισμού για επιθέσεις στον κυβερνοχώρο. Εάν η θαλάσσια πολιτική περιέχει ρήτρα αποκλεισμού για επιθέσεις στον κυβερνοχώρο, η απώλεια ή η ζημία ενδέχεται να μην καλύπτεται. Συνιστάται στις εταιρείες να ελέγχουν εκ των προτέρων τους ασφαλιστές/μεσίτες τους εάν η πολιτική τους καλύπτει αξιώσεις που προκαλούνται από επιθέσεις στον κυβερνοχώρο.

Έχουν δημοσιευθεί κατευθυντήριες γραμμές για την αγορά, στις οποίες συνιστάται στους ναυτιλιακούς ασφαλιστές να θέτουν ερωτήσεις σχετικά με την ευαισθητοποίηση μιας εταιρείας στον κυβερνοχώρο όσον αφορά τον κίνδυνο και τις μη τεχνικές διαδικασίες. Ως εκ τούτου, οι εταιρείες θα πρέπει να αναμένουν αίτημα για μη τεχνικές πληροφορίες σχετικά με την προσέγγισή τους για τη διαχείριση κινδύνων στον κυβερνοχώρο από τους ασφαλιστές. Τα περιορισμένα δεδομένα σχετικά με τη συχνότητα και τη σοβαρότητα της απώλειας ή την πιθανότητα σωματικής βλάβης που προκύπτει από συμβάντα στον κυβερνοχώρο, αποτελούν πρόκληση και σημαίνουν ότι δεν είναι διαθέσιμη η τυπική τιμολόγηση του κόστους μιας κυβερνοεπίθεσης.

5.1.26 Κάλυψη Ευθύνης

Συνιστάται η επικοινωνία με το P&I Club (Protection and Indemnity Insurance - μη κερδοσκοπικές εταιρείες με κεφάλαιο, μέλη των οποίων είναι οι ίδιοι οι πλοιοκτήτες. Στην περίπτωση των P&I Club, ασφαλιστής είναι ο ίδιος ο αλληλασφαλιστικός οργανισμός και κατά αυτού στρέφονται οι απαιτήσεις περί αποζημίωσης, ενώ η ναυτασφάλιση σε P&I Club προσφέρεται σε χαμηλό κόστος για τους πλοιοκτήτες σε σχέση με άλλους τρόπους ασφάλισης), για λεπτομερείς πληροφορίες αναφορικά με την κάλυψη που παρέχεται στους πλοιοκτήτες και τους ναυλωτές σχετικά με την ευθύνη έναντι τρίτων (και των σχετικών εξόδων) που προκύπτουν από τη λειτουργία των πλοίων.

Ένα περιστατικό που προκαλείται, για παράδειγμα από δυσλειτουργία των συστημάτων πλοήγησης ή των συστημάτων μηχανικής ενός πλοίου λόγω εγκληματικής πράξης ή κυβερνοεπίθεσης, δεν προκαλεί από μόνο του αποκλεισμό της κανονικής κάλυψης του P&I club. Σε περίπτωση αξίωσης που αφορά περιστατικό στον κυβερνοχώρο, οι ενάγοντες μπορούν κάλλιστα να επιδιώξουν να υποστηρίξουν ότι η αξίωση προέκυψε ως αποτέλεσμα ανεπαρκούς επιπέδου ετοιμότητας στον κυβερνοχώρο. Αυτό, ως εκ τούτου, τονίζει περαιτέρω τη σημασία της ικανότητας των εταιρειών να αποδεικνύουν ότι ενεργούν με εύλογη προσοχή στην προσέγγισή τους για τη διαχείριση του κινδύνου στον κυβερνοχώρο και την προστασία του πλοίου.

Πρέπει να σημειωθεί ότι πολλές ζημίες, οι οποίες θα μπορούσαν να προκύψουν από μια κυβερνοεπίθεση, δεν έχουν τη φύση των υποχρεώσεων τρίτων που προκύπτουν από τη λειτουργία του πλοίου και, ως εκ τούτου, δεν καλύπτονται από την ασφάλιση του P&I. Για παράδειγμα, η οικονομική ζημία που προκαλείται από ransomware, ή το κόστος της αποκατάστασης αλλοιωμένων δεδομένων δεν θα συμπεριληφθούν στην ασφαλιστική κάλυψη.

Θα πρέπει, ωστόσο, να σημειωθεί ότι η κανονική κάλυψη του P&I club όσον αφορά τις υποχρεώσεις του, για περιστατικά κυβερνοεπίθεσης κατά τη διάρκεια ενός πολέμου ή τρομοκρατίας δεν θα καλύπτονται υπό τους συνήθεις όρους.

5.2 Το Πρότυπο ISO 27001

Το πλήρες όνομα του προτύπου αυτού είναι “ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements.” Πρόκειται για το κορυφαίο διεθνές πρότυπο που επικεντρώνεται στην ασφάλεια των πληροφοριών, που δημοσιεύθηκε από τον Διεθνή Οργανισμό Τυποποίησης (International Organization of Standardization - ISO), σε συνεργασία με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission - IEC). Και οι δύο είναι κορυφαίοι διεθνείς οργανισμοί που αναπτύσσουν διεθνή πρότυπα. Το ISO-27001 αποτελεί μέρος ενός συνόλου προτύπων που έχουν αναπτυχθεί για το χειρισμό της ασφάλειας των πληροφοριών της οικογένειας ISO/IEC 27000.

5.2.1 Σκοπός Του ISO 27001

Το ISO 27001 αναπτύχθηκε για να βοηθήσει τους οργανισμούς, οποιουδήποτε μεγέθους ή οποιουδήποτε κλάδου, να προστατεύσουν τις πληροφορίες τους με συστηματικό και οικονομικά

αποδοτικό τρόπο, μέσω της υιοθέτησης ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System - ISMS). Ο βασικός στόχος του ISO 27001 είναι η προστασία τριών πτυχών των πληροφοριών:

- Εμπιστευτικότητα (Confidentiality): μόνο τα εξουσιοδοτημένα πρόσωπα έχουν το δικαίωμα πρόσβασης σε πληροφορίες.
- Ακεραιότητα (Integrity): μόνο τα εξουσιοδοτημένα πρόσωπα μπορούν να αλλάξουν τις πληροφορίες.
- Διαθεσιμότητα (Availability): οι πληροφορίες πρέπει να είναι προσβάσιμες σε εξουσιοδοτημένα πρόσωπα όποτε χρειάζεται.

5.2.2 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)

Το σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) είναι ένα σύνολο κανόνων που πρέπει να θεσπίσει μια εταιρεία για να:

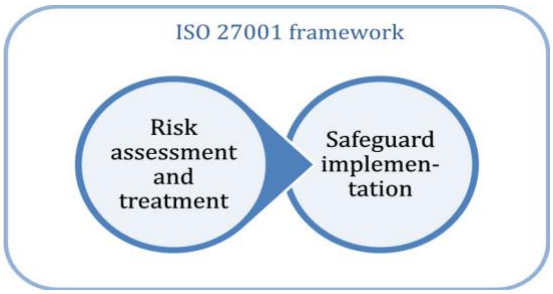
- προσδιορίσει τα ενδιαφερόμενα μέρη και τις προσδοκίες τους από την εταιρεία όσον αφορά την ασφάλεια,
- προσδιορίσει τους κινδύνους που υφίστανται για τις πληροφορίες,
- καθορίσει ελέγχους (διασφαλίσεις) και άλλες μεθόδους μετριασμού και μείωσης για την ικανοποίηση των καθορισμένων προσδοκιών και να χειριστεί κινδύνους,
- καθορίσει σαφείς στόχους σχετικά με το τι πρέπει να επιτευχθεί με την ασφάλεια των πληροφοριών,
- εφαρμόσει όλους τους ελέγχους και άλλες μεθόδους επεξεργασίας κινδύνου,
- μετρά συνεχώς εάν οι εφαρμοζόμενοι έλεγχοι λειτουργούν όπως αναμένεται,
- κάνει συνεχή βελτίωση ώστε το ISMS να λειτουργεί καλύτερα στο σύνολό του.

Αυτό το σύνολο κανόνων μπορεί να καταγραφεί με τη μορφή πολιτικών, διαδικασιών και άλλων τύπων εγγράφων ή μπορεί να έχει τη μορφή καθιερωμένων διαδικασιών και τεχνολογιών που δεν τεκμηριώνονται. Το πρότυπο ISO 27001 ορίζει ποια έγγραφα απαιτούνται, και πρέπει να υπάρχουν κατ' ελάχιστο.

5.2.3 Λειτουργία Του ISO 27001

Το πρότυπο ISO 27001 εστιάζει στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών σε μια εταιρεία. Αυτό γίνεται με την εύρεση των πιθανών προβλημάτων που θα μπορούσαν να συμβούν στις πληροφορίες (δηλαδή, την αξιολόγηση κινδύνου) και στη συνέχεια τον καθορισμό του τι πρέπει να γίνει για την πρόληψη τέτοιων προβλημάτων (π.χ. μετριασμός του κινδύνου ή θεραπεία κινδύνου). Ως εκ τούτου, η κύρια

φιλοσοφία του ISO 27001 βασίζεται σε μια διαδικασία για τη διαχείριση των κινδύνων που στην ουσία λέει να μάθουν - οι ενδιαφερόμενοι - πού βρίσκονται οι κίνδυνοι και στη συνέχεια να τους αντιμετωπίζουν συστηματικά, μέσω της εφαρμογής ελέγχων ασφαλείας (ή μέτρων προστασίας).



Σχήμα 5.1 Το πλαίσιο λειτουργίας του Προτύπου 27001. Πηγή: https://advisera.com/

Το ISO 27001 απαιτεί από μια εταιρεία να απαριθμήσει όλα τα στοιχεία ελέγχου που πρόκειται να εφαρμοστούν σε ένα έγγραφο που ονομάζεται Δήλωση Εφαρμογής (Statement of Applicability) .

5.2.4 Απαιτήσεις Του ISO 27001

Οι υποχρεωτικές απαιτήσεις για το ISO 27001 ορίζονται στις ενότητες 4 έως 10 – αυτό σημαίνει ότι όλες αυτές οι απαιτήσεις πρέπει να εφαρμόζονται σε έναν οργανισμό, εάν θέλει να συμμορφώνεται με το πρότυπο. Οι έλεγχοι του παραρτήματος Α πρέπει να εφαρμόζονται μόνον εφόσον δηλώνεται όπως ισχύει στη Δήλωση Εφαρμογής. Οι απαιτήσεις από τις ενότητες 4 έως 10 μπορούν να συνοψιστούν ως εξής:

- **Ενότητα 4: Πλαίσιο του οργανισμού** – ορίζει απαιτήσεις για την κατανόηση εξωτερικών και εσωτερικών θεμάτων, των ενδιαφερόμενων μερών και των απαιτήσεών τους, καθώς και για τον καθορισμό του πεδίου εφαρμογής του ISMS.
- **Ενότητα 5: Ηγεσία** – ορίζει τις διοικητικές ευθύνες, θέτοντας τους ρόλους και τις ευθύνες και το περιεχόμενο της πολιτικής ασφάλειας πληροφοριών ανώτατου επιπέδου.
- **Ενότητα 6: Σχεδιασμός** – καθορίζει τις απαιτήσεις για την αξιολόγηση του κινδύνου, την αντιμετώπιση κινδύνων, τη δήλωση εφαρμογής, το σχέδιο επεξεργασίας κινδύνου και τον καθορισμό των στόχων ασφάλειας των πληροφοριών.
- **Ενότητα 7: Υποστήριξη** – καθορίζει απαιτήσεις για τη διαθεσιμότητα πόρων, ικανοτήτων, ευαισθητοποίησης, επικοινωνίας και ελέγχου εγγράφων και αρχείων.
- **Ενότητα 8: Λειτουργία** – καθορίζει την εφαρμογή της εκτίμησης και της αντιμετώπισης κινδύνων, καθώς και των ελέγχων και άλλων διαδικασιών που απαιτούνται για την επίτευξη των στόχων ασφάλειας των πληροφοριών.

- **Ενότητα 9: Αξιολόγηση των επιδόσεων** – καθορίζει τις απαιτήσεις για την παρακολούθηση, τη μέτρηση, την ανάλυση, την αξιολόγηση, τον εσωτερικό έλεγχο και την αξιολόγηση της διαχείρισης.
- **Ενότητα 10: Βελτίωση** – ορίζει απαιτήσεις για μη συμμόρφωση, διορθώσεις, διορθωτικές ενέργειες και συνεχή βελτίωση.

5.2.5 Προστατευτικά Μέτρα, Έλεγχοι Και Εφαρμογή Τους

Τα προστατευτικά μέτρα (ή έλεγχοι) του προτύπου ISO 27001 είναι οι πρακτικές που πρέπει να εφαρμόζονται για τη μείωση των κινδύνων σε αποδεκτά επίπεδα. Τα μέτρα αυτά μπορεί να είναι τεχνικά, οργανωτικά, νομικά, φυσικά και ανθρώπινοι πόροι και περιγράφονται συνοπτικά ως εξής:

- Οι **τεχνικοί έλεγχοι** υλοποιούνται κυρίως σε συστήματα πληροφοριών, χρησιμοποιώντας λογισμικό, υλικό και στοιχεία firmware που προστίθενται στο σύστημα. Π.χ. αντίγραφα ασφαλείας, λογισμικό προστασίας από ιούς κ.λπ.
- Οι **οργανωτικοί έλεγχοι** υλοποιούνται με τον καθορισμό κανόνων που πρέπει να ακολουθούνται και την αναμενόμενη συμπεριφορά από χρήστες, εξοπλισμό, λογισμικό και συστήματα. Π.χ. Πολιτική Ελέγχου Πρόσβασης, κλπ.
- Οι **νομικοί έλεγχοι** εφαρμόζονται διασφαλίζοντας ότι οι κανόνες και οι αναμενόμενες συμπεριφορές ακολουθούν και επιβάλλουν τους νόμους, τους κανονισμούς, τις συμβάσεις και άλλα παρόμοια νομικά μέσα με τα οποία πρέπει να συμμορφώνεται ο οργανισμός. Π.χ. Non-Disclosure Agreement (συμφωνία μη αποκάλυψης) κ.λπ.
- Οι **έλεγχοι των ανθρώπινων πόρων** υλοποιούνται παρέχοντας γνώσεις, εκπαίδευση, δεξιότητες ή εμπειρία σε άτομα που θα τους επιτρέψουν να εκτελούν τις δραστηριότητές τους με ασφαλή τρόπο. Π.χ. εκπαίδευση ευαισθητοποίησης για την ασφάλεια, εκπαίδευση εσωτερικών ελεγκτών ISO 27001 κ.λπ.

5.2.6 Οι Τομείς (DOMAINS) Του ISO 27001

Υπάρχουν 14 "τομείς" που απαριθμούνται στο παράρτημα Α του ISO 27001, οργανωμένοι στα τμήματα Α.5 έως Α.18. Οι ενότητες καλύπτουν τα ακόλουθα:

- **Ενότητα Α5. Πολιτικές ασφάλειας πληροφοριών**: Τα στοιχεία ελέγχου σε αυτήν την ενότητα περιγράφουν τον τρόπο χειρισμού των πολιτικών ασφαλείας πληροφοριών.
- **Ενότητα Α6. Οργάνωση της ασφάλειας των πληροφοριών**: Οι έλεγχοι σε αυτή την ενότητα παρέχουν το βασικό πλαίσιο για την εφαρμογή και τη λειτουργία της ασφάλειας των πληροφοριών, καθορίζοντας την εσωτερική της οργάνωση (π.χ. ρόλους, αρμοδιότητες κ.λπ.), καθώς και τις οργανωτικές πτυχές της ασφάλειας των πληροφοριών, όπως η διαχείριση έργων, η χρήση κινητών συσκευών και η τηλεργασία.
- **Ενότητα Α7. Ασφάλεια ανθρώπινου δυναμικού**: Οι έλεγχοι σε αυτήν την ενότητα διασφαλίζουν ότι τα άτομα που βρίσκονται υπό τον έλεγχο του οργανισμού

προσλαμβάνονται, εκπαιδεύονται και εργάζονται με ασφαλή τρόπο. Επίσης, εξετάζονται οι αρχές της πειθαρχικής δίωξης και της καταγγελίας των συμφωνιών.

- **Ενότητα Α9. Έλεγχος πρόσβασης**: Τα στοιχεία ελέγχου σε αυτήν την ενότητα περιορίζουν την πρόσβαση σε πληροφορίες σύμφωνα με τις πραγματικές επιχειρηματικές ανάγκες. Τα στοιχεία ελέγχου είναι τόσο για φυσική όσο και για πρόσβαση σε υπολογιστή όπου απαιτείται είσοδος στο σύστημα με όνομα χρήστη και κωδικό πρόσβασης.
- **Ενότητα Α10. Κρυπτογράφηση**: Οι έλεγχοι σε αυτήν την ενότητα παρέχουν τη βάση για την ορθή χρήση λύσεων κρυπτογράφησης για την προστασία της εμπιστευτικότητας, της αυθεντικότητας ή/και της ακεραιότητας των πληροφοριών.
- **Ενότητα Α11. Φυσική και περιβαλλοντική ασφάλεια**: Οι έλεγχοι σε αυτή την ενότητα εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές περιοχές και προστατεύουν τον εξοπλισμό και τις εγκαταστάσεις από το να τεθούν σε κίνδυνο από την ανθρώπινη ή φυσική παρέμβαση.
- **Ενότητα Α12. Ασφάλεια λειτουργιών**: Τα στοιχεία ελέγχου σε αυτήν την ενότητα διασφαλίζουν ότι τα πληροφοριακά συστήματα, συμπεριλαμβανομένων των λειτουργικών συστημάτων και του λογισμικού, είναι ασφαλή και προστατευμένα από την απώλεια δεδομένων. Επιπλέον, τα στοιχεία ελέγχου σε αυτήν την ενότητα απαιτούν τα μέσα για την καταγραφή συμβάντων και τη δημιουργία αποδεικτικών στοιχείων, την περιοδική επαλήθευση των τρωτών σημείων και τη διενέργεια προληπτικών μέτρων για την αποτροπή της επίδρασης των δραστηριοτήτων ελέγχου σε λειτουργίες.
- **Ενότητα Α13. Ασφάλεια επικοινωνιών**: Οι έλεγχοι σε αυτήν την ενότητα προστατεύουν την υποδομή και τις υπηρεσίες δικτύου, καθώς και τις πληροφορίες που διέρχονται από αυτές.
- **Ενότητα Α14. Απόκτηση, ανάπτυξη και συντήρηση συστημάτων**: Οι έλεγχοι σε αυτήν την ενότητα εξασφαλίζουν ότι η ασφάλεια των πληροφοριών λαμβάνεται υπόψη κατά την αγορά νέων πληροφοριακών συστημάτων ή την αναβάθμιση των υφιστάμενων.
- **Ενότητα Α15. Σχέσεις προμηθευτών**: Οι έλεγχοι σε αυτήν την ενότητα διασφαλίζουν ότι οι δραστηριότητες που ανατίθενται σε εξωτερικούς συνεργάτες που εκτελούνται από προμηθευτές και συνεργάτες χρησιμοποιούν επίσης κατάλληλους ελέγχους ασφάλειας πληροφοριών και περιγράφουν τον τρόπο παρακολούθησης των επιδόσεων ασφαλείας τρίτων.
- **Ενότητα Α16. Διαχείριση συμβάντων ασφάλειας πληροφοριών**: Οι έλεγχοι σε αυτό το τμήμα παρέχουν ένα πλαίσιο για τη διασφάλιση της ορθής επικοινωνίας και χειρισμού συμβάντων και συμβάντων ασφαλείας, ώστε να μπορούν να επιλύονται εγκαίρως· καθορίζουν επίσης τον τρόπο διατήρησης των αποδεικτικών στοιχείων, καθώς και τον τρόπο μάθησης από τα περιστατικά για την πρόληψη της επανάληψής τους.
- **Ενότητα Α17. Πτυχές ασφάλειας πληροφοριών της διαχείρισης της επιχειρησιακής συνέχειας**: Οι έλεγχοι σε αυτή την ενότητα εξασφαλίζουν τη συνέχεια της διαχείρισης της ασφάλειας των πληροφοριών κατά τη διάρκεια κυβερνοεπίθεσης και τη διαθεσιμότητα συστημάτων πληροφοριών.
- **Ενότητα Α18. Συμμόρφωση**: Οι έλεγχοι σε αυτή την ενότητα παρέχουν ένα πλαίσιο για την πρόληψη νομικών, κανονιστικών και συμβατικών παραβάσεων και τον έλεγχο κατά

πόσον η ασφάλεια των πληροφοριών εφαρμόζεται και είναι αποτελεσματική σύμφωνα με τις καθορισμένες πολιτικές, διαδικασίες και απαιτήσεις του προτύπου ISO 27001.

Μια πιο προσεκτική ματιά σε αυτές τις ενότητες μας δείχνει ότι η διαχείριση της ασφάλειας των πληροφοριών δεν είναι μόνο για την ασφάλεια των πληροφοριών (δηλαδή, firewalls, anti-virus, κ.λπ.), αλλά και για τη διαχείριση των διαδικασιών, νομική προστασία, τη διαχείριση των ανθρώπινων πόρων, τη φυσική προστασία, κλπ.

6 ΑΠΑΙΤΗΣΕΙΣ ΒΙΟΜΗΧΑΝΙΑΣ (INDUSTRY REQUIREMENTS)

Με τον όρο Industry Requirements εννοούμε τις απαιτήσεις των παραγόντων της ναυτιλίας όπως είναι το OCIMF, ο BIMCO, ο ICS, ο ISF καθώς και τους νηογνώμονες και άλλους οργανισμούς. Στα πλαίσια της μελέτης αυτής θα ασχοληθούμε με τα προγράμματα TMSA και VIQ που έχουν δημιουργηθεί από το OCIMF καθώς και με τις απαιτήσεις νηογνωμόνων εστιάζοντας στον DNV-GL. Το OCIMF είναι ένα διεθνές ναυτιλιακό φόρουμ των εταιρειών πετρελαίου και αποτελεί την κύρια αρχή για την εξασφάλιση της ασφαλούς και περιβαλλοντικά υπεύθυνης λειτουργίας των πετρελαιοφόρων, τερματικών σταθμών και υπεράκτιων σκαφών υποστήριξης, προωθώντας τη συνεχή βελτίωση των προτύπων σχεδιασμού και λειτουργίας. Συνίσταται από 112 πετρελαϊκές εταιρείες μέσα στις οποίες περιέχονται αυτές που είναι διεθνώς γνωστές αλλά και άλλες που λειτουργούν σε εθνικό επίπεδο.

Το φόρουμ αυτό αναβαθμίζει το ρόλο των μεγάλων πετρελαϊκών εταιρειών καθώς και τη συνεργασία και εναρμόνιση τους με τις διάφορες κυβερνήσεις αλλά και

τον IMO. Το OCIMF λειτουργεί ως στήριγμα των κανονισμών και νομοθετημάτων του IMO που αποσκοπούν στην ασφαλέστερη και αποτελεσματικότερη λειτουργία αλλά και κατασκευή των δεξαμενόπλοιων.

Επίσης, το διεθνές αυτό φόρουμ, εξασφαλίζει στα μέλη του τα εργαλεία και τα μέσα εκείνα που θα συνδράμουν στις υλοποιήσεις προγραμμάτων και ερευνών που μπορεί να σχετίζονται με διάφορα θέματα των δεξαμενοπλοίων. Σκοπός αυτών των παροχών είναι η δημιουργία κατευθύνσεων που θα καλυτερεύσουν τη ναυτιλία σε γενικότερο πλαίσιο. Προκειμένου τα συμβαλλόμενα μέρη να διασφαλίζουν ότι οι πλοιοκτήτες ακολουθούν πιστά τις κατευθύνσεις που δίνονται, δημιουργήθηκε το πρόγραμμα SIRE (Ship Inspection Report Program) με βάση το οποίο γίνεται επιθεώρηση και αναφορά των πλοίων και, γενικά, επιδιώκεται η βελτίωση των πλοίων παγκοσμίως.

6.1 Vessel Inspection Questionnaires (VIQ'S)

Με απώτερο στόχο η τελική αξιολόγηση του δεξαμενόπλοιου να είναι όσο το δυνατό γενικά παραδεκτή και όχι υποκειμενική, ο OCIMF εισήγαγε τα ερωτηματολόγια επιθεώρησης πλοίου που ονομάζονται VIQ (Vessel Inspection Questionnaires). Από τα ερωτηματολόγια αυτά εξάγεται μία «βαθμολογία» για την κατάσταση του πλοίου. Η βαθμολόγηση αυτή γίνεται για να αποτυπωθούν υποδείγματα των δεξαμενοπλοίων με βάση τα οποία είναι σε θέση να πλέουν και να επιχειρούν στο διεθνές εμπόριο. Το VIQ αποτελείται από δώδεκα (12) κεφάλαια. Στο έβδομο με τίτλο "Maritime Security" και στις 7.14, 7.15, 7.16 και 7.17 παραγράφους του βλέπουμε αναφορές για την κυβερνοασφάλεια τις οποίες θα παραθέσουμε παρακάτω.

Παράγραφος 7.14. Υπάρχουν επί του πλοίου πολιτικές και διαδικασίες για την κυβερνοασφάλεια που είναι μέρος του Safety Management System (SMS), καθώς και Σχέδιο Αντίδρασης Κυβερνοχώρου (Cyber Response Plan);

Σημείωση: οι διαδικασίες ενέχουν αξιολόγηση κινδύνου για θέματα όπως:

- Απειλές όπως από κακόβουλο λογισμικό όπως επιθέσεις ηλεκτρονικού "ψαρέματος" (Phishing) και άλλες.
- Ταυτοποίηση και προστασία των ευάλωτων συστημάτων (ECDIS κλπ.)
- Μέτρα μείωσης (έλεγχος USB κλπ.).

- Καθορισμός του κατάλληλου προσωπικού της επιχείρησης (περιλαμβανομένου και εκείνου του μέλους πληρώματος στο οποίο ο πλοίαρχος αναφέρει ύποπτα περιστατικά).
- Διατήρηση έντυπων αντιγράφων για ελεγκτικούς οργανισμούς (όπως ο DPA, ο CSO κλπ.).
- Διαχείριση/Εγγραφή των κωδικών πρόσβασης.
- Συμμόρφωση με τον ανάδοχο.

Σημείωση: Το Σχέδιο Αντίδρασης Κυβερνοχώρου (Cyber Response Plan) ενέχει κατευθύνσεις όπως:

- Τι «συμπτώματα» να αναζητηθούν.
- Άμεσες δράσεις που πρέπει να αναληφθούν και
- Όνομα, θέση, αριθμός τηλεφώνου και email για το υπεύθυνο πρόσωπο προς επικοινωνία.

Παράγραφος 7.15. Γνωρίζει το πλήρωμα την πολιτική της εταιρείας όσον αφορά τον έλεγχο της φυσικής πρόσβασης σε όλα τα τεχνολογικά συστήματα του πλοίου Λειτουργικά ή Πληροφοριακά;

Σημείωση: Οι επιθεωρητές θα πρέπει να παρατηρούν εάν ελέγχεται η πρόσβαση σε θύρες USB στα τερματικά των Λειτουργικών/Πληροφοριακών Τεχνολογικών Συστημάτων επί του πλοίου» (παράδειγμα: υπάρχουν μέτρα για τον αποκλεισμό/κλείδωμα θυρών USB/RJ-45 σε αυτούς τους τερματικούς σταθμούς. Οι διαδικασίες θα πρέπει να περιλαμβάνουν την προστασία του κρίσιμου εξοπλισμού, ειδικότερα δε λογισμικό που έχει να κάνει με την ασφάλεια ναυσιπλοΐας, από επιθέσεις κακόβουλου λογισμικού και ιών. Οι διαδικασίες θα πρέπει να περιλαμβάνουν τον έλεγχο της πρόσβασης σε όλους τους τερματικούς σταθμούς των Λειτουργικών/Πληροφοριακών Τεχνολογικών Συστημάτων επί του πλοίου. Οι διαδικασίες θα πρέπει επίσης να περιλαμβάνουν τον έλεγχο στην πρόσβαση τρίτων όπως τεχνικών και εξωτερικών συνεργατών.

Παράγραφος 7.16. Η εταιρεία έχει πολιτική ή καθοδήγηση σχετικά με τη χρήση προσωπικών συσκευών επί του πλοίου;

Οι προσωπικές συσκευές περιλαμβάνουν τηλέφωνο /tablet κ.λπ.

Ελέγξτε αν η πολιτική εφαρμόζεται τόσο από το πλήρωμα όσο και από τους επισκέπτες, π.χ. από όλους τους εξωτερικούς συνεργάτες και τεχνικούς.

Παράγραφος 7.17. Η μέριμνα για την Κυβερνοασφάλεια προωθείται ενεργά από την εταιρεία στο πλοίο;

Σημείωση: Παραδείγματα ενεργής προώθησης περιλαμβάνουν:

- Υλικό ευαισθητοποίησης στον κυβερνοχώρο που εμφανίζεται από όλους τους τερματικούς σταθμούς πληροφορικής και τους χώρους ανάπαυσης του πληρώματος.
- Ταινίες εκπαίδευσης που προβάλλονται στο πλήρωμα.
- Ειδική εκπαίδευση πληρώματος.
- Οδηγίες για την προστασία των κωδικών πρόσβασης.
- Υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης.
- Πολιτική σχετικά με τη χρήση προσωπικών συσκευών και τη συμπερίληψή τους στους καταλόγους ελέγχου εξοικείωσης που συμμετέχουν στο πλοίο.
- Εταιρεία πιστοποιημένη σύμφωνα με το πρότυπο ISO 27001.

6.2 Tanker Management and Self-Assessment (TMSA 3)

Όσον αφορά την κυβερνοασφάλεια στα δεξαμενόπλοια, από την 1η Ιανουαρίου του 2018, υπάρχει η υποχρεωτική εφαρμογή του 13ου στοιχείου του TMSA 3. Το πρόγραμμα TMSA αναπτύχθηκε επίσης από τον OCIMF. Στόχος του προγράμματος αυτού είναι η διασφάλιση της ασφάλειας και της πρόληψης για την περιβαλλοντική μόλυνση από τα δεξαμενόπλοια. Παρέχεται ένα εργαλείο αξιολόγησης του Safety Management System (SMS) μέσα από κάποιους δείκτες απόδοσης (Key Performance Indicators - KPIs). Το TMSA 3 είναι ένα σύστημα αξιολόγησης δεξαμενοπλοίων με απώτερο σκοπό την δημιουργία ενός ασφαλούς περιβάλλοντος εργασίας. Υπεύθυνος για αυτό, είναι η εκάστοτε ναυτιλιακή εταιρία η οποία για την εξασφάλιση των ανωτέρω, πρέπει όχι μόνο να μειώσει τους ενδεχόμενους κινδύνους από το διαδίκτυο αλλά και τις επιπτώσεις τις οποίες μπορεί να προκαλέσουν οι κίνδυνοι αυτοί, αν περάσουν από τα συστήματα προστασίας. Για την εξυπηρέτηση του σκοπού αυτού, η ναυτιλιακή εταιρία πρέπει να είναι σε θέση να αναγνωρίζει την οποιαδήποτε απειλή και να λαμβάνει τα κατάλληλα μέτρα, την κατάλληλη στιγμή για να μετριάσει τους κινδύνους τους οποίους μπορεί να προκαλέσει μια στοχευμένη κυβερνοεπίθεση. Στόχος της εκάστοτε ναυτιλιακής εταιρίας είναι η καθιέρωση των

διαδικασιών, έτσι ώστε να μειωθούν οι συνέπειες που μπορεί να προκληθούν από μια ενδεχόμενη κυβερνοεπίθεση και όχι μόνο.

Παρακάτω παραθέτουμε τον πίνακα 6.1 ο οποίος απεικονίζει τα KPI's (Βασικοί Δείκτες Απόδοσης) καθώς και κατευθυντήριες γραμμές για το τι πρέπει να ακολουθεί μια εταιρία έτσι ώστε να συμβαδίζει με την βέλτιστη προτεινόμενη πρακτική.

Πίνακας 6.1 KPI's και κατευθυντήριες γραμμές. Πηγή: TMSA 3

Ele/nt	Item	Stage	Element title	KPI	Best Practice
13	1.1	1	Maritime Security	Υπάρχουν τεκμηριωμένα σχέδια ασφαλείας.	Τα σχέδια καλύπτουν όλες τις πτυχές των δραστηριοτήτων, συμπεριλαμβανομένων • Τοποθεσίες με βάση την ξηρά. • Σκάφη. • Προσωπικό. Προσδιορίζεται το προσωπικό που είναι υπεύθυνο για θέματα ασφαλείας.

13	1.2	1	Maritime Security	Η εταιρεία έχει τεκμηριωμένες διαδικασίες για τον εντοπισμό απειλών για την ασφάλεια που ισχύουν για τις εμπορικές περιοχές των πλοίων και τις τοποθεσίες ξηράς.	Οι απειλές για την ασφάλεια μπορεί να περιλαμβάνουν: • Μικροκλοπές • Βανδαλισμούς • Λαθρεπιβάτες. • Κλοπή φορτίου. • Απειλή στον κυβερνοχώρο. • Ανεπαρκής ασφάλεια λιμένα. • Διακίνηση ανθρώπων, όπλων ή ναρκωτικών. • Λαθρεμπόριο. • Πειρατεία. • Σαμποτάζ και εμπρησμός. • Η τρομοκρατία και τα επακόλουθά της αποτελέσματα. Οι εντοπισμένες απειλές εξετάζονται όπως απαιτείται από τις αλλαγές στις περιστάσεις.
13	1.3	1	Maritime Security	Έχουν αναπτυχθεί μέτρα για τον μετριασμό και την αντιμετώπιση όλων των εντοπισμένων απειλών για τα πλοία και τις τοποθεσίες ξηράς.	Τα μέτρα άμβλυνσης μπορούν να περιλαμβάνουν: • Έλεγχος πρόσβασης. • Μέτρα φυσικής ασφάλειας. • Ασκήσεις και εκπαίδευση. • Περιπολίες ασφαλείας. • Αναζητήσεις. Υπάρχουν σχέδια έκτακτης ανάγκης για την αντιμετώπιση ενδεχόμενων παραβιάσεων της ασφάλειας.
13	1.4	1	Maritime Security	Υπάρχουν διαδικασίες για την απόκτηση, τη διαχείριση και την αναθεώρηση των τρεχουσών πληροφοριών που σχετίζονται με την ασφάλεια.	Οι πληροφορίες ασφαλείας λαμβάνονται από την εταιρεία από κατάλληλες πηγές που μπορεί να περιλαμβάνουν: • Διεθνείς και εθνικούς οργανισμούς. • Περιφερειακά κέντρα αναφοράς για την ασφάλεια στη θάλασσα. • Κράτος σημαίας. • Φορείς της βιομηχανίας. • Τοπικούς πράκτορες. • Στρατιωτικές πηγές. • Ειδικούς σύμβουλους. Το αρμόδιο πρόσωπο εξετάζει τις πληροφορίες και εκδίδει σχετικές οδηγίες για τις τοποθεσίες, το

					προσωπικό και τα σκάφη ξηράς, ανάλογα με την περίπτωση.
13	1.5	1	Maritime Security	Οι διαδικασίες περιλαμβάνουν την αναφορά πιθανών απειλών για την ασφάλεια και πραγματικών συμβάντων ασφαλείας.	Οι διαδικασίες υποβολής εκθέσεων μπορούν να περιλαμβάνουν: • Εσωτερικές αναφορές μεταξύ πλοίων. • Από το πλοίο στην εταιρεία. • Από το πλοίο σε εξωτερικές αρχές. • Από την εταιρεία προς εξωτερικές αρχές.
13	2.1	2	Maritime Security	Πραγματοποιούνται επίσημες αξιολογήσεις κινδύνου των δραστηριοτήτων της εταιρείας για τον εντοπισμό και τον μετριασμό πιθανών απειλών για την ασφάλεια.	Οι αξιολογήσεις κινδύνου επανεξετάζονται, ενημερώνονται και οι διαδικασίες της εταιρείας τροποποιούνται ανάλογα με τις ανάγκες. Οι αξιολογήσεις κινδύνου ασφάλειας πλοίου επανεξετάζονται πριν από την είσοδο σε περιοχές που έχουν διαπιστωθεί ότι έχουν αυξημένο κίνδυνο. Όταν από την εκτίμηση κινδύνου κριθεί αναγκαίο, αναπτύσσονται, τεκμηριώνονται και εφαρμόζονται ειδικά μέτρα για την ενίσχυση της άμυνας των πλοίων.

13	2.2	2	Maritime Security	Το προσωπικό που είναι υπεύθυνο για την ασφάλεια λαμβάνει εκπαίδευση κατάλληλη για το ρόλο του 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 εναλλακτικού σχεδίου για βασικούς ρόλους ασφαλείας. Παρέχεται ενημέρωση ασφαλείας σε όλο το προσωπικό στο πλαίσιο της διαδικασίας εξ οικειοποίησής του.
13	2.3	2	Maritime Security	Η πολιτική και οι διαδικασίες περιλαμβάνουν την ασφάλεια στον κυβερνοχώρο και παρέχουν κατάλληλα μέτρα καθοδήγησης και μετριασμού.	Οι κίνδυνοι για τα συστήματα Πληροφορικής μπορεί να περιλαμβάνουν: • Εσκεμμένες και μη εξουσιοδοτημένες παραβιάσεις. • Ακούσιες παραβιάσεις. • Ανεπαρκής ακεραιότητα του συστήματος, όπως τείχη προστασίας. Εντοπίζονται συστήματα με άμεσες ή έμμεσες συνδέσεις επικοινωνίας, τα οποία ενδέχεται να είναι ευάλωτα σε απειλές. Αυτά μπορεί να περιλαμβάνουν συστήματα πλοήγησης, ελέγχου και επικοινωνίας. Κατά την ανάπτυξη διαδικασιών, η εταιρεία μπορεί να αναφέρεται σε σχετικές τρέχουσες οδηγίες του κλάδου.
13	2.4	2	Maritime Security	Η εταιρεία προωθεί ενεργά την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο.	Χρησιμοποιούνται αποτελεσματικά μέσα για την ενθάρρυνση της υπεύθυνης συμπεριφοράς του προσωπικού ξηράς, του προσωπικού του πλοίου και τρίτων. Η συμπεριφορά αυτή μπορεί να περιλαμβάνει: • Κλείδωμα των σταθμών εργασίας χωρίς παρακολούθηση. • Προστασία των κωδικών πρόσβασης. • Καμία χρήση μη

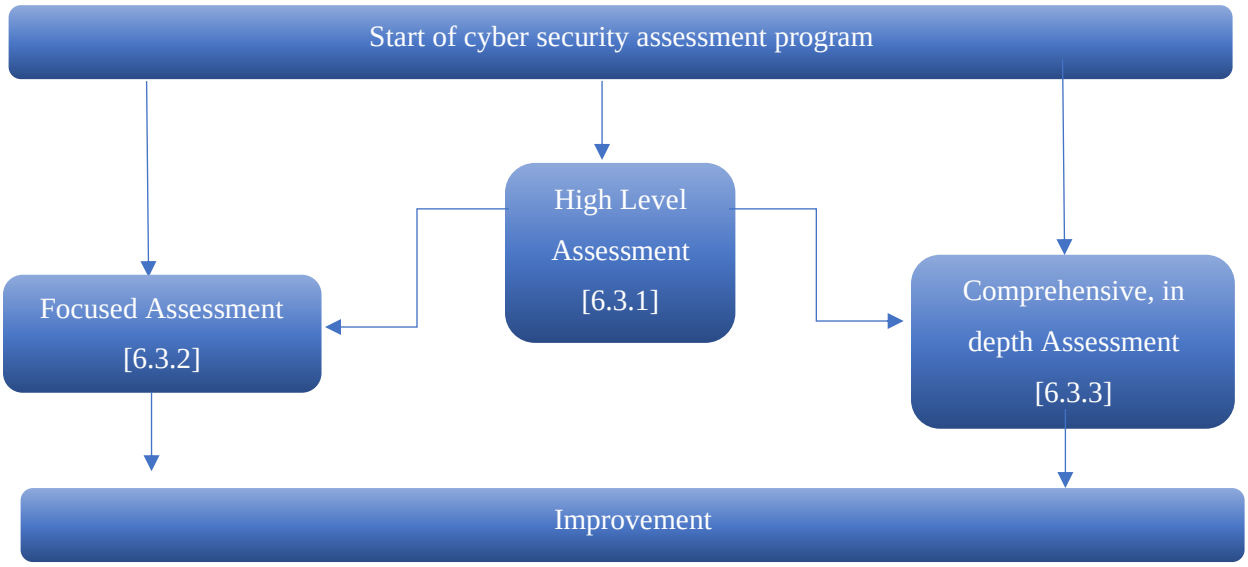
					εξουσιοδοτημένου λογισμικού. • Υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης. • Έλεγχος/πρόληψη κακής χρήσης φορητών ραβδιών αποθήκευσης και μνήμης.
13	3.1	3	Maritime Security	Υπάρχει πολιτική ταξιδιού για την ελαχιστοποίηση των απειλών για την ασφάλεια του προσωπικού.	Η πολιτική βασίζεται στην εκτίμηση κινδύνου και περιλαμβάνει το προσωπικό του πλοίου, το προσωπικό ξηράς και τους εργολάβους που ταξιδεύουν για τις επιχειρήσεις της εταιρείας. Κατά περίπτωση, υπάρχουν περιορισμοί και οδηγίες για τα ταξίδια που χαρακτηρίζονται ως αυξημένου κινδύνου. Η ταξιδιωτική πολιτική επανεξετάζεται τακτικά για να ληφθούν υπόψη οι αλλαγές στις απειλές για την ασφάλεια.
13	3.2	3	Maritime Security	Οι διαδικασίες ασφαλείας επικαιροποιούνται λαμβάνοντας υπόψη τις τρέχουσες οδηγίες.	Οι οδηγίες του κλάδου μπορεί να περιλαμβάνουν: • Θαλάσσια ασφάλεια – Καθοδήγηση σχετικά με τον κώδικα ISPS (ICS). • Διαγράμματα σχεδιασμού ασφαλείας. • Κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο από τη βιομηχανία και την κλάση. • Επιχειρήσεις διάσωσης μεγάλης κλίμακας στη θάλασσα (ICS). • Περιφερειακός οδηγός για την καταπολέμηση της πειρατείας και των ένοπλων ληστειών κατά πλοίων στην Ασία (ReCAAP-ISC). Τα πλοία της εταιρείας εφοδιάζονται με τις τελευταίες εκδόσεις σχετικών εκδόσεων που σχετίζονται με την ασφάλεια.
				Η πολιτική ασφάλειας και οι	

13	3.3	3	Maritime Security	σχετικές διαδικασίες περιλαμβάνονται στο πρόγραμμα εσωτερικού ελέγχου.	Ο έλεγχος αξιολογεί τη συμμόρφωση με όλες τις πτυχές των διαδικασιών ασφάλειας της εταιρείας, συμπεριλαμβανομένης της προσωπικής ευαισθητοποίησης και συμπεριφοράς.
13	4.1	4	Maritime Security	Πραγματοποιούνται αξιολογήσεις των μέτρων ασφαλείας και ετοιμότητας της εταιρείας.	Οι αξιολογήσεις μπορούν να διενεργούνται από το προσωπικό ή από εξωτερικούς επιθεωρητές .
13	4.2	4	Maritime Security	Η ανεξάρτητη εξειδικευμένη υποστήριξη χρησιμοποιείται για τον μετριασμό των εντοπισμένων απειλών για την ασφάλεια.	Οποιεσδήποτε συμβάσεις για εξειδικευμένη υποστήριξη τόσο επί του πλοίου όσο και στην ξηρά, υποστηρίζονται από ένα ολοκληρωμένο πεδίο εργασίας. Η στήριξη αυτή μπορεί να ανατεθεί μέσω δραστηριοτήτων που περιλαμβάνουν την κατάρτιση, την ασφάλεια και τις αξιολογήσεις απειλών και τα καθήκοντα φύλαξης. Πριν από τη σύναψη σύμβασης, η εταιρεία προβαίνει σε διεξοδική αξιολόγηση της δέουσας επιμέλειας του προτεινόμενου αναδόχου, συμπεριλαμβανομένης της συμμόρφωσης με τα σχετικά πρότυπα. Οδηγίες σχετικά με τη διεξαγωγή των συμβούλων ασφαλείας επί του πλοίου και το πεδίο εργασίας τους, παρέχονται στον Πλοίαρχο.

13	4.3	4	Maritime Security	Τα πλοία διαθέτουν ενισχυμένο εξοπλισμό ασφάλειας και παρακολούθησης.	Παραδείγματα τέτοιου εξοπλισμού περιλαμβάνουν: • Κανόνια νερού. • Εξοπλισμός θερμικής απεικόνισης. • Ραντάρ. • Ταινία έκρηξης για παράθυρα. • Συστήματα εισόδου πληκτρολογίου. • Συστήματα παρακολούθησης και καταγραφής cctv. • Ένα δευτερεύον μέσο ανεξάρτητης δορυφορικής τηλεφωνικής επικοινωνίας.
13	4.4	4	Maritime Security	Οι βελτιώσεις ασφαλείας συμπεριλαμβάνονται στις προδιαγραφές ανακατασκευής και στο σχεδιασμό νέας κατασκευής.	Οι βελτιώσεις και οι προδιαγραφές μπορεί να εξαρτώνται από: • Περιοχή συναλλαγών. • Τύπο και μέγεθος πλοίου. • Επίπεδα επάνδρωσης.
13	4.5	4	Maritime Security	Η εταιρεία συμμετέχει στη δοκιμή και εφαρμογή καινοτόμων τεχνολογιών και συστημάτων ασφαλείας.	Αυτό μπορεί να περιλαμβάνει: • Φυσικά μέτρα για τη βελτίωση της ασφάλειας. • Βελτιώσεις λογισμικού σε συστήματα πληροφορικής.

6.3 Συνιστάμενη Πρακτική DNV-GL (Recommended Practice DNV-GL)

Η αξιολόγηση της συσχέτισης μεταξύ των περιουσιακών στοιχείων μιας εταιρείας, των τρωτών σημείων τους και των απειλών στις οποίες εκτίθενται, αποτελεί τη βάση για οποιαδήποτε επιδιωκόμενη βελτίωση της ασφάλειας στον κυβερνοχώρο. Μια ανάλυση χάσματος (gap analysis) μεταξύ των επιπέδων ασφάλειας και των υπαρχόντων αντιμέτρων πρέπει να δείξει τον δρόμο προς την βελτίωση των λογισμικών που παρέχουν προστασία από μια κυβερνοεπίθεση. Αυτή η συνιστάμενη πρακτική (Rrecommended Practice -RP) συνιστά τρεις διαφορετικές προσεγγίσεις. Οι αξιολογήσεις αυτές μπορούν να χρησιμοποιηθούν διαδοχικά ή αυτόνομα ανάλογα και όπως ταιριάζουν στις προτεραιότητες και τα σύνολα δεξιοτήτων του οργανισμού, όπως απεικονίζεται στο σχήμα 6.1.



Σχήμα 6.1 Ακολουθία αξιολόγησης. Πηγή: DNVGL-RP-0496

6.3.1 Αξιολόγηση Υψηλού Επιπέδου (High Level Assessment)

Μια αξιολόγηση υψηλού επιπέδου συνιστάται ως ένα πρώτο βήμα στο πρόγραμμα βελτίωσης της ασφάλειας στον κυβερνοχώρο μιας εταιρείας, όταν τα ανώτερα διοικητικά στελέχη χρειάζονται γρήγορα μια επισκόπηση της εικόνας κινδύνου για την ασφάλεια στον κυβερνοχώρο και θέλει να αποκτήσει μια δομημένη ένδειξη για το πού απαιτούνται πιο εστιασμένες αξιολογήσεις. Η

προσέγγιση αυτή θα πρέπει να βασίζεται στην καλύτερη κρίση, μειώνοντας την απαιτούμενη προσπάθεια. `

Η συνιστάμενη πρακτική προτείνει:

1. Τον προσδιορισμό των βασικών συστημάτων της εταιρείας. Τα συστήματα επί του πλοίου και τα σύνολα των δεδομένων συνήθως καταγράφονται με βάση τις βασικές λειτουργίες των πλοίων, ενώ τα χερσαία συστήματα και τα σύνολα δεδομένων θα καταγράφονται με τη σειρά τους μέσω της ανάλυσης βασικών επιχειρηματικών διαδικασιών.
2. Την αξιολόγηση της επίπτωσης (υψηλή, μεσαία, χαμηλή) μιας επιτυχημένης επίθεσης σχετικά με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα για αυτά τα συστήματα και σύνολα δεδομένων.
3. Την αξιολόγηση της πιθανότητας (υψηλής, μέσης, χαμηλής) επιτυχούς επίθεσης στα συστήματα των πλοίων και στις βασικές επιχειρηματικές διαδικασίες, κρίνοντας την πιθανή αποτελεσματικότητα των εν προκειμένω αντιμέτρων, συμπεριλαμβανομένων των τεχνικών αντιμέτρων, της οργανωτικής ευαισθητοποίησης, των συστημάτων διαχείρισης και των διαδικασιών.
4. Την αποτύπωση των αποτελεσμάτων των βημάτων 2 και 3 σε ένα πίνακα ανάλυσης ρίσκου (Risk Matrix)

Στη συνέχεια, η συνιστάμενη πρακτική συνιστά τη διεξαγωγή μιας πιο εστιασμένης αξιολόγησης [9.4] για τα συστήματα και τα σύνολα δεδομένων που χρησιμοποιούνται στους τομείς ενδιαφέροντος (επιχειρηματικές διαδικασίες ή λειτουργίες των πλοίων) που τοποθετούνται στο μη αποδεκτό μέρος του πίνακα κινδύνου. Μπορεί επίσης να διεξαχθεί διεξοδική, εις βάθος αξιολόγηση προκειμένου να αντιμετωπιστεί ένα ευρύτερο σύνολο συστημάτων με λεπτομερέστερες απαιτήσεις (μετριασμού μιας πιο ουσιαστικής εικόνας κινδύνου), (DNVGL-RP-0496 RECOMMENDED PRACTICE).

6.3.2 Στοχευμένη Αξιολόγηση (Focused Assessment)

Η συνιστάμενη πρακτική προτείνει μια συστηματική και εστιασμένη προσέγγιση για την αξιολόγηση της ευρωστίας του τείχους προστασίας έναντι των απειλών, όταν η ανάγκη είναι να επικεντρωθεί σε επιλεγμένα συστήματα.

Η συνιστάμενη πρακτική προτείνει:

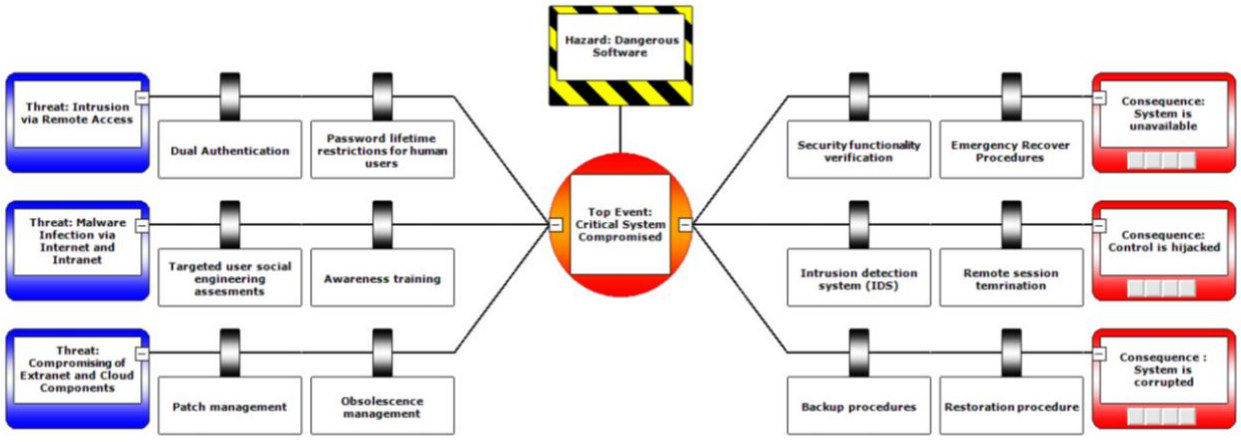
1. Προσδιορισμό των απειλών για συστήματα που υποστηρίζουν συγκεκριμένες λειτουργίες των πλοίων και επιχειρηματικές διαδικασίες.
2. Προσδιορισμό του τείχους προστασίας που αποτρέπει συμβάντα που σχετίζονται με αυτές τις απειλές.
3. Προσδιορισμό του τείχους προστασίας που μειώνει τις συνέπειες σε περίπτωση εμφάνισης αυτών των συμβάντων.

4. Αξιολόγηση της μείωσης των συνεπειών.

Στην ασφάλεια στον κυβερνοχώρο, ένα τείχος προστασίας (ή αντίμετρο) είναι μια ενέργεια, συσκευή, διαδικασία ή τεχνική που μειώνει μια απειλή, ευπάθεια ή επίθεση:

- Εξαφανίζοντάς την.
- Αποτρέποντάς την.
- Ελαττώνοντας την ζημιά που μπορεί να προκαλέσει.
- Εντοπίζοντάς την και αναφέροντάς την έτσι ώστε να παρθούν μέτρα για την εξάλειψή της.

Η εστιασμένη προσέγγιση αξιολόγησης που προτείνεται σε αυτό το τμήμα βασίζεται στη μέθοδο Bow-Tie. Η προσέγγιση αξιολογεί τους κινδύνους που σχετίζονται με τις επιθέσεις στον κυβερνοχώρο, καθώς και τους ελέγχους και τα εμπόδια κατά μιας τέτοιας επίθεσης, χωρίς να επικεντρώνεται στην πιθανότητα ή τη συχνότητά της. Αυτό βοηθά στην γρήγορη απεικόνιση εάν πρέπει να εφαρμοστούν περισσότερα μέτρα. Το σχήμα 6.2 απεικονίζει τη μέθοδο Bow-Tie, όπου το αριστερό μέρος του Bow-Tie δείχνει εμπόδια (γκρίζες γραμμές) που βοηθούν στην πρόληψη των απειλών (μπλε κουτιά) να γίνουν ένα κυβερνο-περιστατικό (κεντρικός κόκκινος κύκλος). Στη δεξιά πλευρά του Bow-Tie φαίνονται εμπόδια μετριασμού που βοηθούν στην πρόληψη των ανεπιθύμητων συνεπειών (κόκκινα κουτιά).



Σχήμα 6.2 Παράδειγμα απεικόνισης των στοιχείων bow-tie για την ασφάλεια στον κυβερνοχώρο. Πηγή: DNVGL-RP-0496

Τα διαγράμματα Bow-Tie μπορούν επίσης να χρησιμοποιηθούν για την απλή καταγραφή των παρατηρήσεων και συνιστώνται ως αποτελεσματικό εργαλείο για την επικοινωνία και την αύξηση της ευαισθητοποίησης σχετικά με τις προσπάθειες της CS (Cyber Security).

Για τον καθορισμό των συστημάτων στα οποία θα διεξαχθεί εστιασμένη αξιολόγηση, ο χρήστης της παρούσας συνιστάμενης πρακτικής μπορεί είτε να ξεκινήσει με τα συστήματα και τις διαδικασίες υψηλού κινδύνου που προσδιορίζονται στην αξιολόγηση υψηλού επιπέδου ή με τη συμπλήρωση ερωτηματολογίου από τους χρήστες των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων. Για τα συστήματα στα πλοία συνίσταται να εντοπιστούν συστήματα υψηλού κινδύνου, κάνοντας στους χρήστες βασικές ερωτήσεις, όπως αναφέρονται στον πίνακα 6.2.

Πίνακας 6.2 Ερωτήσεις αξιολόγησης με επίκεντρο το υπό μελέτη σύστημα. Πηγή: DNVGL-RP-0496.

Τυπικές ερωτήσεις που βοηθούν στον προσδιορισμό συστημάτων για τον επιτόπιο έλεγχο
Είναι το λειτουργικό σύστημα ενημερωμένο;
Πώς αντιμετωπίζονται οι ενημερώσεις λογισμικού; Υπάρχουν κατάλληλες διαδικασίες;
Τι γίνεται με τις ενημερωμένες εκδόσεις κώδικα ασφαλείας λογισμικού, πώς αντιμετωπίζονται αυτά; Υπάρχει πολιτική διαχείρισης ενημερωμένων εκδόσεων κώδικα;
Είναι ενημερωμένες οι βάσεις δεδομένων των λογισμικών προστασίας από ιούς; — Υπάρχει διαδικασία για την επικαιροποίηση των συστημάτων ΟΤ; — Υπάρχει διαδικασία αντίδρασης των συστημάτων ΟΤ σε γνωστά τρωτά σημεία;
Χρησιμοποιούνται και αλλάζουν οι κωδικοί πρόσβασης στα αναμενόμενα χρονικά διαστήματα;
Αλλάζουν οι προεπιλεγμένοι κωδικοί πρόσβασης;
Υπάρχουν μέσα για τον εντοπισμό συμβάντων και εισβολών στον τομέα της κυβερνοασφάλειας;
Υπάρχουν διαθέσιμα αρχεία καταγραφής ασφαλείας (π.χ. ανίχνευση ιών και κακόβουλου λογισμικού); Χρησιμοποιούνται; Αναφέρονται;
Υπάρχει κάποιο σχέδιο αντιμετώπισης παραβίασης ασφαλείας; Αν ναι, γνωστοποιούνται διαδικασίες που προβλέπονται;
Είναι περιορισμένα τα δικαιώματα διαχειριστή;
Εφαρμόζεται η προστασία του ηλεκτρονικού ταχυδρομείου και του προγράμματος περιήγησης;
Υπάρχουν στοιχεία ελέγχου πρόσβασης για το ασύρματο δίκτυο;
Χρησιμοποιείται κρυπτογράφηση; Που;
Επιτρέπονται προσωπικές συσκευές αποθήκευσης (USB) στο εταιρικό δίκτυο; Σαρώνονται τα USB sticks; Καθαρίζονται;
Πώς απορρίπτονται τα δεδομένα που αποθηκεύονται σε τηλέφωνα/PDA της εταιρείας;
Πού είναι αποθηκευμένα τα αντίγραφα ασφαλείας; Παρακολουθούνται οι συσκευές αποθήκευσης; Ελέγχονται τα αντίγραφα ασφαλείας;

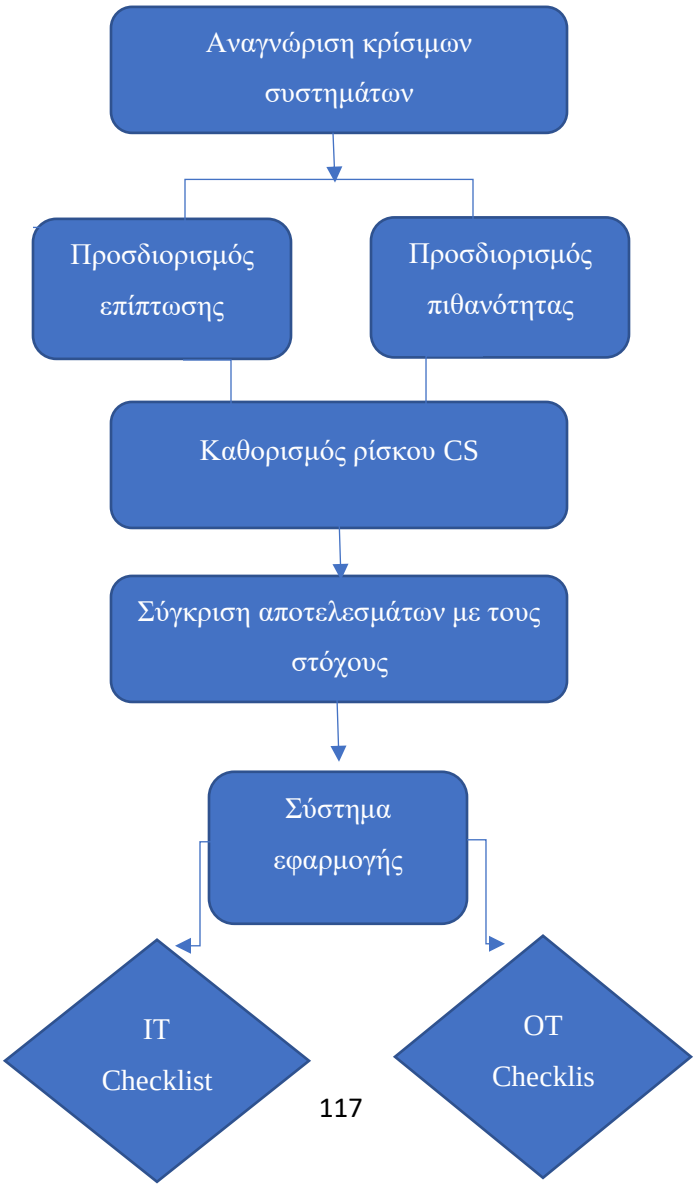
Οι εργαζόμενοι είναι εκπαιδευμένοι στις πολιτικές ασφάλειας στον κυβερνοχώρο;
Ελέγχονται οι ανάδοχοι για επαρκή εξουσιοδότηση ασφαλείας;
Επιτρέπεται η εξωτερική πρόσβαση στους υπεργολάβους; Πώς ελέγχεται;
Η απομακρυσμένη συντήρηση εκτελείται;
Είναι ασφαλείς οι δορυφορικές επικοινωνίες και οι ραδιοεπικοινωνίες;
Εάν το σύστημα φυλάσσεται σε ασφαλές χώρο με κλειδωμένες πόρτες και έλεγχο εισόδου, ισχύει; εφαρμόζεται;
Είναι ασφαλές το σύστημα από κλοπή, φωτιά και τυχαία ζημιά;

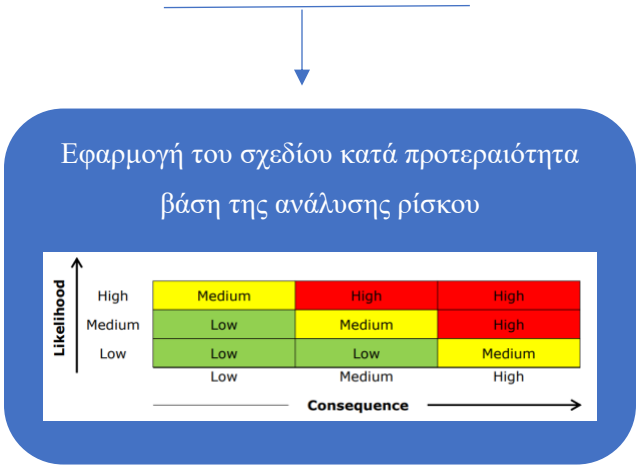
6.3.3 Ολοκληρωμένη Σε Βάθος Αξιολόγηση (Comprehensive, In Depth Assessment)

Μια ολοκληρωμένη, σε βάθος αξιολόγηση χρησιμοποιείται όταν τα ανώτερα διοικητικά στελέχη χρειάζονται λεπτομερέστερη αξιολόγηση κινδύνου, ιδίως όταν οι συνέπειες των συμβάντων CS είναι κρίσιμες και εάν υπάρχουν σημαντικές αλληλεξαρτήσεις του συστήματος. Λόγω του πιο τεχνικού χαρακτήρα της εις βάθους αξιολόγησης, η προσέγγιση αυτή συχνά απαιτεί τη συμμετοχή εξωτερικών ειδικών. Η αξιολόγηση αυτή θα πρέπει να διενεργείται για κρίσιμες επιχειρηματικές διαδικασίες και συνήθως περιλαμβάνει:

1. προσδιορισμός κρίσιμων συστημάτων IT/OT που είναι ευάλωτα σε απειλές CS μέσω της χαρτογράφησης βασικών επιχειρηματικών διαδικασιών και αντίστοιχων λειτουργιών των πλοίων.
2. τον εντοπισμό των συνεπειών μιας επιτυχημένης επίθεσης για καθένα από τα συστήματα
3. τον καθορισμό της ευκολίας πρόσβασης σε καθένα από τα συστήματα ως μέτρο μέτρησης και σύγκρισης για την πιθανότητα επίθεσης.
4. αξιολόγηση των συστημάτων όσον αφορά τον κίνδυνο της CS (που καθορίζεται από την πιθανότητα επίθεσης επί τη συνέπεια της επιτυχούς επίθεσης).
5. σύγκριση των υφιστάμενων διασφαλίσεων με τους στόχους που θέλουν να επιτευχθούν στα επίπεδα προστασίας.

Το διάγραμμα 6.1 παρουσιάζει τα βήματα και τις δραστηριότητες που περιλαμβάνονται στην προτεινόμενη ολοκληρωμένη, σε βάθος προσέγγιση αξιολόγησης.

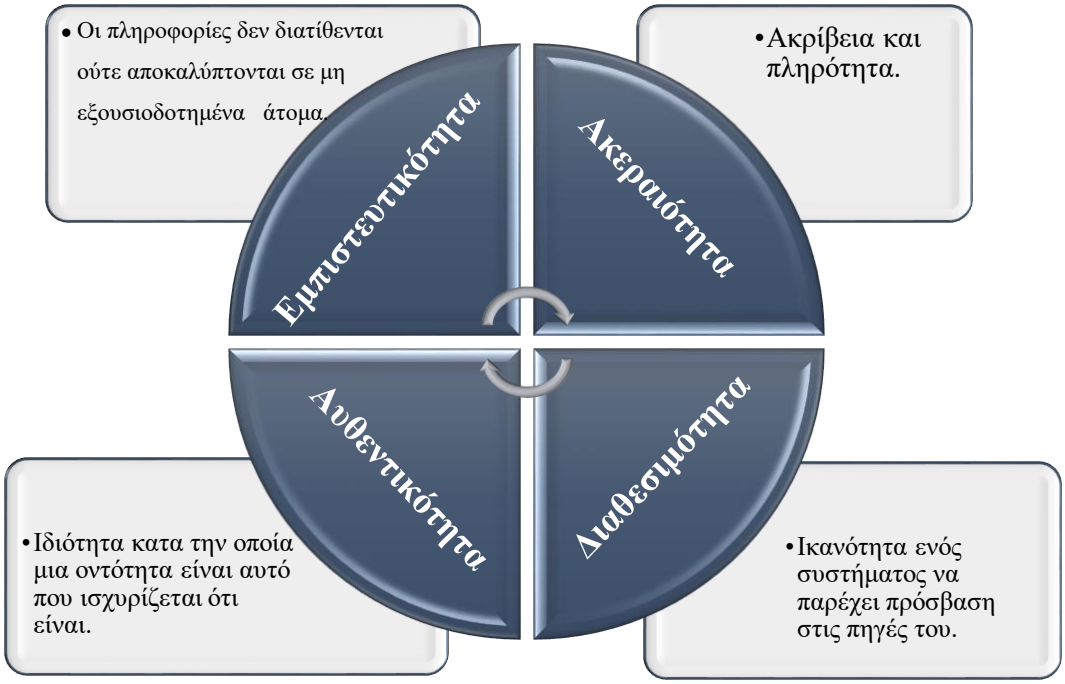

Αναγνώριση κρίσιμων συστημάτων
Προσδιορισμός επίπτωσης
Προσδιορισμός πιθανότητας
Καθορισμός ρίσκου CS
Σύγκριση αποτελεσμάτων με τους στόχους
Σύστημα εφαρμογής
IT Checklist
OT Checklis



Διάγραμμα 6.1 Στάδια ολοκληρωμένης, σε βάθος αξιολόγησης. Πηγή: DNVGL-RP-0496

6.3.4 Αποτίμηση Επιπτώσεων Επιτυχημένης Κυβερνοεπίθεσης

Ως επόμενο βήμα, οι ανάγκες προστασίας για το σύστημα της εταιρείας που θα δεχτεί επίθεση πρέπει να καθοριστούν για να καθοδηγήσουν τις προσπάθειες για την προστασία του συστήματος. Αυτό γίνεται με την αξιολόγηση των συνεπειών μιας επιτυχημένης επίθεσης χρησιμοποιώντας το μοντέλο CIAA (Confidentiality, Integrity, Availability, Authenticity, ref. /39/) που περιγράφεται στο σχήμα 6.3:



Σχήμα 6.3 Μοντέλο CIAA (εφαρμόζεται στην έκδοση 2014 του ISO/IEC 27000). Πηγή: DNVGL-RP-0496

Οι τέσσερις ιδιότητες ασφαλείας μπορεί να έχουν μεγαλύτερη ή χαμηλότερη σημασία. Για παράδειγμα, για ένα σύστημα ηλεκτρονικών γραφημάτων η εμπιστευτικότητα του συστήματος είναι άνευ σημασίας, καθώς τα γραφήματα είναι δημοσιευμένες πληροφορίες προσβάσιμες από όλους, αλλά η διαθεσιμότητα και η ακεραιότητα έχουν μεγάλη σημασία. (DNVGL-RP-0496 RECOMMENDED PRACTICE)

Πίνακας 6.3 Τυπικά ερωτήματα για την αξιολόγηση των συνεπειών

Ιδιότητες ασφαλείας (CIAA)	***Τυπικές ερωτήσεις για αξιολόγηση της CIAA***
Εμπιστευτικότητα	Πόσο σημαντική είναι η εμπιστευτικότητα αυτών των πληροφοριών; Τι θα συνέβαινε αν αυτές οι πληροφορίες αποκαλυφθούν;
Ακεραιότητα	Πόσο σημαντικό είναι για αυτές τις πληροφορίες να είναι ακριβείς και πλήρεις; Τι θα συνέβαινε αν οι πληροφορίες ήταν λανθασμένες ή τροποποιημένες;
Διαθεσιμότητα	Εάν το σύστημα / πληροφορίες δεν είναι διαθέσιμα για (5min/30min/1hr/1 ημέρα), τι θα συμβεί;
Αυθεντικότητα	Πόσο σημαντικό είναι να γνωρίζουμε ότι η πηγή των πληροφοριών είναι αυτή που ισχυρίζεται ότι είναι;

Αυτή η αξιολόγηση χρησιμεύει επίσης ως μια λογική εκτίμηση της ελκυστικότητας για έναν εισβολέα. Αν και δεν είναι όλοι οι δυνητικά επιτιθέμενοι παρακινούμενοι από το ίδιο κίνητρο, θα πρέπει να υποτεθεί ότι οποιαδήποτε επίθεση που έχει ως αποτέλεσμα σημαντικές συνέπειες είναι πιθανό να είναι ελκυστική για κάποιο είδος εισβολέα (οικονομικό κέρδος, ανταγωνιστικό πλεονέκτημα, περιέργεια, σαμποτάζ ή ακόμα και τρομοκρατία, θα μπορούσαν να είναι όλα κίνητρα για ορισμένους πιθανούς επιτιθέμενους). (DNVGL-RP-0496 RECOMMENDED PRACTICE).

6.3.5 Προσδιορισμός Της Πιθανότητας Μιας Επίθεσης

Μετά τον προσδιορισμό και την αξιολόγηση των συνεπειών μιας επιτυχημένης επίθεσης, η πιθανότητα μιας επίθεσης καθορίζεται στη συνέχεια για το κάθε υπό εξέταση σύστημα ξεχωριστά.

Διάφοροι παράγοντες μπορούν να οδηγήσουν την πιθανότητα μιας επίθεσης, όπως οι δυνατότητες του επιτιθέμενου, τα κίνητρα και η ευκαιρία προς την επίθεση.

Στο πλαίσιο της συνιστάμενης πρακτικής (πλοία σε λειτουργία), θεωρείται ανέφικτο να εξεταστούν όλες οι πτυχές που οδηγούν την πιθανότητα που αναφέρεται στη βιβλιογραφία. Η εφαρμογή τέτοιων πτυχών θα περιλαμβάνει την αντιμετώπιση πληροφοριών που είτε είναι εξαιρετικά δύσκολο να υπολογιστούν ή δεν είναι διαθέσιμες, και θα απαιτούσε βαθιά γνώση του κώδικα του λογισμικού, της αρχιτεκτονικής του και της διαθεσιμότητας εργαλείων αυτοματισμού τα οποία βρίσκονται στη διάθεση των επιτιθέμενων.

Στην συνιστάμενη πρακτική η αξιολόγηση της «ευκολίας πρόσβασης» χρησιμοποιείται ως πρακτική προσέγγιση της πιθανότητας επίθεσης (ref. /40/, /41/, /42/, /43/). Για παράδειγμα, ένα σύστημα που μπορεί να ενημερωθεί και να ελεγχθεί μέσω μιας απομακρυσμένης σύνδεσης στο Internet είναι πιο εύκολο στην πρόσβαση από ένα αυτόνομο σύστημα, αποσυνδεδεμένο από το διαδίκτυο και διατηρείται ασφαλισμένο πίσω από «κλειδωμένες πόρτες». Στην συνιστάμενη πρακτική χρησιμοποιούνται ως παράδειγμα οι ακόλουθες ιδιότητες, για τον προσδιορισμό της ευκολίας πρόσβασης:

- Απομακρυσμένη σύνδεση (remote access), δηλαδή πρόσβαση στο σύστημα από θέση που δεν βρίσκεται επί του πλοίου. Για παράδειγμα οι απομακρυσμένες συνδέσεις σε ένα κέντρο χερσαίων επιχειρήσεων ή στο σύστημα παρακολούθησης στην ξηρά ενός προμηθευτή εξοπλισμού.
- Φυσικά προσβάσιμη (physically accessible), δηλαδή πρόσβαση στον εξοπλισμό επί του πλοίου. Τα παραδείγματα περιλαμβάνουν τις ξεκλείδωτες πόρτες γραφείων και τις εύκολες ευκαιρίες αλλοίωσης του εξοπλισμού.
- Συνδεδεμένο ή/και ενσωματωμένο (Connected and/or integrated), σύστημα συνδεδεμένο με άλλα συστήματα μέσω δικτύου. Συνήθως η ανταλλαγή πληροφοριών και η κεντρική διαχείριση θα μπορούσαν να αποτελέσουν λόγο για την ενσωμάτωση συστημάτων ή τη δημιουργία διεπαφών.
- Η απαίτηση ενημερώσεων λογισμικού παίζει ρόλο (software updates), καθώς αυτό θα απαιτεί π.χ. τη σύνδεση usb stick ή HDD, προκειμένου να εκτελεστεί μια ενημέρωση στην έκδοση του υπάρχοντος λογισμικού.

Ο συνδυασμός των απαντήσεων σε αυτά τα ερωτήματα μπορεί να συμβάλει στην αξιολόγηση της ευκολίας πρόσβασης, όπως φαίνεται στον πίνακα 6.4:

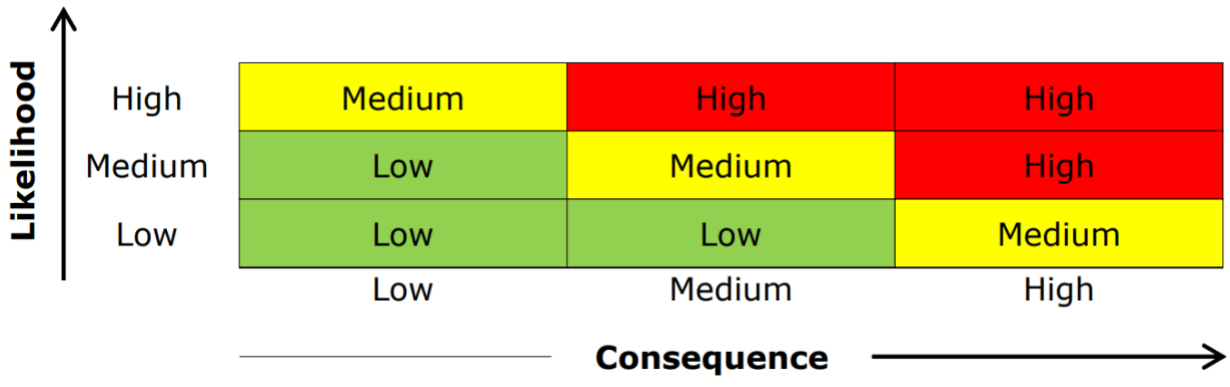
Πίνακας 6.4 Παράδειγμα αξιολόγησης της «ευκολίας πρόσβασης». Πηγή: DNVGL-RP-0496

Απομακρυσμένη Σύνδεση	Φυσικά Προσβάσιμη	Συνδεδεμένο ή Ενσωματωμένο	Απαίτηση για ενημερώσεις λογισμικού	Ευκολία Πρόσβασης
✓	-	-	-	Μεσαία
✓	-	-	✓	Υψηλή
✓	-	✓	Καμμιά επίπτωση στην ευκολία πρόσβασης	Υψηλή
✓	✓	-		Υψηλή
-	-	✓		Μεσαία
-	✓	-		Μεσαία
-	✓	✓		Μεσαία
✓	✓	✓		Υψηλή
-	-	-	✓	Μεσαία
-	-	-	-	Χαμηλή

6.3.6 Προσδιορισμός Του Ρίσκου Μιας Κυβερνοεπίθεσης

Ο ορισμός του ρίσκου είναι η πιθανότητα του να συμβεί ένα γεγονός επί την συνέπεια που θα επιφέρει. Στην παρούσα περίπτωση, ο συνδυασμός της πιθανότητας (ευκολία πρόσβασης) με τις συνέπειες μιας επιτυχημένης επίθεσης καθορίζει τον κίνδυνο του συγκεκριμένου κρίσιμου συστήματος. Όπως φαίνεται στον πίνακα 6.5, η υψηλή πιθανότητα επίθεσης σε συνδυασμό με την υψηλή συνέπεια της επιτυχούς επίθεσης έχει ως αποτέλεσμα υψηλό κίνδυνο (risk) για το υπό εξέταση σύστημα.

Πίνακας 6.5. Πίνακας ρίσκου κυβερνοεπίθεσης (Cyber Security Risk Matrix). Πηγή: DNVGL-RP-0496



Συνδυαστικά από τα ανωτέρω προκύπτει ο πίνακας 6.6 ο οποίος απεικονίζει ένα παράδειγμα κρίσιμου συστήματος ΟΤ (σύστημα AIS), και ενός κρίσιμου συστήματος IT, (PMS - Planned

Maintenance System - Σύστημα Προγραμματισμένης Συντήρησης). Μπορούμε εύκολα να διακρίνουμε το επίπεδο κινδύνου που συνδέεται με καθένα από αυτά, λαμβάνοντας υπόψη τις διαστάσεις της πιθανότητας επίθεσης και τις συνέπειες της επιτυχούς επίθεσης.

Πίνακας 6.6. Παράδειγμα ανάλυσης ρίσκου κυβερνοασφάλειας (Cyber security risk analysis) (DNVGL-RP-0496 RECOMMENDED PRACTICE).

Λειτουργία/σύστημα υπό εξέταση			*Επίπτωση*			*Πιθανότητα*	*Ρίσκο*
Λειτουργία	Σύστημα	Εξάρτημα	Ιδιότητα ασφαλείας (CIAA)	Σημασία της ιδιότητας ασφαλείας	Αιτιολογία για την κατάταξη ιδιότητας ασφαλείας	(X, M, Y)	(X,M,Y)
Πλοήγηση	AIS (OT)	Δ/Ε	Εμπιστευτικότητα	Δ/Ε	…	Υψηλή	Υψηλή
			Ακεραιότητα	Υψηλή	Εσφαλμένα δεδομένα μπορεί να οδηγήσουν σε σύγκρουση ή προσάραξη		
			Διαθεσιμότητα	Χαμηλή	…		
			Αυθεντικότητα	Μεσαία	…		
	GPS (OT)	…	Εμπιστευτικότητα	…	…	…	…
			Ακεραιότητα	…	…		
			Διαθεσιμότητα	…	….		
			Αυθεντικότητα	…	…		
			Εμπιστευτικότητα	Χαμηλή	…		
					Παράβλεψη συντήρησης η οποία		

Προληπτική συντήρηση	PMS (IT)	Δ/Ε	Ακεραιότητα	Μεσαία	μπορεί να είναι επιβλαβής ή δαπανηρή	Μεσαία	Μεσαία
			Διαθεσιμότητα	Μεσαία	Παράβλεψη συντήρησης η οποία μπορεί να είναι επιβλαβής ή δαπανηρή		
			Αυθεντικότητα	Χαμηλή	…		

(Χ=Χαμηλή, Μ=Μεσαία, Υ=Υψηλή, Δ/Ε= Δεν Εφαρμόζεται)

Για τα Λειτουργικά Τεχνολογικά Συστήματα, οι αξιολογήσεις CIAA σε συνδυασμό με την πιθανότητα μιας επίθεσης δίνουν μια ατομική εκτίμηση κινδύνου (μία για τα C, I, A και A ξεχωριστά). Για τα Πληροφοριακά Τεχνολογικά Συστήματα, η υψηλότερη από τις τέσσερις πτυχές (C, I, A, A) σε συνδυασμό με την πιθανότητα επίθεσης χρησιμοποιείται ως αξιολόγηση κινδύνου.

Ανάλογα με το μέγεθος του συστήματος και το επίπεδο λεπτομέρειας της ανάλυσης, η υπό εξέταση λειτουργία ή σύστημα μπορεί είτε να βαθμολογηθεί σε επίπεδο στοιχείου είτε σε επίπεδο συστήματος. Το απαιτούμενο επίπεδο ανάλυσης θα πρέπει να καθορίζεται κατά περίπτωση.

Αποδεκτές εναλλακτικές λύσεις μπορούν να ληφθούν υπόψη για να μετριαστεί η κατάταξη των κινδύνων. Για παράδειγμα, σε περίπτωση που το σύστημα πλοήγησης αποσυνδεθεί, έμπειροι πλοηγοί θα μπορούσαν να καταφύγουν στη χρήση χαρτών και χειροκίνητων μέσων πλοήγησης για την μείωση των συνεπειών. Ως εκ τούτου, ένας οργανισμός θα μπορούσε να επιλέξει να αποδεχθεί την κατάταξη κινδύνου CS του συστήματος εάν υπάρχουν και αποδεκτές εναλλακτικές λύσεις στην περίπτωση μιας κυβερνοεπίθεσης. Στην περίπτωση αυτή, η αποδεκτή εναλλακτική λύση θα καταγράφεται κατά τη διαδικασία κατάταξης και θα προτιμηθεί σαν λύση για να επιβεβαιωθεί η αποτελεσματικότητά της, να διασφαλιστεί ότι είναι γνωστή και κατανοητή από τους χρήστες, και στη συνέχεια θα κοινοποιηθεί και θα διατεθεί στους χρήστες.

6.3.7 Σύγκριση Τρεχόντων Μέτρων Με Τον Τελικό Στόχο

Μόλις προσδιοριστεί ο ειδικός κίνδυνος CS ενός κρίσιμου συστήματος, οι υφιστάμενες διασφαλίσεις θα πρέπει να συγκριθούν με τις διασφαλίσεις-στόχους ανάλογα με τη φύση των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων. Η σύγκριση αυτών των απαιτήσεων με την τρέχουσα κατάσταση των διασφαλίσεων της CS απαιτεί την προετοιμασία προσαρμοσμένων καταλόγων ελέγχου και τη συνέντευξη των σχετικών εμπειρογνωμόνων, του υπεύθυνου προσωπικού και των χρηστών των Πληροφοριακών και Λειτουργικών Τεχνολογικών Συστημάτων. Μετά τη δημιουργία των καταλόγων ελέγχου, διενεργούνται λεπτομερείς έλεγχοι για κάθε ένα από τα υπό εξέταση συστήματα. Αυτοί οι έλεγχοι στη συνέχεια καταγράφονται, περιγράφονται λεπτομερώς και παρακολουθούνται μέσω ενός προγράμματος συνεχούς βελτίωσης. (DNVGL-RP-0496 RECOMMENDED PRACTICE)

6.3.8 Βελτίωση

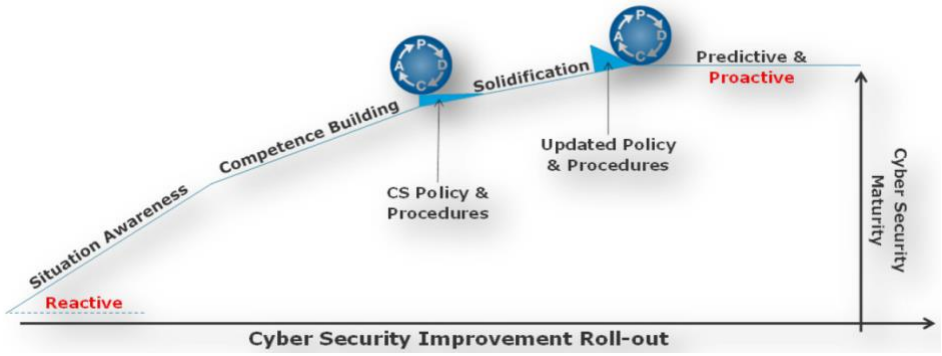
Οι αξιολογήσεις που συνιστώνται στην συνιστάμενη πρακτική συμβάλουν στον εντοπισμό των υπό βελτίωση τομέων. Αυτό ισχύει ιδιαίτερα για την εστιασμένη αξιολόγηση και τη συνολική, σε βάθος αξιολόγηση (με την αξιολόγηση υψηλού επιπέδου να στοχεύει περισσότερο στον εντοπισμό τομέων για περαιτέρω και διεξοδικότερη έρευνα). Ανάλογα με τους διαθέσιμους πόρους και την αξιολόγηση κινδύνου, η διοίκηση θα αποφασίσει φυσικά να εστιάσει αρχικά το σχέδιο βελτίωσης της CS σε συστήματα με υψηλούς κινδύνους CS. Για την αντιμετώπιση των κινδύνων, υπάρχουν διαφορετικές επιλογές μετριασμού, όπως περιγράφεται στον πίνακα 6.7.

Πίνακας 6.7 Επιλογές μετριασμού του κινδύνου. Πηγή: DNVGL-RP-0496

Επιλογές περιορισμού του κινδύνου	***Συνέπειες***
Αποφυγή	Παράκαμψη του κίνδυνου αλλάζοντας την πορεία δράσης (το αντίθετο της αποδοχής κινδύνου)
Μείωση	Εφαρμογή διορθωτικών μέτρων για τη μείωση της πιθανότητας ή/και της σοβαρότητας του κινδύνου
Αποδοχή	Αποδοχή του κίνδυνου και υπολογισμός της πιθανότητας της αρνητικής επίδρασης (το αντίθετο της αποφυγής κινδύνου)
Μεταφορά	Ανάθεση των κινδύνων σε τρίτους (π.χ. ασφάλιση στον κυβερνοχώρο)

Απαιτείται ανάλυση κόστους-οφέλους (Cost-Benefit Analysis) για τον προσδιορισμό της αποτελεσματικότερης στρατηγικής μετριασμού του κινδύνου. Η ανάλυση αυτή απαιτεί

πληροφορίες σχετικά με την εικόνα κινδύνου CS που αποτελείται από τις απειλές, τα τρωτά σημεία και την κρισιμότητα των συστημάτων. Όταν η μείωση του κινδύνου είναι η προτιμώμενη επιλογή, η συνιστάμενη πρακτική συνιστά να χρησιμοποιηθούν τα κενά που εντοπίστηκαν στους αντίστοιχους καταλόγους ελέγχου για τη δημιουργία ενός σχεδίου εργασίας που πρέπει να συμφωνηθεί και να εφαρμοστεί από την αρμόδια ομάδα διαχείρισης. Δεδομένου ότι η εικόνα κινδύνου διαφέρει ανά τμήμα και εταιρεία, δεν είναι εφικτό ένα γενικό σχέδιο βελτίωσης που να ταιριάζει σε όλες τις ανάγκες. Επιπλέον, καθώς η εικόνα κινδύνου CS αλλάζει συνεχώς, απαιτούνται συνεχείς κύκλοι βελτίωσης για να επιβεβαιωθεί ότι οι κατάλογοι ελέγχου και οι πολιτικές-διαδικασίες και τα εμπόδια εξακολουθούν να είναι αποτελεσματικά, να διατηρούνται και να ενημερώνονται. Η προσέγγιση PDCA (Plan, Do, Check, Act) που χρησιμοποιείται για αυτούς τους κύκλους συνεχούς βελτίωσης απαιτείται για κάθε σύστημα διαχείρισης, όπως απεικονίζεται στο διάγραμμα 6.2. Μέσω αυτών των συνεχών κύκλων βελτίωσης, η ωριμότητα και η ανθεκτικότητα του οργανισμού στο CS θα αυξηθούν με την πάροδο του χρόνου, μετατρέποντας το σε ένα προγνωστικό σύστημα το οποίο θα μπορεί να προβλέπει τις πιθανές επιθέσεις ή το σε πιο κομμάτι υστερεί η ασφάλεια του συστήματος.



Διάγραμμα 6.2 Αύξηση των επιπέδων ωριμότητας του οργανισμού στον τομέα της ασφάλειας στον κυβερνοχώρο. Πηγή: DNVGL-RP-0496 RECOMMENDED PRACTICE

Η έγκριση των επενδύσεων που απαιτούνται για τις δράσεις βελτίωσης θα απαιτήσει πιθανότατα μια ανάλυση κόστους-οφέλους. Μια ενημερωμένη εικόνα κινδύνου με αξιολόγηση των σημερινών αναγκών προστασίας και ευκολίας πρόσβασης/ ευρωστίας των τοίχων προστασίας που υπάρχουν μπορεί να είναι χρήσιμη για την κατασκευή των οικονομικών μοντέλων. Η εικόνα αυτή θα βοηθήσει στη λήψη επενδυτικών αποφάσεων καθώς και στην απεικόνιση των υφιστάμενων κινδύνων της CS. Ανάλογα με την επιλεγείσα αξιολόγηση, οι διάφορες προσεγγίσεις απεικόνισης

προτείνονται από την συνιστάμενη πρακτική. (DNVGL-RP-0496 RECOMMENDED PRACTICE)

6.3.9 Ικανότητα Επίγνωσης

Το ηλεκτρονικό ψάρεμα, η κοινωνική μηχανική και οι ακούσιες λήψεις κακόβουλου λογισμικού είναι συνηθισμένα ζητήματα. Το προσωπικό σε πολλούς οργανισμούς δεν είναι επαρκώς προετοιμασμένο και δεν είναι ικανό να αντιδρά σωστά σε περίπτωση συμβάντων CS με αποτέλεσμα οι ενέργειές τους να μην συμβάλλουν επαρκώς στη μείωση των κινδύνων και στον περιορισμό της κατάστασης. Οι αξιολογήσεις που προτείνονται στην συνιστάμενη πρακτική θα πρέπει να επισημαίνουν τμήματα του οργανισμού όπου λείπει η ευαισθητοποίηση ή οι ικανότητες αποτελούν ζήτημα. Συνιστάται να επικεντρωθούν οι εκστρατείες ευαισθητοποίησης και ανάπτυξης ικανοτήτων σε αυτά τα τμήματα του οργανισμού. Οι ηλεκτρονικές γνώσεις σε συνδυασμό με εκπαιδεύσεις μπορούν να συμβάλουν στη βελτίωση της κατάστασης.

Διάφορες ερευνητικές μελέτες ρίχνουν φως στα ποσοστά διατήρησης των ανθρώπινων πληροφοριών. Συνεπώς, η επιθυμητή συμπεριφορά και ευαισθητοποίηση όσον αφορά την CS πρέπει να αξιολογηθεί όπως κάθε άλλος στόχος. Αυτό σημαίνει ότι ο οργανισμός θα πρέπει να έχει περιοδικές ανανεώσεις με βάση την μεταβαλλόμενη εικόνα κινδύνου, το ποσοστό διατήρησης και τις μεταβαλλόμενες απαιτήσεις.

Η απειλή εμπιστευτικών πληροφοριών έχει συνδεθεί ιστορικά με τους φυσικούς συμβιβασμούς και τις παραβιάσεις ασφάλειας. Οι πιο πρόσφατες εκθέσεις της βιομηχανίας έχουν διαπιστώσει ότι πάνω από 60 τοις εκατό των κλεμμένων πληροφοριών (ηλεκτρονικά) ή των παραβιάσεων CS συνδέονται άμεσα με τις απειλές εμπιστευτικών πληροφοριών. Ενώ το ISO/IEC 27001 περιλαμβάνει εν συντομία την απειλή εμπιστευτικών πληροφοριών στο πλαίσιο της πολιτικής των οργανισμών CS, η συνιστάμενη πρακτική προτείνει την αντιμετώπιση της απειλής εμπιστευτικών πληροφοριών της CS. Οι επιχειρήσεις, ιδίως οι μικρές και μεσαίες επιχειρήσεις, πρέπει να εξισορροπούν την πρόσβαση στους εργαζομένους σε πληροφορίες, ενώ παράλληλα να παρακολουθούν την χρήση του δικτύου. Αυτό μπορεί να γίνει με ένα γραπτό, ετήσιο αναθεωρημένο σχέδιο ασφάλειας και διακυβέρνησης πληροφοριών που υπογράφεται από κάθε εργαζόμενο για τη θέσπιση πολιτικών για τη διασφάλιση ιδιόκτητων και ευαίσθητων

πληροφοριών τόσο από την κυβερνοασφάλεια όσο και από την τυχόν φυσική απώλεια. Ιδιαίτερη προσοχή θα πρέπει να δοθεί σε πρώην, δυσαρεστημένους ή προσωρινούς υπαλλήλους που διαθέτουν διαπιστευτήρια για πρόσβαση σε ευαίσθητα ή ιδιόκτητα δεδομένα. Συνιστάται να μην παραχωρείται πρόσβαση στις πληροφορίες των εργαζομένων, εκτός εάν απαιτείται. Επιπλέον, η περιοδική επανεξέταση και η επακόλουθη ανάκληση των διαπιστευτηρίων πρόσβασης αποτελεί απαραίτητο μέρος της προστασίας των δεδομένων της εταιρείας και θα πρέπει να συμπεριληφθούν στην περαιτέρω έκθεση της πολιτικής του οργανισμού για την CS.

6.3.10 Τεχνικές Βελτιώσεις

Υπάρχει ευρύ φάσμα επιλογών για την ενίσχυση των τεχνικών πτυχών της CS και συχνά θα χρησιμοποιούνται από ή σε στενή συνεργασία με τους παρόχους του αντίστοιχου συστήματος. Στην συνιστάμενη πρακτική προτείνεται να επισημανθούν οι τυπικές ευκαιρίες βελτίωσης που βρίσκονται συνήθως στις ναυτιλιακές και υπεράκτιες βιομηχανίες:

- *Ο διαχωρισμός δικτύων (Network segregation)* είναι μια κοινή βέλτιστη πρακτική στα πλοία ανάλογα με την κρισιμότητα των δικτυωμένων συσκευών. Η ελάχιστη απαίτηση είναι να υπάρχουν χωριστά δίκτυα τόσο για τα συστήματα ασφαλείας όσο και για κρίσιμα συστήματα για τη λειτουργία του πλοίου. Συνιστάμενη πρακτική είναι να υπάρχουν ξεχωριστά δίκτυα για τους διαχειριστές, για την ψυχαγωγία και πρόσβαση στο διαδίκτυο, με δίκτυα φυσικά ή σχεδόν διαχωρισμένα. Η φυσική πρόσβαση σε καλωδιώσεις πρέπει να περιορίζεται, όπως και η διοικητική πρόσβαση στους διακόπτες VLAN. Βλέπε App.A και ISO/ IEC 27002:2013 ref. /7/, ενότητα 13.1.3. Εάν επιτρέπεται η κυκλοφορία δεδομένων μεταξύ τμημάτων, η κυκλοφορία αυτή θα πρέπει να ελέγχεται από τείχος προστασίας ή συσκευή δικτύου με λειτουργία τείχους προστασίας. Πιο ακριβείς οδηγίες σχετικά με τις ρυθμίσεις τείχους προστασίας είναι διαθέσιμες στο ref. /25/. Όταν ο διαχωρισμός δικτύου χρησιμοποιείται ως μέσο για την αντιμετώπιση των απαιτήσεων ασφάλειας, αξιοπιστίας ή ασφάλειας στον κυβερνοχώρο, διατηρούνται τυχόν αλλαγές στην κατάτμηση, π.χ. με την εισαγωγή του WLAN και οι αλλαγές στην καλωδίωση ή τη διαμόρφωση VLAN απαιτούν διεξοδική και τεκμηριωμένη διαχείριση της διαδικασίας αλλαγής, συμπεριλαμβανομένης της εκτίμησης κινδύνου.
- *Οι εργοστασιακοί προεπιλεγμένοι λογαριασμοί και κωδικοί πρόσβασης (Factory default accounts and passwords)* δεν πρέπει να επιτρέπονται σε καμία συσκευή. Πολλά συστήματα και στοιχεία δικτύου (δρομολογητές, πολυπλέκτες φωνητικών δεδομένων κ.λπ.) παραδίδονται με προεπιλεγμένους κωδικούς πρόσβασης κατασκευαστή, οι οποίοι θα πρέπει να αλλάξουν κατά την εγκατάσταση.
- *Ο έλεγχος πρόσβασης (Access control)* είναι ένα βασικό στοιχείο ελέγχου για τον μετριασμό των κινδύνων. Για παράδειγμα, ο περιορισμός των αδειών πρόσβασης σε ένα μικρό σύνολο μπορεί να αποτρέψει την εισαγωγή κακοήθων αρχείων, να εξασφαλίσει την

ακεραιότητα του τείχους προστασίας, κλπ. Αυτό μπορεί για παράδειγμα να βοηθήσει στην αποφυγή ακούσιας καταστροφής αρχείων κατά τη διάρκεια καθημερινών και συνηθισμένων λειτουργιών από χρήστες οι οποίοι έχουν διαπιστευτήρια διαχειριστή ενώ δεν είναι απαραίτητο.

- *Αυστηροποίηση ασφαλών απομακρυσμένων συνδέσεων (Hardening secure remote connections)*. Οι απομακρυσμένες συνδέσεις σε Πληροφοριακά και Λειτουργικά Τεχνολογικά Συστήματα θα πρέπει να ελέγχονται αυστηρά. Οι κωδικοί πρόσβασης από μόνοι τους είναι μια αδύναμη μέθοδος προστασίας. Τα συστήματα ελέγχου ταυτότητας δύο παραγόντων, όπως τα διακριτικά, οι εφάπαξ κωδικοί πρόσβασης ή τα ψηφιακά πιστοποιητικά, ενδέχεται να είναι δύσκολο να διατηρηθούν με ασφάλεια σε ένα θαλάσσιο περιβάλλον για όλη τη διάρκεια ζωής ενός πλοίου. Θα πρέπει να διερευνηθούν οι σύγχρονες προσεγγίσεις των πλαισίων ελέγχου ταυτότητας δύο παραγόντων, όπως το OAuth (που βασίζεται σε έλεγχο ταυτότητας μέσω του smartphone του χρήστη).
- *Η διαχείριση διαμόρφωσης λογισμικού (Software configuration management)* αποτελεί σημαντικό στοιχείο των μειώσεων του κινδύνου στον κυβερνοχώρο. Η παρακολούθηση των αλλαγών λογισμικού θα πρέπει να περιλαμβάνεται σε μια διαδικασία διαχείρισης αλλαγών.
- *Η διαχείριση ενημερωμένων εκδόσεων κώδικα λογισμικού (Software patch management)* βοηθά στην αντιμετώπιση ενός από τα πιο συνηθισμένων θεμάτων ευπάθειας, δηλαδή του λογισμικού χωρίς επιδιόρθωση (unpatched software). Η εφαρμογή αυτής της πρακτικής συμβάλλει στον περιορισμό της αποτελεσματικότητας των επιτιθέμενων που εκμεταλλεύονται τη γνώση ευπαθειών που μπορούν να έχουν πρόσβαση όλοι. Η διαχείριση ενημερωμένων εκδόσεων κώδικα λογισμικού αποτελεί μέρος της γενικής πρακτικής διαχείρισης παραμέτρων λογισμικού.
- *Η δημιουργία πληροφοριών τοπολογίας λογισμικού (Creating software topology information)* θα ελέγξει εάν έχουν εφαρμοστεί αρχές διαχωρισμού δικτύου. Αυτό μπορεί εύκολα να γίνει με τη χρήση της τοπολογίας δικτύου ως σημείο εκκίνησης και τη σύνδεση ή / και την εμφάνιση των ονομάτων του συστήματος λογισμικού που εκτελούνται σε αυτά τα συστήματα διασταυρώνοντας τα με το μητρώο του εκάστοτε λογισμικού.

6.3.11 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Πολλοί οργανισμοί θεωρούν ότι αξίζει τον κόπο να δημιουργήσουν ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών (Information Safety Management System - ISMS) σύμφωνα με το διεθνές πρότυπο ISO/IEC 27001 ref. /7/. Το πρότυπο είναι πλήρως ευθυγραμμισμένο με τις πρόσφατες εκδόσεις των συνηθισμένων προτύπων συστημάτων διαχείρισης ISO, όπως το ISO 9001:2015 (για τη διαχείριση της ποιότητας) και το ISO 14001:2015 (για την περιβαλλοντική διαχείριση), επιτρέποντας την εύκολη ενσωμάτωση του ISMS στο ευρύτερο πεδίο εφαρμογής του ολοκληρωμένου συστήματος διαχείρισης μιας εταιρείας, εάν το επιθυμεί.

Το ISO/IEC 27001 απαιτεί συνεχή διαχείριση της CS, μέσω της εφαρμογής ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ISMS). Το ISMS καθιερώνεται, εφαρμόζεται, συντηρείται και βελτιώνεται συνεχώς σύμφωνα με τις απαιτήσεις του ISO/IEC 27001, καλύπτοντας την οργάνωση, τις αρμοδιότητες και τη διαχείριση των Λειτουργικών και Πληροφοριακών Τεχνολογικών Συστημάτων. Η συνιστάμενη πρακτική ασχολείται με τις επιχειρησιακές πτυχές της διαχείρισης της CS, εστιάζοντας στο εν λειτουργία πλοίο. Η προσέγγιση κατά ISO/ IEC 27001 συμπληρώνει την προσέγγιση της συνιστάμενης πρακτικής με μια οργανωτική προσέγγιση, δίνοντας μεγάλη έμφαση στο σχεδιασμό, τους πόρους και τη συνεχή βελτίωση.

Οι χρήστες της παρούσας συνιστάμενης πρακτικής θα διαπιστώσουν ότι η αντιμετώπιση των προκλήσεων που σχετίζονται με την CS έχει πολλά κοινά σημεία με άλλα καθήκοντα που διαχειρίζονται. Η αξιολόγηση, η βελτίωση και η επαλήθευση είναι απαραίτητη για κάθε διαδικασία, όπως και η συνεχής βελτίωση αυτών των δραστηριοτήτων για την εξασφάλιση της προόδου με την πάροδο του χρόνου και την προσαρμογή σε ένα συνεχώς μεταβαλλόμενο περιβάλλον. Δεδομένου ότι η CS αποτελεί μια αρκετά νέα πρόκληση για τη ναυτιλιακή και υπεράκτια βιομηχανία, αυτή η συνιστάμενη πρακτική δίνει έμφαση σε μια διεξοδική αξιολόγηση της εικόνας του κινδύνου. Προτείνει την κατανόηση των απειλών, των τρωτών σημείων και των πιθανών συνεπειών ως βάση για οποιαδήποτε δραστηριότητα βελτίωσης και επαλήθευσης. (DNVGL-RP-0496 RECOMMENDED PRACTICE)

7 ΣΥΜΠΕΡΑΣΜΑΤΑ

Μέσα από την παρούσα μελέτη είδαμε, σε όσο το δυνατό αναλυτικό βαθμό, τα θέματα νομοθεσίας και βέλτιστων πρακτικών που αφορούν την ασφάλεια στον Κυβερνοχώρο στον τομέα της ναυτιλίας. Προς αυτήν την κατεύθυνση, αφού δόθηκαν κάποιοι βασικοί ορισμοί, παρουσιάστηκε η νομοθεσία τόσο σε παγκόσμιο όσο και σε Ευρωπαϊκό επίπεδο.

Το 2017, ο IMO εξέδωσε τις κατευθυντήριες γραμμές MSC-FAL.1/Circ.3 με θέμα «Κατευθυντήριες γραμμές για τη διαχείριση των θαλάσσιων κινδύνων στον κυβερνοχώρο». Αυτές οι κατευθυντήριες γραμμές παρείχαν συστάσεις υψηλού επιπέδου για την προστασία της ναυτιλίας από τρέχουσες και αναδυόμενες απειλές και τρωτά σημεία στον κυβερνοχώρο, συμπεριλαμβανομένων λειτουργικών στοιχείων για την υποστήριξη της αποτελεσματικής διαχείρισης του κινδύνου στον κυβερνοχώρο. Στη συνέχεια, ο IMO ενέκρινε τις κατευθυντήριες αυτές γραμμές μέσω του ψηφίσματος (Resolution) MSC.428(98) με τίτλο «Θαλάσσια διαχείριση κινδύνων στον κυβερνοχώρο στα συστήματα διαχείρισης της ασφάλειας».

Αυτό το ψήφισμα ενθάρρυνε τις διοικήσεις να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται δεόντως στα υφιστάμενα συστήματα διαχείρισης της ασφάλειας (όπως ορίζονται στον διεθνή κώδικα διαχείρισης της ασφάλειας ISM) το αργότερο κατά την πρώτη ετήσια επαλήθευση του εγγράφου συμμόρφωσης (Document of Compliance - DoC) της εταιρείας μετά την 1η Ιανουαρίου 2021.(https://www.lr.org)

Το ψήφισμα (Resolution) MSC.428(98) με τίτλο «Θαλάσσια διαχείριση κινδύνων στον κυβερνοχώρο στα συστήματα διαχείρισης της ασφάλειας» , που εκδόθηκε για τον παραπάνω λόγο από την επιτροπή αυτή , περιλαμβάνει επίσης περαιτέρω συστάσεις, οι οποίες μπορούν να συνοψιστούν ως εξής:

- **Προσδιορισμός (Identify)**: Ορισμός ρόλων και ευθυνών προσωπικού για τη διαχείριση κινδύνων στον κυβερνοχώρο και προσδιορισμός των συστημάτων, των περιουσιακών στοιχείων, των δεδομένων και των δυνατοτήτων που, όταν διαταραχθούν, ενέχουν κινδύνους για τις λειτουργίες των πλοίων.
- **Προστασία (Protect)**: Εφαρμογή διαδικασιών και μέτρων ελέγχου κινδύνων και σχεδιασμός έκτακτης ανάγκης για την προστασία από ένα γεγονός στον κυβερνοχώρο και τη διασφάλιση της συνέχειας των ναυτιλιακών δραστηριοτήτων.
- **Εντοπισμός (Detect)**: Ανάπτυξη και υλοποίηση δραστηριοτήτων που είναι απαραίτητες για τον έγκαιρο εντοπισμό ενός συμβάντος στον κυβερνοχώρο.
- **Αντίδραση (Respond)**: Ανάπτυξη και υλοποίηση δραστηριοτήτων και σχεδίων για την παροχή ανθεκτικότητας και την αποκατάσταση των συστημάτων που είναι απαραίτητα για τις λειτουργίες ή τις υπηρεσίες αποστολής που έχουν υποστεί προβλήματα λόγω ενός συμβάντος στον κυβερνοχώρο.
- **Ανάκτηση (Recover)**: Προσδιορισμός μέτρων για την υποστήριξη και την αποκατάσταση των συστημάτων στον κυβερνοχώρο που είναι απαραίτητα για τις ναυτιλιακές επιχειρήσεις που επηρεάζονται από ένα συμβάν στον κυβερνοχώρο (https://safety4sea.com)

Επικεντρώνοντας στη νομοθεσία του IMO, ως το βασικότερο εργαλείο που έχουν οι ενδιαφερόμενοι στα χέρια τους, θα θέλαμε να επισημάνουμε πως, έτσι όπως έχει διατυπωθεί, κινείται σε εξαιρετικά αφαιρετικό και γενικό επίπεδο. Αυτό το γεγονός δεν βοηθά, αυτούς που πρόκειται να προβούν στην τήρηση της νομοθεσίας, να κινηθούν μέσα σε συγκεκριμένα και πιο «απτά» πλαίσια. Επόμενο είναι, λοιπόν, οι πλοιοκτήτες και οι διαχειριστές των πλοίων να μην γνωρίζουν με σαφήνεια, αλλά και ακρίβεια, σε ποιες δράσεις θα πρέπει να προβούν προκειμένου να αντιμετωπίσουν αποτελεσματικά τα πλοία τους από έναν ακόμη, μεταξύ τόσων άλλων, κίνδυνο αυτός στον Κυβερνοχώρο.

Από τη σκοπιά που αναπτύξαμε παραπάνω κρίνεται απαραίτητο και αναγκαίο να δοθούν σαφείς οδηγίες – τόσο από τα κράτη όσο και από τους νομοθέτες – που να είναι συγκεκριμένες και

περιγραφικές. Αυτό θα βοηθήσει τους πλοιοκτήτες, ως αποδέκτες της νομοθεσίας, να κατανοήσουν πλήρως το τι πρέπει να πράξουν για να προστατευθεί ο στόλος τους και η εταιρεία τους από τον κίνδυνο στον Κυβερνοχώρο.

Σίγουρα θα προκύψουν περισσότερα κόστη όσον αφορά εξοπλισμό αλλά και προσωπικό που θα είναι εξειδικευμένο ή θα αποκτήσει την απαραίτητη γνώση επί του συγκεκριμένου θέματος. Επίσης ανακύπτει και θέμα γραφειοκρατικό με την έννοια της μίας ακόμη δουλειάς – της εκπόνησης του Risk Assessment - που θα πρέπει να γίνει για να μπορεί να αντιμετωπιστεί αυτός ο νέος κίνδυνος. Για αυτό το λόγο, και με βάση τη σαφήνεια της νομοθεσίας, χρειάζεται οι πλοιοκτήτες να έχουν «στα χέρια τους» συγκεκριμένες κατευθύνσεις που θα τους βοηθήσουν να πορευτούν όσο γίνεται εντός νομοθετικών πλαισίων αλλά και να αντιμετωπίσουν τα οποιαδήποτε κόστη, οικονομικά και γραφειοκρατικά, προκύπτουν από τη νέα αυτή πρόκληση.

Η νομοθεσία, όντας περισσότερο συγκεκριμένη και περιγραφική, βοηθά και τα όποια μέτρα και διαδικασίες προβλεφθούν και ληφθούν να είναι όσο γίνεται πιο «καθαρά» σε επικείμενη επιθεώρηση τους. Είναι βασικό να έχουμε ποσοτικοποιήσει τους παράγοντες του ρίσκου στον κυβερνοχώρο, έτσι ώστε ο επιθεωρητής που θα πραγματοποιήσει επιθεώρηση να μπορεί να ελέγξει «μετρήσιμα» μεγέθη, και για να έχουν υπόσταση οι αποφάσεις που επίκειται να λάβει. Η εκπόνηση, λοιπόν, ενός Risk Assessment, που θα γίνει από το επιθεωρούμενο μέρος, είναι απαραίτητο να κινείται εντός όσο γίνεται μέσα σε ένα σαφές και περιγραφικό επίπεδο ώστε ο επιθεωρητής με βάση τα δεδομένα και τα αποτελέσματα που βλέπει να γνωρίζει τι θα πράξει και τι θα αποφασίσει.

Ένα βασικό θέμα αφορά και την εκπαίδευση του πληρώματος πάνω στο θέμα της αντιμετώπισης του κινδύνου στον Κυβερνοχώρο. Αυτήν την στιγμή το πλήρωμα ενός πλοίου, επίσημα, δεν υπόκειται σε κάποια εκπαίδευση που να αφορά την ασφάλεια στον Κυβερνοχώρο. Ταυτόχρονα, στο δυναμικό εντός του πλοίου, παρέχεται εκπαίδευση για άλλα θέματα όπως για παράδειγμα η ναυσιπλοΐα, στην ασφάλεια για την περιουσία (safety) κλπ. Κρίνεται, έτσι, επιτακτική η ανάγκη ενσωμάτωσης στον κώδικα STCW συγκεκριμένων διαδικασιών εκπαίδευσης πάνω στο θέμα του Κυβερνοχώρου. Ο IMO, να σημειωθεί, δημιουργεί νομοθεσία για την εκπαίδευση μέσα από μία υποεπιτροπή - της βασικής επιτροπής MSC – που ονομάζεται Human element, Training and Watchkeeping (HTW).

Στη συνέχεια της μελέτης αυτής ασχοληθήκαμε με τις βέλτιστες πρακτικές που προτείνονται όσον αφορά την ασφάλεια στον Κυβερνοχώρο. Οι βέλτιστες πρακτικές έχουν σχεδιαστεί για την ανάπτυξη της κατανόησης και της συνειδητοποίησης βασικών πτυχών της ασφάλειας στον κυβερνοχώρο και δεν αποσκοπούν στην παροχή τεχνικής καθοδήγησης για το πλοίο ή το προσωπικό επί του πλοίου. Οι πρακτικές αυτές, ως κατευθυντήριες γραμμές, επικεντρώνονται σε ξεχωριστά ζητήματα επί των πλοίων και αναλαμβάνουν ένα υψηλό επίπεδο δέσμευσης από την εταιρεία στην ξηρά. Γενικά, παρέχουν καθοδήγηση στους πλοιοκτήτες και τους φορείς εκμετάλλευσης σχετικά με τον τρόπο αξιολόγησης των λειτουργιών τους και την ανάπτυξη των απαραίτητων διαδικασιών και δράσεων για τη βελτίωση της ανθεκτικότητας και τη διατήρηση της ακεραιότητας των συστημάτων επί των πλοίων τους. Υπογραμμίζουμε πως οι βέλτιστες πρακτικές είναι προτάσεις που δεν έχουν υποχρεωτικό χαρακτήρα όπως η επίσημη νομοθεσία του IMO. (https://www.intercargo.org)

Εκτός από τις βέλτιστες πρακτικές, κρίναμε απαραίτητο να κάνουμε και μία παρουσίαση των απαιτήσεων βιομηχανίας (Industry Requirements). Αυτές ασφαλώς και δίνουν κατευθυντήριες γραμμές περισσότερο εξειδικευμένες αλλά κινούνται εκτός του νομοθετικού πλαισίου αφού δεν είναι υποχρεωτικό να εκτελεστούν από τους πλοιοκτήτες. Παρόλα αυτά, ειδικά για τα δεξαμενόπλοια, εάν δεν εφαρμοστούν οι απαιτήσεις αυτές τότε ο πλοιοκτήτης δεν μπορεί να συνεργαστεί με βασικές πετρελαϊκές εταιρείες που θέτουν τις εν λόγω απαιτήσεις.

Οι κίνδυνοι στον Κυβερνοχώρο είναι μία νέα πραγματικότητα που, πλέον, αγγίζει τα τελευταία χρόνια αισθητά και τον τομέα της ναυτιλίας. Σε προηγούμενες εποχές, ο κυβερνοχώρος τοποθετείτο σε δεύτερη μοίρα από τη ναυτιλιακή βιομηχανία καθώς υπήρχαν άλλες προτεραιότητες από την κοινότητα αλλά και συγχρόνως οι φορείς των κυβερνοεπιθέσεων δεν την είχαν βάλει ακόμη στο στόχαστρό τους. Μετά από πολύ ηχηρά και ειδικά ζημιογόνα και καίρια χτυπήματα των χάκερς είτε στις ναυτιλιακές εταιρείες είτε στα πλοία των στόλων τους οι αρμόδιοι φορείς με κύριο άξονα τον IMO ξεκίνησαν τις σχετικές διαδικασίες και νομοθέτησαν επί του σοβαρού ζητήματος του κυβερνοχώρου. Με την είσοδο του 2021, οπότε και θα αρχίζει η εφαρμογή της νομοθεσίας όπως την παρουσιάσαμε, γεννιέται η προσδοκία πως το νομοθετικό πλαίσιο θα επηρεάσει θετικά την αντιμετώπιση των κινδύνων του Κυβερνοχώρου. Όπως παρατηρήσαμε, ίσως χρειάζεται η νομοθεσία να κινείται σε πιο σαφές και περιγραφικό πλαίσιο, αλλά σε πρώτη φάση έχουν τεθεί επί τάπητος και οι ανάλογες βέλτιστες πρακτικές που

συμπληρώνουν τα ενδιαφερόμενα μέρη να προχωρήσουν σε πιο συγκεκριμένες κινήσεις. Κρίνεται, έτσι , σκόπιμο να παρατηρηθούν οι πρώτοι αντίκτυποι της νομοθεσίας πάνω στο νέο αυτό πρόβλημα και, εάν χρειαστεί, σε κατάλληλο χρόνο να γίνουν οι οποιεσδήποτε νέες παρεμβάσεις από το νομοθέτη και να μπορέσει έγκαιρα να διορθώσει τα κακώς κείμενα. Μέσα σε αυτή τη διαδικασία συνεχούς παρατήρησης και έγκαιρης, αν χρειαστεί, επανόρθωσης πιστεύεται ότι σταδιακά το φλέγον θέμα των κινδύνων από τον Κυβερνοχώρο θα είναι υπό έλεγχο και επιτήρηση οπότε η ναυτιλία θα μπορεί να νοιώθει και σε αυτόν τον τομέα πλήρης αλλά και στιβαρή.

8 ΒΙΒΛΙΟΓΡΑΦΙΑ

8.1 ΄ΕΝΤΥΠΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1) 2020. *Cyber security resilience management for ships and mobile offshore units in operation*. DNVGL-RP-0496.
2) 2016. *CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES*. 2nd ed. ABS CyberSafetyTM VOLUME 2.
3) 2017. *Tanker Management and Self Assessment 3 (TMSA3) A Best Practice Guide*. 3rd ed. The Oil Companies International Marine Forum.
4) 2017. *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT MSC-FAL.1/Circ.3*.
5) 1998. *MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS RESOLUTION MSC.428(98)*. 1st ed. THE MARITIME SAFETY COMMITTEE,.
6) 2004. *Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance)*.
7) 2006. *Regulation (EC) No 336/2006 of the European Parliament and of the Council of 15 February 2006 on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) No 3051/95 (Text with EEA relevance)*.

8) 2020. *The guidelines on cyber security onboard ships*. 3rd ed. BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL.
9) 2016. *Best Practices for Cyber Security On-board Ships*. 1st ed. Agence Nationale de la Sécurité des Systèmes d'information ANSSI
10) Drougkas, A., Sarri, A., Kyranoudi, P. and Zisi, A., 2019. *Port cybersecurity*.

8.2 ΗΛΕΚΤΡΟΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1) Iacs.org.uk. 2021. *12 IACS RECOMMENDATIONS ON CYBER SAFETY MARK STEP CHANGE IN DELIVERY OF CYBER RESILIENT SHIPS - IACS*. [online] Available at: <http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/> [Accessed 1 February 2021].
2) Enisa.europa.eu. 2021. [online] Available at: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> [Accessed 5 January 2021].
3) He-alert.org. 2021. [online] Available at: <https://www.he-alert.org/filemanager/root/site_assets/standalone_article_pdfs_1220-/he01335.pdf> [Accessed 28 January 2021].
4) https://www.ics-shipping.org/. 2021. [online] Available at: <https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20> [Accessed 8 January 2021].
5) Ship Technology. 2021. [online] Available at: <https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/> [Accessed 8 January 2021].

6) Emsa.europa.eu. 2021. *Awareness in Maritime Cybersecurity*. [online] Available at: <http://www.emsa.europa.eu/fc-default-view/item/3477-cybersec.html> [Accessed 15 January 2021].
7) Emsa.europa.eu. 2021. *Awareness in Maritime Cybersecurity - International legal framework*. [online] Available at: <http://emsa.europa.eu/e-learning/cybersec/AMC003/story_html5.html> [Accessed 26 January 2021].
8) Eur-lex.europa.eu. 2021. *EUR-Lex - 32004R0725 - EN - EUR-Lex*. [online] Available at: <https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A32004R0725> [Accessed 15 January 2021].
9) GTMaritime. 2021. *IMO 2021 Cyber Guideline Compliance - GTMaritime*. [online] Available at: <https://www.gtmaritime.com/tools-and-guides/imo-2021-cyber-guideline-compliance/> [Accessed 8 January 2021].
10) SAFETY4SEA. 2021. *ISM Code as the key driver in addressing cyber risk - SAFETY4SEA*. [online] Available at: <https://safety4sea.com/cm-ism-code-as-the-key-driver-in-addressing-cyber-risk/> [Accessed 8 January 2021].
11) Cult of Sea. 2021. *ISPS code - A measure to enhance the security of Ships and Port facilities*. [online] Available at: <https://cultofsea.com/security/isps-ships-port-facilities/> [Accessed 8 January 2021].
12) Imo.org. 2021. *Maritime cyber risk*. [online] Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 8 January 2021].
13) Tools.ietf.org. 2021. *RFC 2828 - Internet Security Glossary*. [online] Available at: <https://tools.ietf.org/html/rfc2828> [Accessed 8 January 2021].
14) Lloyd's Register. 2021. *The clock is ticking for compliance with IMO's 2021 cyber security regulations.*. [online] Available at: <https://www.lr.org/en-gb/insights/articles/cyber-security-regulation-compliance/> [Accessed 28 January 2021].
15) Intercargo. 2021. *The Guidelines on Cyber Security onboard Ships - Intercargo*. [online] Available at: <https://www.intercargo.org/guidelines-cyber-security-onboard-ships/> [Accessed 28 January 2021].
16) Tripwire, I., 2021. *Maritime Cybersecurity-The Challenges, Best Practices and Risk Mitigation*. [online] The State of Security. Available at: <https://www.tripwire.com/state-

of-security/security-data-protection/biggest-challenges-best-practices-mitigate-risks-maritime-cybersecurity/> [Accessed 27 January 2021].

17) 27001Academy. 2021. *What is ISO 27001? A beginner's guide.*. [online] Available at: <https://advisera.com/27001academy/what-is-iso-27001/> [Accessed 22 January 2021].

https://orcid.org/0000-0002-7388-7613