ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΠΡΟΗΓΜΕΝΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ

Συνεργατικά Συστήματα Διαχείρισης Κινδύνου στα Πληροφοριακά Συστήματα Λιμένων

Παναγιώτης Αθανασίου
ΜΠΣΠ 14002

Επιβλέποντες Καθηγητές

Κοτζανικολάου Παναγιώτης (Επικ. Καθ)
Πατσάκης Κωνσταντίνος (Λεκ.)
Δουληγέρης Χρήστος (Καθ.)

ΠΕΙΡΑΙΑΣ
ΟΚΤΩΒΡΙΟΣ 2015

Σύνοψη

Στην παρούσα διπλωματική εργασία διερευνάται το θέμα της ασφάλειας των εμπορικών λιμένων. Στόχος είναι να επιτευχθεί ολιστικός έλεγχος και αξιολόγηση της ασφάλειας, ο οποίος να περιλαμβάνει τόσο την φυσική ασφάλεια των εγκαταστάσεων, όσο και την ασφάλεια των πληροφοριακών τους συστημάτων.
Εφόσον επισημανθούν τα κενά στις υφιστάμενες, νομοθεσίες, πρότυπα και τα υπάρχοντα εργαλεία διαχείρισης κινδύνου, προτείνεται μία λύση για να αντιμετωπιστούν τα θέματα που προκύπτουν.

Η εργασία ολοκληρώνεται με την παρουσίαση μίας ιστοσελίδας που αναπτύχθηκε η οποία προσφέρει ένα εργαλείο για την αξιολόγηση του επιπέδου της ασφάλειας ενός εμπορικού λιμένα, το εργαλείο Medusa.

Abstract

The present thesis explores the issue of security in commercial ports. The main goal is the achievement of a holistic security control and assessment that includes both physical security of port facilities and their information systems.
After identifying the gaps in existing laws, standards and port security management tools we propose a solution to address the emerging issues.

The thesis concludes with the presentation of a developed website, which provides a tool for the assessment of a commercial port's security level, the risk assessment tool, Medusa

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω την καθηγήτρια κα. Δέσποινα Πολέμη που μου ανέθεσε αυτήν την διπλωματική εργασία και μου επέτρεψε να ασχοληθώ με ένα τόσο καινοτόμο θέμα, ανοίγοντας μου νέους δρόμους στον κόσμο της Πληροφορικής και της Ασφάλειας.

Ευχαριστώ επίσης ιδιαίτερα τον Δρ. Κλεάνθη Δέλλιο, τον υποψήφιο διδάκτορα Σπύρο Παπαστεργίου και τον συμφοιτητή μου Νίκο Λυκουσά για την βοήθεια τους.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Η ολοένα αυξανόμενη ανάγκη για την χρήση πληροφοριακών συστημάτων σε οργανισμούς και σε εταιρίες είναι πλέον γεγονός. Κρίνεται απαραίτητη η ανάγκη για την ασφάλεια αυτών των πληροφοριακών συστημάτων με σκοπό την διασφάλιση της βιωσιμότητας του οργανισμού.
Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Σαν αποτέλεσμα, στο μεγαλύτερο ποσοστό των οργανισμών η χρήση των πληροφοριακών συστημάτων είναι απολύτως αναγκαία για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Έτσι, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του οργανισμού να λειτουργήσει αποδοτικά.

Εκτός από τις οικονομικές επιπτώσεις όμως, τα προβλήματα ασφαλείας πληροφοριακών συστημάτων γίνονται ακόμα πιο αισθητά σε συστήματα που περιέχουν ευαίσθητα δεδομένα ή επιτελούν «ευαίσθητες» και σημαντικές λειτουργίες. Παραδείγματα τέτοιων συστημάτων είναι συστήματα με απόρρητα στρατιωτικά δεδομένα, συστήματα ελέγχου εναέριας κυκλοφορίας, συστήματα με ευαίσθητα ιατρικά δεδομένα, συστήματα που περιέχουν ευαίσθητα προσωπικά δεδομένα κ.α.
Είναι φανερό ότι η ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα την ανθρώπινη ζωή και την ασφάλεια σε τοπικό, εθνικό αλλά και σε παγκόσμιο επίπεδο. Δεν υπάρχει λοιπόν αμφιβολία ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύοντα ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

Τα λιμάνια, θεωρούνται τα πλέον πιο πολύπλοκα πληροφορικά συστήματα, καθώς πολλές και πολύπλοκες οντότητες παίζουν σημαντικό ρόλο για την επίτευξη ενός στόχου. Πρέπει λοιπόν να αναγνωριστούν οι ευπάθειες τους και οι πιθανοί κίνδυνοι που προέρχονται από αυτές, και να προταθούν λύσεις για την έγκαιρη αντιμετώπισή αυτών των προβλημάτων. Η διαδικασία αυτή ονομάζεται εκτίμηση κινδύνου, και είναι πλέον αναγκαία σε κάθε σύγχρονη εταιρεία και οργανισμό.

Σκοπός την παρούσας διπλωματικής εργασίας είναι η κατασκευή ενός web based εργαλείου, με σκοπό την ανάλυση κινδύνων στα λιμάνια, που θα είναι συγχρόνως και μια πλατφόρμα που θα μπορούν να έχουν πρόσβαση πολλοί χρήστες παγκοσμίως, ταυτόχρονα με σκοπό την συλλογική αξιολόγηση και αντιμετώπιση

των κινδύνων αυτών. Το εργαλείο Medusa, όπως και ονομάζεται, αποτελεί μια προέκταση του εργαλείου CYSM, και θα είναι cloud based, υπό την έννοια ότι οποιοσδήποτε χρήστης θα είναι σε θέση να αξιολογήσει τις υπηρεσίες του εκάστοτε λιμανιού, απλά με την χρήση του λογαριασμού του, από μια ευρεία γκάμα αντιμέτρων που θα είναι καταχωρημένα στην βάση του συστήματος Medusa και με την περαιτέρω δυνατότητα επέκτασης τους.

Η εύρεση αδυναμιών και η συνολική αξιολόγηση της υποδομής ενός λιμένα, θα έχει ως σκοπό την έγκαιρη πρόληψη κινδύνων για την αποφυγή επαγγελματικών και οικονομικών επιπτώσεων καθώς και την προστασία της ασφάλειας και της υγείας των εργαζομένων.

1.1 Ιστορική Αναδρομή

Η επίθεση της 11ης Σεπτεμβρίου 2001 οδήγησε με τραγικό τρόπο στη συνειδητοποίηση της απειλής για το παγκόσμιο σύστημα μεταφορών από έκνομες ενέργειες, και αντίστοιχα στην ανάγκη για ενίσχυση των συνθηκών ασφάλειας σε όλα τα μέσα μεταφοράς. Η αναθεωρημένη Διεθνής Σύμβαση για την Ασφάλεια της Ζωής στη Θάλασσα (SOLAS 1974), με την υιοθέτηση του Διεθνούς Κώδικα για την Ασφάλεια Πλοίων και Λιμενικών Εγκαταστάσεων από Έκνομες Ενέργειες (ISPS Code), σε συνδυασμό με τον Κανονισμό (ΕΚ) 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης, αποτελούν ουσιαστικές πρωτοβουλίες που θα συμβάλλουν στην ενίσχυση των συνθηκών ασφάλειας των λιμένων. Οι τροποποιήσεις θεσπίζουν ένα τυποποιημένο, συμβατό διεθνές πλαίσιο για την ανίχνευση των απειλών κατά της ασφάλειας ενώ μεταξύ των άλλων ρυθμίζουν και τις επί μέρους υποχρεώσεις των φορέων και αρμοδίων αρχών που εμπλέκονται στην θαλάσσια μεταφορά και την εξυπηρέτηση του πλοίου στο λιμένα, λαμβάνοντας προληπτικά μέτρα για να μειωθεί ο κίνδυνος ενεργειών προσβολής της ασφάλειας πλοίων και λιμενικών εγκαταστάσεων που χρησιμοποιούνται στο διεθνές εμπόριο.

Οι υπόψιν διατάξεις της SOLAS εφαρμόζονται από 1η Ιουλίου 2004 σε Φ/Γ πλοία διεθνών πλόων άνω των 500 g.t. και σε όλα τα Ε/Γ πλοία διεθνών πλόων, καθώς και στις λιμενικές εγκαταστάσεις που καταπλέουν τα πλοία αυτά. Οι διατάξεις του Μέρους Α' του Κώδικα είναι δεσμευτικές για τους υπόχρεους φορείς ενώ οι διατάξεις του Μέρους Β' του Κώδικα, αποτελούν οδηγίες και κατευθύνσεις για την εφαρμογή του Μέρους Α' οι οποίες όμως δεν είναι δεσμευτικές. Σημειώνεται, ότι με τον Κανονισμό (ΕΚ) 725/2004 από 1η Ιουλίου 2005 κατέστη δεσμευτικό τμήμα του Μέρους Β' του Κώδικα ISPS για τα Κράτη Μέλη και επεκτάθηκε η εφαρμογή του Κώδικα σε λιμενικές εγκαταστάσεις που εξυπηρετούν επιβατικά πλοία εσωτερικών πλόων Κατηγορίας Α (υπό την έννοια του άρθρου 4 της οδηγίας 98/18/ΕΚ του Συμβουλίου της 17ης Μαρτίου 1998), ενώ τα Κράτη Μέλη έπειτα από υποχρεωτική αξιολόγηση του κινδύνου για την ασφάλεια, αποφασίζουν, έως την 1η Ιουλίου 2007 την έκταση στην οποία θα εφαρμόσουν τις διατάξεις του Κανονισμού σε διάφορες άλλες κατηγορίες

πλοίων που εκτελούν εσωτερικούς πλόες πέραν της κατηγορίας Α καθώς και τις λιμενικές εγκαταστάσεις που προσεγγίζουν.
Παράλληλα, έχει επέλθει συμφωνία μεταξύ των ΗΠΑ και της Ευρωπαϊκής Ένωσης αναφορικά με την πρωτοβουλία για την Ασφάλεια διακίνησης των Εμπορευματοκιβωτίων (Container Security Initiative – CSI).
Για την εφαρμογή των νέων κανονισμών και προτύπων ασφαλείας συστάθηκε στο ΥΕΝ η Διεύθυνση Ελέγχου Διαχείρισης της Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ΔΕΔΑΠΛΕ). Ειδικότερα, όσον αφορά τα θέματα λιμένων, η Διεύθυνση αυτή βρίσκεται σε άμεση συνεργασία με τη Διεύθυνση Λιμενικής Πολιτικής της ΓΓΛ&ΛΠ.

Το επίπεδο ετοιμότητας των Ελληνικών λιμένων, σε σχέση με τις απαιτήσεις που προκύπτουν από την εφαρμογή του ISPS Code, ανταποκρίνεται στους σχεδιασμούς και στις στοχεύσεις που έχει θέσει η ηγεσία του ΥΕΝ. Αξίζει δε να σημειωθεί ότι οι Ολυμπιακοί Αγώνες του 2004 έφεραν τους εμπλεκόμενους λιμένες σε υψηλό επίπεδο ετοιμότητας, με αποτέλεσμα τα μέτρα που λαμβάνονται να κρίνονται ως ισοδύναμου αποτελέσματος (σύμφωνα με Κανονισμό 12 Κεφ. XI-2 ISPS Code) και σε πολλές περιπτώσεις να υπερβαίνουν τις απαιτήσεις του Κώδικα. Πιο συγκεκριμένα, για την αντιμετώπιση συμβάντων που θέτουν σε κίνδυνο την ασφάλεια των Ελληνικών λιμένων και των πλοίων που ελλιμενίζονται εκεί, οι Λιμενικές αρχές εφαρμόζουν μέτρα ασφαλείας του επιπέδου ένα (1) με την συνεχή λήψη προληπτικών μέτρων (εφαρμογή των υπαρχόντων σχεδίων λιμένων, έλεγχος στις πύλες πρόσβασης, ενίσχυση φωτισμού, περιπολίες, κλπ.), φροντίζοντας τα μέτρα και οι διαδικασίες ασφαλείας να εφαρμόζονται με την ελάχιστη δυνατή παρέμβαση σε επιβάτες, πλοία, ναυτικούς, εργαζόμενους και με τη μικρότερη δυνατή καθυστέρηση.

Από 1η Ιουλίου 2004, η Χώρα μας ανακοίνωσε στο Διεθνή Ναυτιλιακό Οργανισμό κατάλογο των λιμένων που είναι υπόχρεοι στην εφαρμογή του Κώδικα, των λιμένων που λαμβάνουν ισοδύναμα μέτρα και των πιστοποιημένων λιμένων.
Η εφαρμογή των νέων προτύπων ασφαλείας στους λιμένες και η συντήρηση του εξοπλισμού συνεπάγεται υψηλό οικονομικό κόστος, γεγονός που επιβάλλει στη ΓΓΛ&ΛΠ την ορθολογική διαχείριση των διαθέσιμων πόρων και την λήψη νέων μέτρων. Η ΓΓΛ&ΛΠ καταβάλλει συστηματικές προσπάθειες, έτσι ώστε τα Λιμενικά Ταμεία που εμπίπτουν στο πεδίο εφαρμογής του Κώδικα να μπορέσουν να ανταποκριθούν στις υποχρεώσεις που συνεπάγεται η εφαρμογή του. Αξίζει να σημειωθεί ότι έχει ήδη εξασφαλιστεί χρηματοδότηση από κρατικούς πόρους για την εκπόνηση των Αξιολογήσεων Ασφάλειας Λιμενικών εγκαταστάσεων και των Σχεδίων Ασφάλειας Λιμένα, ενώ για την πραγματοποίηση έργων, αλλά και για τη συντήρηση του συστήματος ασφάλειας, ο υφιστάμενος σχεδιασμός προβλέπει παρεμβάσεις, οι οποίες θα αντιμετωπίζουν το πρόβλημα, τόσο συνολικά όσο και κατά περίπτωση. Συγκεκριμένα, το ΥΕΝ προχώρησε στις απαιτούμενες διαδικασίες για την εκπόνηση μελετών Αξιολόγησης και Σχεδίων Ασφάλειας

Λιμενικών Εγκαταστάσεων (ΑΑΛΕ και ΣΑΛΕ), και με μέριμνα της ΓΓΛ&ΛΠ, ήδη οι Οργανισμοί Λιμένα Α.Ε. βρίσκονται στο τελικό στάδιο εκπόνησης των Σχεδίων Ασφάλειας Λιμένα.

Παράλληλα, μέχρι σήμερα περισσότερες από 65 ιδιωτικές λιμενικές εγκαταστάσεις έχουν υποβάλλει Μελέτες Αξιολόγησης και Σχέδια Ασφάλειας Λιμενικής Εγκατάστασης στην αρμόδια διεύθυνση του ΥΕΝ (ΔΕΔΑΠΛΕ) και έχει κριθεί ότι έχουν εκπονηθεί σε συμφωνία με τη SOLAS Κεφάλαιο XI-2 και τον Κώδικα ISPS Μέρος Α, λαμβανομένου υπόψη των σχετικών απαιτήσεων του Μέρους Β.

Επιπρόσθετα, προωθείται η δημιουργία Ειδικού Λογαριασμού στη ΓΓΛ&ΛΠ, με σκοπό την εξασφάλιση πόρων, οι οποίοι θα διατίθενται αποκλειστικά για την λειτουργία και τη βελτίωση των συστημάτων ασφάλειας των λιμενικών εγκαταστάσεων.
Θα πρέπει να τονιστεί, επίσης, ότι εκπονήθηκε Εθνικό Σχέδιο Ασφάλειας των Λιμένων με στόχο την διαρκή μέριμνα για την ασφάλεια των θαλάσσιων μεταφορών και του περιβάλλοντος από κάθε απειλή διάπραξης έκνομων ενεργειών έπειτα από σύσταση Διυπουργικής Επιτροπής. Στην επιτροπή συμμετείχαν εκπρόσωποι των Υπουργείων Εμπορικής Ναυτιλίας, Οικονομίας & Οικονομικών, Δημόσιας Τάξης, Τουριστικής Ανάπτυξης και Αγροτικής Ανάπτυξης & Τροφίμων. Το Σχέδιο αυτό πρόκειται να επεκταθεί ώστε να καλύπτει και τις ανάγκες των υπόχρεων πλοίων (κατ' εφαρμογή του άρθρου 9 § 3 του Κανονισμού 725/2004).
Τέλος, σημειώνεται ότι η εφαρμογή του Κώδικα επηρεάζει ποικίλες οικονομικές και κοινωνικές δραστηριότητες που συνδέονται με τη λιμενική λειτουργία. Η ΓΓΛ&ΛΠ αναγνωρίζει τις δυσκολίες που δημιουργούνται από την εφαρμογή του Κώδικα και επιδιώκει λύσεις, οι οποίες θα αντιμετωπίζουν τα προβλήματα κατά περίπτωση και θα περιορίζουν τις αρνητικές συνέπειες από την εφαρμογή των νέων μέτρων.
Σημαντικά βήματα προς την κατεύθυνση εφαρμογής των νέων προτύπων και κανονισμών ασφαλείας στους ελληνικούς λιμένες πραγματοποιούνται σε καθημερινή βάση με δεδομένες και τις συνεχείς νομοθετικές εξελίξεις σε διεθνές επίπεδο. Θα πρέπει να καταβληθούν συνεχείς προσπάθειες από όλους τους εμπλεκόμενους φορείς προκειμένου να εξασφαλισθεί η πλήρης συμμόρφωση της χώρας μας στο νέο διεθνές νομοθετικό πλαίσιο. Η Γενική Γραμματεία Λιμένων και Λιμενικής Πολιτικής αναγνωρίζει τις δυσκολίες που δημιουργούνται από την εφαρμογή του Κώδικα και επιδιώκει λύσεις, οι οποίες θα αντιμετωπίζουν τα προβλήματα κατά περίπτωση και θα περιορίζουν τις αρνητικές συνέπειες από την εφαρμογή των νέων μέτρων.

Πρωταρχική σημασία για την αντιμετώπιση και επίλυση των προβλημάτων ασφάλειας (security) έχει η αναγνώριση των πραγματικών απαιτήσεων ασφάλειας που παρουσιάζονται, απο τον οργανισμό. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό [0]:

- Η αποτίμηση των κινδύνων (risk assessment) που αντιμετωπίζει ο οργανισμός: Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τον οργανισμό, υπολογίζεται η ευπάθεια του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους και το κόστος που θα έχουν για τον οργανισμό.

- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία του.

Ένας αριθμός απαιτήσεων ελέγχου και προστασίας θεωρούνται θεμελιώδεις για την ασφάλεια πληροφοριών σε κάθε οργανισμό. Αυτές, είτε βασίζονται σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική σε θέματα ασφάλειας. Απαιτήσεις απαραίτητες σε έναν οργανισμό, που βασίζονται στη νομοθεσία, είναι η διαφύλαξη των προσωπικών δεδομένων, η διαφύλαξη των δεδομένων του οργανισμού και τα δικαιώματα πνευματικής ιδιοκτησίας. Απαιτήσεις που έχουν καθιερωθεί ως κοινή πρακτική είναι η εκπόνηση πολιτικής ασφάλειας, ο καταμερισμός καθηκόντων σχετικών με την ασφάλεια, η εκπαίδευση σε θέματα ασφάλειας, η αναφορά συμβάντων και η διαχείριση της επιχειρησιακής συνέχειας.

1.2 Βασικές έννοιες

Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες (CIA) [13]

Εμπιστευτικότητα (Confidentiality)
Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Ακεραιότητα (Integrity)
Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Διαθεσιμότητα (Availability)
Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Σε περίπτωση που μία επιχείρηση ή ένας οργανισμός επιθυμεί να καταγράψει και αντιμετωπίσει τα προβλήματα ασφάλειας που υπάρχουν, μπορεί να ακολουθήσει διάφορες στρατηγικές [0].

Αν η επιχείρηση είναι μικρής κλίμακας, μπορεί να εφαρμόσει κατευθείαν τη βασική προσέγγιση (baseline approach), στα πλαίσια της οποίας επιλέγονται απευθείας βασικά μέτρα προστασίας, τα οποία είναι ευρέως γνωστά από υπάρχοντες κώδικες ακολουθητέας πρακτικής σε διεθνές επίπεδο.

Αν η επιχείρηση είναι μεγαλύτερη και τα πληροφοριακά συστήματα έχουν ιδιαίτερη σημασία για τη λειτουργία της, για την αποτελεσματική και ολοκληρωμένη καταγραφή των προβλημάτων ασφάλειας που δυνητικά αντιμετωπίζει, ως επαρκέστερη επιστημονικά μέθοδος προτείνεται η εκπόνηση λεπτομερούς μελέτης ανάλυσης και διαχείρισης επικινδυνότητας (detailed risk analysis and management review) με χρήση πρότυπης αυτοματοποιημένης μεθοδολογίας, από έμπειρους μελετητές. Στα πλαίσια της μελέτης αυτής, αρχικά καταγράφονται λεπτομερώς και αποτιμώνται συγκριτικά τα αγαθά (assets) που περιλαμβάνονται στο πληροφοριακό σύστημα, μελετώνται διεξοδικά οι απειλές (threats) που υφίσταται το σύστημα και τα σημεία ευπάθειας που αυτό

παρουσιάζει (vulnerabilities) και ακολούθως υπολογίζεται ο βαθμός επικινδυνότητας (risk factor) του συστήματος. Τελικά, αναπτύσσεται ένα ολοκληρωμένο σχέδιο ασφάλειας (Security Plan) για τον οργανισμό, το οποίο περιλαμβάνει τόσο τα προτεινόμενα αντίμετρα (countermeasures), όσο και την πολιτική ασφάλειας (Security Policy) του οργανισμού.
Τα προτεινόμενα αντίμετρα μπορεί να είναι κυρίως τεχνικά, αλλά και διοικητικά και οργανωτικά.
Η πολιτική ασφάλειας περιγράφει το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο ένας οργανισμός προστατεύει τα πληροφοριακά του συστήματα, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας. Η πολιτική ασφάλειας συντάσσεται λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά του οργανισμού και του τομέα της οικονομίας στον οποίο δραστηριοποιείται, βασίζεται στα αποτελέσματα της μελέτης ανάλυσης επικινδυνότητας, καθώς και στις βασικές διαστάσεις των στρατηγικών κατευθύνσεων του οργανισμού, σε σχέση με την αξιοποίηση των τεχνολογιών Πληροφορικής και Επικοινωνιών. Αξίζει να σημειωθεί, ότι η πολιτική ασφάλειας αποτελεί υπηρεσιακό κείμενο και θα πρέπει να λαμβάνεται μέριμνα, ώστε όλα τα μέλη του προσωπικού που έχουν ρόλο στη λειτουργία των συστημάτων, είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.

Αναλυτικότερα κατά την ανάλυση κινδύνων συναντάμε τις παρακάτω έννοιες

Στοιχείο (Asset)
ένα στοιχείο περιουσίας που ανήκει σε ένα πρόσωπο ή σε μια εταιρεία , θεωρείται ότι έχει αξία

Αδυναμία (vulnerability)
Βαθμός στον οποίο οι άνθρωποι, η ιδιοκτησία , οι πόροι , τα συστήματα, η πολιτιστική , οικονομική , περιβαλλοντική και κοινωνική δραστηριότητα είναι επιρρεπείς σε βλάβες (υποβάθμιση ή καταστροφή) όταν εκτίθενται σε ένα εχθρικό παράγοντα

Απειλή (Threat)
Οντότητα που μπορεί να προκαλέσει ζημιά ή παραβίαση σε τμήμα ή στο σύνολο του δικτύου

Επίθεση (Attack)
Είναι η εκμετάλλευση μιας αδυναμίας (vulnerability) από εισβολέα για την πραγματοποίηση απειλής

Αντίμετρα (Countermeasures)
Μηχανισμός ή διαδικασία με στόχο τον περιορισμό ή την εξάλειψη επιπτώσεων απειλής

1.3 **Το φυσικό περιβάλλον** (Λιμενικές εγκαταστάσεις – αρχιτεκτονική λιμένα)

Με βάση τον εξοπλισμό, τις εγκαταστάσεις και την εξέλιξη των δραστηριοτήτων τους τα λιμάνια χωρίζονται σε τρεις βασικές κατηγορίες [8]:

- **Το λιμάνι πρώτης γενιάς**. Λιμάνια που αποτελούν απλά πρόσβαση στην ξηρά από την θάλασσα, κύρια δραστηριότητα των οποίων είναι η φορτοεκφόρτωση γενικών φορτίων. Οργανωτικά και διοικητικά το λιμάνι αποτελεί μία μεμονωμένη οντότητα και οι εμπλεκόμενοι φορείς δεν συνεργάζονται μεταξύ τους.

- **Το λιμάνι δεύτερης γενιάς**. Αποτελούν κέντρα μεταφορικών και εμπορικών δραστηριοτήτων, παρέχουν διάφορες υπηρεσίες στους χρήστες, περιέχουν βιομηχανικές εγκαταστάσεις και σε αντίθεση με τα λιμάνια πρώτης γενιάς βρίσκονται σε συνεργασία με τους εμπορικούς συνεργάτες τους και τους δήμους στους οποίους ανήκουν.

- **Το λιμάνι τρίτης γενιάς**. Τα λιμάνια αυτά είναι δυναμικοί επιχειρηματικοί και μεταφορικοί κόμβοι και σημαντικά σημεία logistics για το παγκόσμιο δίκτυο παραγωγής και κατανάλωσης και η διοίκησή τους αναλαμβάνει ενεργό ρόλο στο παγκόσμιο εμπόριο. Πέρα από τις παραδοσιακές λιμενικές υπηρεσίες, προσφέρουν βιομηχανικές και περιβαλλοντικές υπηρεσίες, διοικητικές και εμπορικές υπηρεσίες (διεκπεραίωση εγγράφων, οργάνωση και προγραμματισμός εργασίας) και υπηρεσίες διανομής.

1.4 Αρχιτεκτονική του ΤΠΕ περιβάλλοντος ενός λιμένα

Σε αυτήν την παράγραφο θα δοθεί μία επισκόπηση στο πως είναι οργανωμένη η αρχιτεκτονική του ΤΠΕ περιβάλλοντος ενός εμπορικού λιμένα. Ένα λιμενικό σύστημα ΤΠΕ μπορεί να οργανωθεί στα πέντε επίπεδα που φαίνονται στην εικόνα παρακάτω, και τα οποία περιγράφονται αναλυτικά στη συνέχεια.

ΤΠΕ Αρχιτεκτονική Εμπορικού Λιμένα

– Φυσική υποδομή

Το κατώτερο επίπεδο αφορά τις φυσικές οντότητες του ΤΠΕ περιβάλλοντος, και περιλαμβάνει κτιριακές εγκαταστάσεις, κέντρα δεδομένων, αποθήκευση δεδομένων, δωμάτια των server, καλωδιώσεις, δίκτυα (ασύρματα δίκτυα, LAN δίκτυα, δίκτυα οπτικών ινών), διακομιστές, δρομολογητές, δορυφορικά και πληροφοριακά συστήματα, σταθμοί αναμετάδοσης κτλ.

– Εξοπλισμός ΤΠ / Λογισμικό

Το δεύτερο επίπεδο συγκεντρώνει τον απαραίτητο εξοπλισμό λειτουργίας των λιμενικών ΤΠΕ συστημάτων, από τα κλασσικά δομικά στοιχεία ενός τηλεπικοινωνιακού δικτύου μέχρι τον εξειδικευμένο για τις λιμενικές δραστηριότητες εξοπλισμό και το αντίστοιχο λογισμικό. Βασικά παραδείγματα αυτών είναι κεντρικοί υπολογιστές - εξυπηρετητές, λειτουργικά συστήματα, τερματικά, κάμερες ασφαλείας, ραντάρ, αισθητήρες sonar, συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID), συστήματα SCADA, (Supervisory Control and Data Acquisition), διάφορα ηλεκτρονικά συστήματα όπως ECDIS (Electronic Chart Display and Information System), RCDS (Raster Chart Display System), ECS (Electronic Chart System), VTS (Vessel Traffic Services), AIS (Automatic Identification System), λειτουργικά συστήματα λιμενικών τερματικών (Terminal Operating Systems), βιομηχανικά συστήματα ελέγχου (Industrial control Systems), συστήματα επιχειρηματικής δραστηριότητας (Business Operation Systems), συστήματα παρακολούθησης και ελέγχου πρόσβασης, συστήματα διαχείρισης της εφοδιαστικής αλυσίδας (Logistics Management Systems) και άλλα πολλά.

– Ηλεκτρονικές Υπηρεσίες

Στο επίπεδο αυτό συγκεντρώνονται οι υπηρεσίες που προσφέρει ένα τέτοιο σύστημα οι βασικότερες των οποίων είναι:

- ✓ Υπηρεσίες διαχείρισης πλοίων.
- ✓ Υπηρεσίες διαχείρισης φορτίου.
- ✓ Χερσαίες υπηρεσίες Logistics.
- ✓ Υπηρεσίες διαχείρισης και ελέγχου εξοπλισμού.
- ✓ Υπηρεσίες επικοινωνίας.
- ✓ Ενοποιημένες υπηρεσίες για συνεργασία με τελωνεία, αστυνομικές αρχές κτλ.
- ✓ Εντοπισμός και διαχείριση επικίνδυνων υλικών.
- ✓ Υπηρεσίες διαχείρισης Σειράς Εργασιών.
- ✓ Αυτοματοποιημένη τιμολόγηση.
- ✓ Υπηρεσίες ηλεκτρονικής ανταλλαγής δεδομένων (EDI).
- ✓ Υπηρεσίες Web

– Δεδομένα

Το επίπεδο αυτό αφορά την ροή και αποθήκευση δεδομένων και εξασφαλίζει την μεταφορά τους. Τα δεδομένα που διαχειρίζεται είναι ποικίλα ναυτιλιακά δεδομένα, παράκτια δεδομένα, δεδομένα για την κίνηση πλοίων, δεδομένα επικίνδυνου φορτίου και δεδομένα ασφάλειας.

– Χρήστες

Χρήστες του συστήματος είναι όλοι όσοι αλληλεπιδρούν με αυτό, όπως επιβάτες, πλήρωμα, χειριστές, προσωπικό εκτός του σκάφους, σκάφη, τελωνεία, επιχειρήσεις, εμπορικοί φορείς, λιμενικές αρχές, τράπεζες, υπουργεία και άλλες κρίσιμες υποδομές (π.χ. σιδηρόδρομοι, αεροδρόμια).

Το πληροφοριακό σύστημα ενός εμπορικού λιμένα είναι ασφαλές όταν κάθε ένα από τα παραπάνω επίπεδα ικανοποιούν όλες τις διαστάσεις ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και αυθεντικοποίηση κατά τον έλεγχο πρόσβασης). Τα υφιστάμενα πρότυπα και κανόνες ασφάλειας για την ναυτιλία και τα υπάρχοντα εργαλεία και μεθοδολογίες ασφάλειας επικεντρώνονται στην φυσική ασφάλεια χωρίς να λαμβάνουν υπόψη την ψηφιακή διάσταση των σύγχρονων εμπορικών λιμένων. Στην επόμενη ενότητα, αναλύεται με βάση όλα τα παραπάνω το φυσικό και ψηφιακό περιβάλλον του εμπορικού λιμένα της Μυκόνου.

1.5 Τι είναι σχέδιο επιχειρησιακής συνέχειας;

Το «σχέδιο επιχειρησιακής συνέχειας» (“business continuity plan”) ενός οργανισμού αποτελεί ένα λεπτομερή οδηγό τόσο για την αντιμετώπιση εκτάκτων περιστατικών που θέτουν σε κίνδυνο την εύρυθμη λειτουργία ενός οργανισμού, όσο και για την ανάκαμψη (recovery) συστημάτων έπειτα από οποιαδήποτε ζημία ή καταστροφή.
Σκοπός της εκπόνησης ενός Σχεδίου Επιχειρησιακής Συνέχειας, είναι η αποτροπή εμποδίων στις επιχειρηματικές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών στα συστήματα του. Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού (business continuity management process) θα πρέπει να αξιοποιείται για τη μείωση, σε ανεκτό επίπεδο, των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την ασφάλεια του οργανισμού. Τέτοιες καταστροφές μπορεί να είναι αποτέλεσμα φυσικών καταστροφών, αστοχίας υλικών ή σκόπιμων ενεργειών. Επιπλέον θα πρέπει να περιλαμβάνονται και μέτρα για την αποκατάσταση της ομαλής λειτουργίας του οργανισμού. Ο σχεδιασμός για την αντιμετώπιση απρόοπτων γεγονότων θα πρέπει να εξασφαλίζει την αποκατάσταση των επηρεαζόμενων λειτουργιών μέσα σε ένα ρεαλιστικό και αποδεκτό χρονικό πλαίσιο.[0]

Κεφάλαιο 2

2.1 Λιμενικές εγκαταστάσεις και εφαρμογή του Κώδικα ISPS

Σχεδόν 10 χρόνια μετά την υιοθέτηση του Κώδικα ISM (Διεθνής Κώδικας Ασφαλούς Διαχείρισης Πλοίων) ένας νέος, υποχρεωτικός Κώδικας δημιουργεί νέες απαιτήσεις για τη ναυτιλία προκαλώντας μεγάλες συζητήσεις και ερωτηματικά για το νέο πλαίσιο λειτουργίας των ποντοπόρων πλοίων.
Ο Διεθνής Κώδικας ISPS (Διεθνής Κώδικας για την Ασφάλεια των Πλοίων και Λιμενικών Εγκαταστάσεων από έκνομες ενέργειες – International Ship and Port Facility Security Code) χτύπησε την πόρτα της ναυτιλιακής βιομηχανίας το Δεκέμβριο του 2002 σχεδόν 10 ολόκληρα χρόνια μετά την υιοθέτηση του Κώδικα ISM (ως Απόφαση της Ολομέλειας του IMO και ως νέο Κεφάλαιο στη Διεθνή Σύμβαση SOLAS).
Τότε πολλοί εκπρόσωποι της ναυτιλίας αντιμετώπισαν με σκεπτικισμό τη μονομερή εφαρμογή μέτρων από τα πλοία, που σκόπευαν στη δημιουργία ενός μοντέλου λειτουργίας των ναυτιλιακών εταιρειών, με απώτερο στόχο την ασφάλεια και την προστασία του περιβάλλοντος, τη στιγμή που η γνωστή αλυσίδα της ευρύτερης ναυτιλίας περιλαμβάνει τα λιμάνια, τους τερματικούς σταθμούς, τους νηογνώμονες, τα ναυπηγεία, τους προμηθευτές καυσίμων, τους κατασκευαστές ναυτικού τύπου εξοπλισμού, τα P & I Clubs κλπ, όλους δηλαδή αυτούς που επηρεάζουν με κάποιο τρόπο την ασφαλή λειτουργία των πλοίων.

Από τους κρίκους εκείνους της αλυσίδας που δέχθηκαν επικρίσεις για τη μη εφαρμογή ενός παρόμοιου μοντέλου λειτουργίας ήταν τα λιμάνια, η λειτουργία, ο εξοπλισμός και η συντήρηση των οποίων συνδέεται άμεσα με την ασφάλεια της ναυσιπλοΐας και την προστασία του περιβάλλοντος στην ευρύτερη περιοχή δικαιοδοσίας τους. Η απαίτηση για την προέκταση ενός ανάλογου Κώδικα ISM στους φορείς διαχείρισης λιμένων θεωρήθηκε άστοχη αφού το ζητούμενο εκείνη την εποχή ήταν η βελτίωση της λειτουργίας των πλοίων ιδιαίτερα μετά τα τις τραγωδίες του Estonia, του Herald of Free Enterprise κ.α.
Ο νέος Κώδικας ISPS όμως που υιοθετήθηκε στις 12 Δεκεμβρίου 2002 (ένα χρόνο μόλις μετά τις τρομοκρατικές επιθέσεις στις Η.Π.Α.) έχει ως πεδίο εφαρμογής όχι μόνο τα φορτηγά πλοία διεθνών πλόων άνω των 500 κοχ. και όλα τα επιβατηγά πλοία επίσης διεθνών πλόων, αλλά και τις λιμενικές εγκαταστάσεις στις οποίες καταπλέουν τα παραπάνω πλοία. Ο Κώδικας, προϊόν πολιτικής συναίνεσης των κρατών μελών που συμμετέχουν στις εργασίες του Διεθνούς Ναυτιλιακού Οργανισμού, συμπεριλήφθηκε στις τροποποιήσεις του Κεφαλαίου XI της SOLAS ώστε να καταστεί υποχρεωτικός και αποτελεί πλέον ένα νέο πλαίσιο για την αναγνώριση και διαχείριση απειλών κατά της ασφάλειας πλοίων και λιμανιών με στόχο τον περιορισμό του κινδύνου και των πιθανών επιπτώσεων.
Από πλευράς λιμενικών εγκαταστάσεων οι βασικές υποχρεώσεις των φορέων διαχείρισής τους είναι οι εξής:

- **Η διενέργεια αξιολόγησης ασφάλειας** της εγκατάστασης (ΑΑΛΕ) σύμφωνα με τους όρους που θέτει ο Κώδικας ISPS, με αντικειμενικό στόχο τον προσδιορισμό των πιθανών απειλών και των ευαίσθητων σημείων στα οποία ο λιμένας είναι ευάλωτος αλλά και την ανεύρεση τρόπων και μεθόδων εξάλειψης αυτών των αδυναμιών.
Ουσιαστικά πρόκειται για μια μελέτη εκτίμησης των μέτρων και του κόστους υλοποίησης αυτών για την εφαρμογή των διατάξεων του Κώδικα στη βάση των ιδιαιτεροτήτων θέσης και λειτουργίας των λιμενικών εγκαταστάσεων. Η παραπάνω Αξιολόγηση γίνεται από αναγνωρισμένους από την Αρχή του κράτους (Υπουργείο Εμπορικής Ναυτιλίας για τα λιμάνια της χώρας μας) Οργανισμούς Ασφαλείας (ΑΟΑ) οι οποίοι βέβαια πρέπει να πληρούν συγκεκριμένους όρους και προϋποθέσεις που αναφέρονται λεπτομερώς στον Κώδικα. Το τελευταίο χρονικό διάστημα, αιχμές κυρίως από τον περιοδικό τύπο του εξωτερικού εξαπολύθηκαν για την καθυστέρηση της συμμόρφωσης των Ολυμπιακών λιμανιών της χώρας μας, ωστόσο η προπαρασκευή των λιμανιών αυτών έχει ξεκινήσει αρκετά νωρίτερα αφού εκτιμάται ότι στην ουσία αξιοποιείται ο εκπονημένος σχεδιασμός θωράκισης της ασφάλειάς τους κατά τη διάρκεια των Ολυμπιακών Αγώνων.
Οι πιθανές απειλές στις ζωτικές λειτουργίες μιας λιμενικής εγκατάστασης που πρέπει να αξιολογηθούν περιλαμβάνουν για παράδειγμα δολιοφθορές, τοποθέτηση βόμβας, λαθρεμπόριο, κλπ. Η μελέτη που γίνεται δεν έχει στατικό χαρακτήρα αλλά πρέπει να γίνεται περιοδικά λαμβάνοντας υπόψη τυχόν αλλαγές στην υποδομή και τη λειτουργία της εγκατάστασης και συνεκτιμώντας τα τυχόν, διαθέσιμα μέτρα ασφαλείας ή τον εγκατεστημένο εξοπλισμό ελέγχου και παρακολούθησης, το σχεδιασμό κατάσβεσης πυρκαγιάς, αντιμετώπισης περιστατικού ρύπανσης της θάλασσας, το σχεδιασμό παραλαβής και διαχείρισης των αποβλήτων των πλοίων κλπ.

- **Η κατάρτιση σχεδίου ασφάλειας** Λιμενικής Εγκατάστασης, με βάση την Αξιολόγηση Ασφαλείας το οποίο καλύπτει αποτελεσματικά τη διασύνδεση πλοίου/λιμένα (ship – port interface), προβλέποντας τρία επίπεδα ασφαλείας.
Τα όρια της λιμενικής εγκατάστασης επεκτείνονται από τη διεπαφή πλοίου – λιμένα μέχρι μια νοητή περίμετρο ασφαλείας που περιλαμβάνει τις περιοχές εκείνες στις οποίες λαμβάνει χώρα ο χειρισμός, στοιβασία και η αποθήκευση φορτίου, τις ζώνες περιορισμένης πρόσβασης και τις ζώνες όπου γίνεται η αποβίβαση/επιβίβαση επιβατών. Οι ζώνες περιορισμένης πρόσβασης αποτελούν τις περιοχές εκείνες μιας εγκατάστασης που προσδιορίζονται από τον διαχειριστή της ως ουσιαστικές για την ασφάλεια των λειτουργιών, του ελέγχου, των εργασιών χειρισμού φορτίου όπως για παράδειγμα τα κέντρα επικοινωνιών, τα αντλιοστάσια, οι δεξαμενές και το δίκτυο σωληνώσεων που τις εξυπηρετεί, οι χώροι αποθήκευσης επικίνδυνων φορτίων, οι χώροι παρακολούθησης κλειστών συστημάτων, κ.α.
Το επίπεδο ασφάλειας 1 είναι το επίπεδο για το οποίο τηρούνται πάντα και συστηματικά τα ελάχιστα μέτρα προστασίας και ετοιμότητας, το επίπεδο 2

χαρακτηρίζει πρόσθετα, κατάλληλα μέτρα ασφάλειας τα οποία διατηρούνται για μια χρονική περίοδο ως αποτέλεσμα ενός αυξημένου κινδύνου και το 3 σημαίνει πρακτικά το επίπεδο εκείνο για το οποίο τα περαιτέρω μέτρα θα διατηρηθούν για μια περιορισμένη χρονικά περίοδο όταν ένα γεγονός ασφάλειας των μεταφορών είναι πιθανό και επικείμενο.
Το σχέδιο προβλέπει όχι μόνο τον τρόπο αντιμετώπισης ενός περιστατικού που δύναται να θέσει σε κίνδυνο την εγκατάσταση και το πλοίο που είναι ελλιμενισμένο σε αυτή, αλλά συγχρόνως οργανώνει το μηχανισμό πρόληψης προσδιορίζοντας τους αναγκαίους πόρους, ανθρώπινο δυναμικό και μέσα για τον έλεγχο και επιτήρηση των ζωνών περιορισμένης πρόσβασης και γενικά όλα τα κρίσιμα σημεία της εγκατάστασης, Πρέπει επίσης να περιλαμβάνει τουλάχιστον:

- Μέτρα ή/και εξοπλισμό αποφυγής μη εξουσιοδοτημένης μεταφοράς επικίνδυνων ουσιών, όπλων και συσκευών που προορίζονται για χρήση ενάντια σε ανθρώπους, πλοία και εγκαταστάσεις,

- Διαδικασίες ανταπόκρισης στις απειλές ασφάλειας, εκκένωσης σε περίπτωση απειλών ή παραβιάσεων της ασφάλειας

- Διαδικασίες αναφοράς έκνομων γεγονότων κατά της ασφάλειας των μεταφορών

- Διαδικασίες εκτέλεσης ενεργειών σε περίπτωση που ενεργοποιείται το σύστημα αναγγελίας ασφάλειας ενός πλοίου που βρίσκεται εντός της λιμενικής εγκατάστασης

- **Διορισμό του Υπεύθυνου Ασφαλείας Λιμενικής Εγκατάστασης**. Ουσιαστικά ορίζεται ένας Υπεύθυνος Ασφαλείας που μπορεί να έχει παράλληλα καθήκοντα και για άλλους ρόλους και εργασίες υπό τον όρο ότι είναι πλήρως ικανός να φέρει σε πέρας το έργο που του έχει ανατεθεί στο πλαίσιο της υλοποίησης του Σχεδίου (προπαρασκευή για τη διενέργεια της αρχικής ή άλλης περιοδικής Αξιολόγησης Ασφάλειας, εξασφάλιση επαρκούς εκπαίδευσης του προσωπικού που έχει ρόλο στην ασφάλεια της εγκατάστασης, υποβολή έκθεσης προς τις υπεύθυνες αρχές και τήρηση στοιχείων που σκιαγραφούν περιστατικά που έθεσαν σε κίνδυνο την εγκατάσταση, κ.α.)
Ο φορέας διαχείρισης ενός τερματικού σταθμού που κείτεται εντός ενός εκτενούς λιμενικού συγκροτήματος δεν απαλλάσσεται της ευθύνης εφαρμογής των διατάξεων του Κώδικα ISPS, αφού ουσιαστικά υποδέχεται και εξυπηρετεί πλοία για τις δικές του ανάγκες (π.χ. εισαγωγή πρώτων υλών, εξαγωγές έτοιμων προϊόντων προς/από το γειτνιάζον εργοστασιακό συγκρότημα, τερματικοί σταθμοί χύδην φορτίων, κ.α.)
Η ικανότητα προσαρμογής ενός φορέα διαχείρισης λιμένα στον οποίο καταπλέουν πλοία SOLAS – όπως λέμε απλά – στο νέο πλαίσιο λειτουργίας που

διαμορφώνεται από τις διεθνείς εξελίξεις για την ασφάλεια, εξαρτάται από πολλούς παράγοντες. Εύκολη προσαρμογή και ωριμότητα μπορεί κανείς να υποθέσει ότι υπάρχει για τα λιμάνια στα οποία γίνεται χειρισμός και αποθήκευση επικίνδυνων φορτίων ή γενικά σε αυτά στα οποία έχουν εκπονηθεί και υλοποιούνται σχέδια αντιμετώπισης τεχνολογικών ατυχημάτων (υπόχρεες εγκαταστάσεις των Οδηγιών Seveso I/II) καθώς και σχέδια αντιμετώπισης περιστατικών ρύπανσης από πετρέλαιο και άλλες υγρές χημικές, επιβλαβείς ουσίες.[2]

2.2 Τι είναι το διεθνές πρότυπο ISO 27001:2005;

Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών
Το ISO/IEC 27001 είναι το μόνο διεθνές πρότυπο που μπορεί να επιθεωρηθεί και το οποίο καθορίζει τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS).
Η πληροφορία είναι αποφασιστικής σημασίας για τη λειτουργία και πιθανόν την επιβίωση ενός οργανισμού. Η πιστοποίηση κατά ISO/IEC 27001 βοηθά έναν οργανισμό να διαχειριστεί και να προστατεύσει τα πολύτιμα περιουσιακά του στοιχεία που περιέχουν πληροφορίες.
Το πρότυπο είναι σχεδιασμένο έτσι ώστε να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά ένα οργανισμό να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη και ιδιαίτερα οι πελάτες του.
Το πρότυπο είναι βασισμένο στη διεργασιακή προσέγγιση για την εδραίωση, εφαρμογή, λειτουργία, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση ενός ΣΔΑΠ.
Το ISO/IEC 27001 είναι κατάλληλο για όλους τους οργανισμούς, μικρούς ή μεγάλους και σε κάθε εργασιακό χώρο. Είναι ιδιαίτερα κατάλληλο για οργανισμούς που η προστασία της πληροφορίας είναι κρίσιμη, όπως σε χρηματοπιστωτικούς οργανισμούς, τηλεπικοινωνίες, υγεία, δημόσιο και πληροφορική.
Το ISO/IEC 27001 είναι επίσης κατάλληλο για εταιρείες που διαχειρίζονται πληροφορίες για λογαριασμό άλλων, όπως εταιρείες παροχής υπηρεσιών πληροφορικής που μπορεί να λειτουργήσει σαν εγγύηση ότι οι πληροφορίες των πελατών τους προστατεύονται.

2.2.1 Οφέλη του ISO/IEC 27001

Η πιστοποίηση ενός ΣΔΑΠ σύμφωνα με τις απαιτήσεις του ISO/IEC 27001 μπορεί να προσφέρει τα παρακάτω οφέλη σε ένα οργανισμό:

– Αποδεικνύει μέσω ενός ανεξάρτητου φορέα ότι οι εσωτερικοί έλεγχοι του οργανισμού πραγματοποιούνται και ικανοποιούν τους εταιρικούς στόχους και στρατηγικές

– Αποδεικνύει ότι οι απαιτήσεις για σωστή διακυβέρνηση και επιχειρησιακή συνέχεια ικανοποιούνται

– Αποδεικνύει ότι η σχετική νομοθεσία και οι τυποποιημένοι κανονισμοί εφαρμόζονται.

– Παρέχει ανταγωνιστικό πλεονέκτημα στην ικανοποίηση συμβατικών υποχρεώσεων και επιδεικνύει στους πελάτες του οργανισμού ότι η ασφάλεια των πληροφοριών τους είναι πρωταρχικής σημασίας για τον οργανισμό

– Αποδεικνύει μέσω ενός ανεξάρτητου φορέα ότι τα οργανωτικά ρίσκα έχουν αναγνωριστεί, αξιολογηθεί και διαχειριστεί ικανοποιητικά και σωστά

– Αναδεικνύει την ύπαρξη ενός επίσημου και λειτουργικού συστήματος διαχείρισης ασφάλειας πληροφοριών

– Αποδεικνύει τη δέσμευση της ανώτατης διοίκησης του οργανισμού στην ασφάλεια των πληροφοριών του

– Αποδεικνύει ότι μέσω τακτικών αξιολογήσεων βοηθά τον οργανισμό να παρακολουθεί την απόδοσή του και να βελτιώνεται

– Αναδεικνύει ότι όλες οι πληροφορίες που αποθηκεύονται, επεξεργάζονται ή επικοινωνούν μέσω των πληροφοριακών συστημάτων έχουν αξία για τον οργανισμό

Το ISO/IEC 27001
χρησιμοποιεί την αξιολόγηση των ρίσκων ώστε να δημιουργηθεί ένα σύστημα διαχείρισης που παρέχει:

Μεγιστοποίηση της διαθεσιμότητας των συστημάτων

Διαβεβαίωση ότι η ακεραιότητα των συστημάτων, των συστημάτων επεξεργασίας και της πληροφορίας συντηρείται

Επιβεβαίωση ότι η εμπιστευτικότητα της πληροφορίας διατηρείται. [4]

Ποια η διαφορά του ISO 27001 & ISO 27002;
Το πρότυπο ISO 27001 είναι μια πιστοποίηση και σε αυτό περιγράφονται οι απαιτήσεις που πρέπει να πληρεί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του. Το πρότυπο ISO 27002 παρέχει τις κατευθυντήριες οδηγίες για την κάλυψη του προτύπου. [5]

2.3 Τι είναι το διεθνές πρότυπο ISO 27001:2013;

Το ISO/IEC 27001:2013 [33] παρέχει και καθορίζει τις απαιτήσεις για την εγκατάσταση, υλοποίηση, διατήρηση και βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών και την αξιολόγηση και επεξεργασία κινδύνων της ασφάλειας πληροφοριών ενός οργανισμού. Οι απαιτήσεις που καθορίζει το διεθνές αυτό πρότυπο μπορούν να εφαρμοστούν σε κάθε οργανισμό. Το πρότυπο μπορεί να χρησιμοποιηθεί από φορείς, εντός ή εκτός του οργανισμού, για την αξιολόγηση της ικανότητας του να καλύψει της απαιτήσεις ασφάλειας του. Το πρότυπο διατηρεί συμβατότητα με τα υπόλοιπα τις ίδιας ομάδας (π. χ. ISO/IEC 27001:2005, ISO/IEC 27002:2005) και περιέχει μία ολοκληρωμένη λίστα αντιμέτρων, συμβατή με αυτήν του ISO/IEC 27001:2005, στην οποία προσθέτει ορισμένους νέους ελέγχους.

2.4 Λοιπή Νομοθεσία και Εγκύκλιοι σχετικά με την Ασφάλεια στην Θάλασσα

Όλες οι δραστηριότητες και οι λειτουργίες σε ένα λιμάνι θα πρέπει να διεξάγονται σύμφωνα με τους ισχύοντες διεθνής, ευρωπαϊκούς και εθνικούς κανονισμούς και τα αντίστοιχα πρότυπα. Παρακάτω παρουσιάζονται μια σειρά από τους βασικούς αυτούς κανονισμούς και πρότυπα.

2.4.1 *Παγκοσμίως*

– Διεθνής Σύμβαση για την Ασφάλεια της ζωής στη θάλασσα (international Convention for the Safety of Life at Sea (SOLAS), 1974)

Η σύμβαση SOLAS είναι η πιο σημαντική από όλες τις σχετικές διεθνείς συνθήκες και καθορίζει την νομική βάση και τις ελάχιστες προδιαγραφές ασφάλειας για την κατασκευή, τον εξοπλισμό και την λειτουργία των εμπορικών και επιβατηγών πλοίων. Η πρώτη έκδοση υιοθετήθηκε το 1914, ως συνέπεια του καταστροφικού ναυαγίου του Τιτανικού. Έκτοτε εφαρμόσθηκαν αρκετές εκδόσεις του με πιο γνωστή αυτή του 1974 η οποία τέθηκε σε εφαρμογή το 1980. Η σύμβαση του 1974 έχει ανανεωθεί και τροποποιηθεί επανειλημμένως [28]. Η σύμβαση είναι ένας από τους σημαντικότερους και παλαιότερους κανονισμούς που θεσπίζει κανόνες ασφαλείας για τις θαλάσσιες δραστηριότητες και αυτός είναι ο λόγος που αναφέρεται σε αυτό το κεφάλαιο παρά το γεγονός ότι τα κεφάλαια της που είναι αφιερωμένα στην μεταφορά των φορτίων, επικίνδυνων εμπορευμάτων και τη διαχείριση ασφαλών λειτουργιών, σχετίζονται με τα πλοία και όχι με τις λιμενικές εγκαταστάσεις ή την διεπαφή πλοίου / λιμένα. Στην SOLAS οι λιμενικές εγκαταστάσεις θεωρούνται χώροι εργασίας, βιομηχανικές περιοχές, περιοχές αποθήκευσης, παραγωγής και διακίνησης και εμπίπτουν στο πεδίο εφαρμογής των γενικών κανόνων και της νομοθεσίας που εκδίδεται από τις χώρες και τους διεθνείς οργανισμούς.

– Κώδικας Πρακτικής για την Ασφάλεια και την Υγεία στους Λιμένες (ILO Code of Practice on Safety and Health in Ports)

Εκδόθηκε το 2005 και καλύπτει όλες τις πτυχές της εργασίας στους λιμένες που αφορούν την φορτοεκφόρτωση αγαθών και επιβατών, την κυκλοφορία των οχημάτων κάθε τύπου, τις δραστηριότητες στην ακτή και εντός των πλοίων, τον φωτισμό, τον ατομικό εξοπλισμό προστασίας, ειδικές προβλέψεις για άτομα με αναπηρία και λεπτομέρειες για τον χειρισμό ορισμένων φορτίων.

– General Conference of the International ILO Convention and Recommendation concerning Occupational Safety and Health in Dock Work, C-152, (1979)

Η συνθήκη τέθηκε σε ισχύ το 1979 και προβλέπει μέτρα σχετικά με τον εξοπλισμό και τη συντήρηση των υποδομών, με στόχο την αύξηση της ασφάλειας και τη μείωση των τραυματισμών. Περιλαμβάνει μέτρα για την ασφαλή πρόσβαση στις

εργασίας και παρέχει, πληροφορίες σχετικές με την ασφάλεια των εργαζομένων όπως η κατάλληλη ένδυση ασφαλείας, ο εξοπλισμός διάσωσης, η προσφορά πρώτων βοηθειών και η αντιμετώπιση περιστατικών ασφαλείας.

– Διεθνής Ναυτιλιακός Κώδικας Στερεών Φορτίων Χύδην (International Maritime Solid Bulk Cargoes Code (IMSBC Code))

Ο κώδικας IMSBC υιοθετήθηκε από την Επιτροπή Ναυτικής Ασφάλειας του IMO το 2008 και αντικαθιστά τον «Κώδικα Ασφαλούς Πρακτικής για Στερεά Φορτία Χύδην (Code of Safe Practice for Solid Bulk Cargoes (BC Code))». Σκοπός του κώδικα είναι να διευκολύνει την ασφαλή στοιβασιά και μεταφορά των στερεών χύδην φορτίων παρέχοντας πληροφορίες για τους κινδύνους που σχετίζονται με την μεταφορά τους καθώς και οδηγίες σχετικές με τις ενδεδειγμένες διαδικασίες που πρέπει να υιοθετηθούν. Στην Ελλάδα ο κώδικας υιοθετήθηκε με το Προεδρικό Διάταγμα υπ' αριθμόν 52 τον Απρίλιο του 2013 (ΠΔ52_2013).

– Διεθνής Κώδικας για την Κατασκευή και τον Εξοπλισμό των Πλοίων που Μεταφέρουν Επικίνδυνα Χημικά Χύδην (International Code for the Construction and Equipment of Ships carrying Dangerous Chemicals in Bulk (IBC Code))

Ο κώδικας IBC, θέτει το διεθνές πρότυπο για την ασφαλή μεταφορά διά θαλάσσης επικίνδυνων και επιβλαβών χύδην υγρών χημικών ουσιών. Ο κώδικας ορίζει το σχεδιασμό και τα πρότυπα κατασκευής των πλοίων και τον αντίστοιχο εξοπλισμό που πρέπει αυτά να φέρουν, λαμβάνοντας δεόντως υπόψη τη φύση των σχετικών προϊόντων που μεταφέρονται [25]. Από το 1985 ο κώδικας έχει επεκταθεί για να καλύπτει θέματα θαλάσσιας ρύπανσης. Στην Ελλάδα ο κώδικας υιοθετήθηκε με το προεδρικό διάταγμα ΠΔ41_1994 (ΦΕΚ 31/Α/10.3.1994).

– Διεθνής Σύμβαση για την Αποφυγή της Ρύπανσης από Πλοία (International Convention for the Prevention of Pollution from Ships (MARPOL))

Η σύμβαση MARPOL υιοθετήθηκε στις 2 Νοεμβρίου 1973 στον IMO, τέθηκε σε εφαρμογή τον Οκτώβριο του 1983 και είναι η κύρια διεθνής σύμβαση που καλύπτει την πρόληψη της ρύπανσης του θαλάσσιου περιβάλλοντος από τα πλοία. Η σύμβαση, η οποία έχει αναβαθμισθεί με διάφορες τροποποιήσεις μέσα στα χρόνια, περιλαμβάνει έξι τεχνικά παραρτήματα τα οποία στοχεύουν στην πρόληψη και την ελαχιστοποίηση της ρύπανσης, ακούσιας ή από συνήθεις λειτουργίες, που μπορεί να προκαλέσει ένα πλοίο [27].

– Διεθνής Σύμβαση για τα Πρότυπα Εκπαίδευσης, Έκδοσης Πιστοποιητικών και Τήρησης Φυλακών των Ναυτικών (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW))

Η Σύμβαση STCW που υιοθετήθηκε το 1978 και τέθηκε σε εφαρμογή το 1984 είναι η πρώτη που θέτει τις βασικές προϋποθέσεις για την εκπαίδευση, την πιστοποίηση και την τήρηση φυλακών των ναυτικών σε διεθνές επίπεδο. Η

σύμβαση ορίζει τις ελάχιστες προδιαγραφές σχετικά με αυτά τα θέματα τις οποίες οι χώρες είναι υποχρεωμένες να πληρούν [19].

– Διεθνής Σύμβαση για τη Ναυτική Έρευνα και Διάσωση (International Convention on Maritime Search and Rescue (SAR))

Στόχος της σύμβασης του 1979, που εγκρίθηκε κατά την διάσκεψη του Αμβούργου ήταν η διεθνής ανάπτυξη ενός σχεδίου έρευνας και διάσωσης, έτσι ώστε, ανεξάρτητα από το πού συμβαίνει ένα ατύχημα, η διάσωση των ανθρώπων που βρίσκονται στην θάλασσα να συντονίζεται από έναν οργανισμό έρευνας και διάσωσης (SAR organisation) ή/και, όταν κρίνεται αναγκαίο, από συνεργαζόμενους τέτοιους οργανισμούς. Μέχρι την έκδοση της σύμβασης SAR, δεν υπήρχε διεθνές σύστημα που να καλύπτει επιχειρήσεις έρευνας και διάσωσης [20].

– Μνημόνιο Συνεννόησης των Παρισίων (Paris Memorandum of Understanding of port state control (Paris MoU))

Το Paris MoU αποτελεί ένα πρωτόκολλο σύμβασης μεταξύ είκοσι επτά διαφορετικών Λιμενικών Αρχών. Υπογράφηκε από 14 Ευρωπαϊκές χώρες τον Ιανουάριο του 1982 στο Παρίσι και τέθηκε σε εφαρμογή τον Ιούλιο του ίδιου έτους. Το μνημόνιο καλύπτει την ασφάλεια της ζωής στη θάλασσα, την πρόληψη της ρύπανσης από τα πλοία και τις συνθήκες διαβίωσης και εργασίας επί των πλοίων. Το Paris MoU έχει τροποποιηθεί αρκετές φορές ώστε να ανταποκριθεί στις εκάστοτε απαιτήσεις ασφαλείας που θέτει ο IMO [21].

2.4.2 *Ευρώπη*

– Κανονισμός (ΕΚ) αριθ.725/2004 Του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαρτίου 2004 για την ενίσχυση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (Regulation 725/2004/EC).

Ο κύριος στόχος του κανονισμού είναι η θέσπιση και εφαρμογή μέτρων που αποσκοπούν στη βελτίωση της ασφάλειας στα πλοία που εκτελούν διεθνή δρομολόγια και στην διεθνή θαλάσσια κυκλοφορία, συμπεριλαμβανομένων των σχετικών λιμενικών εγκαταστάσεων [22]. Ωστόσο, ο κανονισμός περιλαμβάνει διατάξεις που επεκτείνουν τα μέτρα αυτά και σε πλοία που εκτελούν εθνικά δρομολόγια εντός της ΕΕ, καθώς και τις συναφείς λιμενικές εγκαταστάσεις που εξυπηρετούν τα πλοία αυτά. Ο κανονισμός παρέχει τη βάση για την εναρμονισμένη ερμηνεία και εφαρμογή, των ειδικών μέτρων για την ενίσχυση της ασφάλειας στη θάλασσα, που εγκρίθηκαν από τον IMO το 2002 ως τροποποίηση της σύμβασης SOLAS, 1974 και την εφαρμογή του κώδικα ISPS. Ο κανονισμός καθιστά υποχρεωτική μια σειρά συστάσεων του μέρους Β του κώδικα ISPS [23].

– Οδηγία 2005/65/ΕΚ σχετικά με την ενίσχυση της ασφάλειας των λιμένων (Directive 2005/65/EC)

Η οδηγία συμπληρώνει τα μέτρα ασφάλειας που θεσπίστηκαν από τον παραπάνω κανονισμό (ΕΚ/725/2004) θέτοντας έναν ολόκληρο λιμένα σε ένα καθεστώς ασφαλείας. Προκειμένου να επιτευχθεί η μέγιστη δυνατή προστασία για θαλάσσιες και λιμενικές δραστηριότητες, πρέπει να ληφθούν μέτρα που να καλύπτουν όλους τους λιμένες σε περίμετρο που ορίζεται από το εν λόγω κράτος μέλος. Τα μέτρα αυτά πρέπει να εφαρμόζονται σε όλους τους λιμένες και τις λιμενικές εγκαταστάσεις που εμπίπτουν στο πλαίσιο του κανονισμού. Η οδηγία προβλέπει επίσης μηχανισμούς για την εφαρμογή αυτών των μέτρων και τον έλεγχο της συμμόρφωσης προς αυτούς.

– Οδηγία 2010/65/ΕΕ (Directive 2010/65/EU)

Η συγκεκριμένη οδηγία αφορά στην απλούστευση και εναρμόνιση των διοικητικών διαδικασιών που εφαρμόζονται στις θαλάσσιες μεταφορές, μέσω της τυποποίησης της ηλεκτρονικής διαβίβασης πληροφοριών και την εξυγίανση των διατυπώσεων υποβολής δηλώσεων. Ορίζει συγκεκριμένα ότι οι πληροφορίες για το φορτίο, το πλήρωμα ή/και τους επιβάτες που μεταδίδονται κατά την άφιξη πλοίων σε ευρωπαϊκά λιμάνια πρέπει να κοινοποιούνται σε ηλεκτρονική μορφή (e-messages) [24] μέσω μιας Ενιαίας θύρας (single window). Ο κανονισμός πρέπει να έχει εκτελεστεί από τα κράτη μέλη μέχρι την 1η Ιουνίου 2015. Αυτή η Ενιαία Θύρα είναι ο μόνος τρόπος όπου όλες οι πληροφορίες θα δηλώνονται και απ' όπου θα διατίθενται στις διάφορες αρμόδιες αρχές και στα άλλα κράτη μέλη.

– Οδηγία 96/98/ΕΚ σχετικά με τον εξοπλισμό των πλοίων (Directive 96/98/EC)

Με αυτήν την ντιρεκτίβα η Ευρωπαϊκή Ένωση (ΕΕ) θεσπίζει πρότυπα για τη διασφάλιση της ασφάλειας και της ποιότητας του θαλάσσιου εξοπλισμού των πλοίων. Τα πρότυπα αυτά συμβάλουν επίσης στην αντιμετώπιση της θαλάσσιας ρύπανσης και στη διασφάλιση της ελεύθερης κυκλοφορίας του θαλάσσιου εξοπλισμού εντός της εσωτερικής αγοράς.

– Κανονισμός (ΕΚ) αριθ. 324/2008 σχετικά με τις διαδικασίες για τη διενέργεια των επιθεωρήσεων της Επιτροπής στο πεδίου της ασφάλειας της ναυσιπλοΐας (Regulation 324/2008/EC)

Προκειμένου να παρακολουθεί την εφαρμογή της Ευρωπαϊκής νομοθεσίας στον τομέα της ασφάλειας στην θάλασσα, η επιτροπή διενεργεί επιθεωρήσεις. Ο κανονισμός αυτός θεσπίζει τις διαδικασίες, για την επιτήρηση, από μέρους της Επιτροπής, της εφαρμογής της ντιρεκτίβας 2005/65/ΕΚ καθώς και για τις επιθεωρήσεις που προβλέπονται για τα πλοία και τις λιμενικές εγκαταστάσεις [25].

2.4.3 *Εθνική*

Παρακάτω αναφέρονται οι σημαντικότεροι νόμοι που ισχύουν στην Ελλάδα, οι οποίοι διευθετούν θέματα ασφαλείας στην θάλασσα και εξασφαλίσουν την ευθυγράμμιση της χώρας με τις διεθνής και ευρωπαϊκές απαιτήσεις σε αυτόν τον τομέα.

– Νόμος 1045/1980 – (ΦΕΚ 95)
Ο νόμος αυτός αποτελεί την πρώτη πράξη κύρωσης της Διεθνούς Σύμβασης Περί Ασφαλείας της Ανθρώπινης Ζωής στη Θάλασσα (ΠΑΑΖΕΘ (SOLAS, 1974)) και εκδόθηκε στις 25 Απριλίου 1980. Έκτοτε έχουν εκδοθεί πολυάριθμοι νόμοι και Προεδρικά Διατάγματα που επικυρώνουν τις διάφορες τροποποιήσεις της ΠΑΑΖΕΘ με τελευταίο το ΠΔ98/2009 – (ΦΕΚ 124) [26].

– Νόμος 3622/2007 – ΦΕΚ 281/Α'/20.12.2007
Στόχος του νόμου αυτού αποτελεί ο καθορισμός των αρμοδιοτήτων, ο σχεδιασμός δράσεων σε εθνικό επίπεδο, καθώς και ο συντονισμός αυτών για τη διασφάλιση της εφαρμογής του Κανονισμού ΕΚ/725/2004 (L129/6 της 29.4.2004) και της Ευρωπαϊκής Οδηγίας 2005/65 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (L130 της 25.11.2005) για την ενίσχυση της ασφάλειας των πλοίων, των λιμενικών εγκαταστάσεων και των λιμένων [18].

– ΠΔ241/2006
Το συγκεκριμένο Προεδρικό Διάταγμα προχωρά στην αποδοχή των τροποποιήσεων της Διεθνούς Σύμβασης «Για πρότυπα εκπαίδευσης, έκδοσης πιστοποιητικών και τήρησης φυλακών των ναυτικών, 1978», η οποία κυρώθηκε με τον ν.1314/1983 (Α'2), όπως αυτή τροποποιήθηκε.

– ΠΔ56/2004
Το Προεδρικό Διάταγμα υπ'αριθ.56 εκδόθηκε την 11η Φεβρουαρίου 2004 και προχωρά στην κύρωση των τροποποιήσεων της «ΠΑΑΖΕΘ, 1974» που υιοθετήθηκαν στην Διάσκεψη των Συμβαλλομένων Κυβερνήσεων της Διεθνούς Σύμβασης την 12η Δεκεμβρίου 2002 [26], εφαρμόζοντας πρακτικά τον ISPS κώδικα για τα ελληνικά πλοία και τις ελληνικές λιμενικές εγκαταστάσεις.

– ΠΔ125/2012
Το διάταγμα αυτό είναι η προσαρμογή της ελληνικής νομοθεσίας στις διατάξεις της Οδηγίας 2010/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις διατυπώσεις υποβολής δηλώσεων για τα πλοία κατά τον κατάπλου ή/και απόπλου από τους λιμένες των κρατών μελών.

– ΠΔ347/1998

Το διάταγμα αυτό είναι η προσαρμογή της ελληνικής νομοθεσίας για την αποδοχή των διατάξεων της οδηγίας 96/98/ΕΚ της Κομισιόν και στοχεύει στη βελτίωση της ασφάλειας στην θάλασσα και την πρόληψη της θαλάσσιας ρύπανσης εφαρμόζοντας διεθνή κανονισμούς που αφορούν τον εξοπλισμό των πλοίων.

2.5 **Αυτόματο σύστημα εντοπισμού** - (Automatic Identification System - AIS)

Το σύστημα AIS σχεδιάστηκε αρχικά για να βοηθήσει την αποφυγή συγκρούσεων πλοίων, καθώς και να υποστηρίξει τις λιμενικές αρχές στην επίτευξη του καλύτερου έλεγχου της θαλάσσιας κυκλοφορίας. Οι πομποί AIS που είναι εγκατεστημένοι στα πλοία περιλαμβάνουν έναν δέκτη εντοπισμού θέσης GPS (Global Positioning System) που υπολογίζει τις συντεταγμένες της θέσης του πλοίου, την ταχύτητά του και την πορεία του. Περιλαμβάνει επίσης έναν πομπό VHF, ο οποίος μεταδίδει περιοδικά τις πληροφορίες αυτές σε δυο κανάλια VHF (συχνότητες 161,975 MHz και 162,025 MHz – παλιά VHF κανάλια 87 & 88). Άλλα πλοία ή σταθμοί βάσης μπορούν να λάβουν τις πληροφορίες αυτές χρησιμοποιώντας έναν δέκτη AIS. Στη συνέχεια, με χρήση ειδικού λογισμικού που επεξεργάζεται τα δεδομένα, τα πλοία εμφανίζονται στις οθόνες συστημάτων πλοήγησης ή σε υπολογιστή.

Τυπικά, τα σκάφη με δέκτη AIS με μια εξωτερική κεραία που τοποθετείται 15 μέτρα πάνω από το επίπεδο της θάλασσας, θα λάβουν τις πληροφορίες AIS, εντός μιας ακτίνας 15-20 ναυτικών μιλίων. Οι σταθμοί βάσης που εγκαθίστανται σε μεγαλύτερο υψόμετρο, μπορούν να επεκτείνουν την εμβέλεια μέχρι 40-60 ν.μ., ακόμη και πίσω από απομακρυσμένα βουνά. Η εμβέλεια εξαρτάται από το ύψος της κεραίας, τα εμπόδια γύρω από την κεραία και τις καιρικές συνθήκες. Ο σημαντικότερος παράγοντας είναι βέβαια το υψόμετρο. Έχουμε δει πλοία έως 150 ν.μ. μακριά με μια μικρή φορητή κεραία τοποθετημένη σε βουνό νησιού με υψόμετρο 700 μέτρα! Οι σταθμοί βάσης μας καλύπτουν πλήρως μια ακτίνα 40 μιλίων και περιοδικά λαμβάνουν πληροφορίες από πλοία που βρίσκονται μέχρι και 100 μίλια μακριά.

Κάθε σταθμός βάσης είναι εξοπλισμένος με έναν δέκτη AIS, έναν ηλεκτρονικό υπολογιστή και μια σύνδεση στο Internet. Ο δέκτης AIS λαμβάνει δεδομένα, τα οποία υποβάλλονται σε επεξεργασιά από ένα απλό λογισμικό στον υπολογιστή και στη συνέχεια αποστέλλονται σε μια κεντρική βάση δεδομένων μέσω ενός «web service». Αυτό το λογισμικό είναι ελεύθερο για όσους ενδιαφέρονται, με άδεια χρήσης GNU.Τα δεδομένα που λαμβάνονται από τον δέκτη AIS είναι κωδικοποιημένα σε μηνύματα NMEA (6-bit απλό κείμενο).

παράδειγμα:!AIVDM,1,1,,B,1INS<8@P001cnWFEdSmh00bT0000,0*38

Τα μηνύματα AIS περιλαμβάνουν τους παρακάτω βασικούς τύπους πληροφορίας:
1. Δυναμική πληροφορία, όπως η θέση του πλοίου, η ταχύτητα, η πορεία, και η ταχύτητα στροφής.
2. Στατική πληροφορία, όπως το όνομα του πλοίου, ο αριθμός IMO, ο αριθμός MMSI και οι διαστάσεις του.
3. Πληροφορίες που σχετίζονται με το συγκεκριμένο ταξίδι που εκτελεί, όπως προορισμός, εκτιμώμενη άφιξη (ETA)και βύθισμα.

Η κεντρική βάση δεδομένων λαμβάνει και επεξεργάζεται ένα σημαντικό όγκο δεδομένων. Από αυτά αποθηκεύει τα πιο σημαντικά, τα οποία είναι απαραίτητα να δώσουν μια καλή εικόνα των θέσεων των πλοίων. Περιλαμβάνει επίσης γεωγραφικές πληροφορίες για τα λιμάνια και για άλλες περιοχές, φωτογραφίες πλοίων και άλλες χρήσιμες πληροφορίες. [3]

Κεφάλαιο 3

3.1 Πώς διεξάγεται η εκτίμηση κινδύνου

Σε επίπεδο ΕΕ δεν υφίστανται παγιωμένοι κανόνες σχετικά με τον τρόπο διεξαγωγής της εκτίμησης κινδύνου (θα πρέπει να συμβουλευθείτε την νομοθεσία της χώρας σας όσον αφορά την εκτίμηση κινδύνου). Εντούτοις, κατά την προσέγγιση μιας εκτίμησης κινδύνου θα πρέπει πάντοτε να λαμβάνονται υπόψη οι εξής δύο αρχές:

- η διάρθρωση της εκτίμησης θα πρέπει να διασφαλίζει την κάλυψη όλων των συναφών πηγών κινδύνων και πιθανών κινδύνων (ούτως ώστε, π.χ. να μην παραμεληθούν εργασίες (όπως η καθαριότητα) που διεξάγονται ενδεχομένως εκτός κανονικού ωραρίου εργασίας ή δευτερογενείς όπως η ανακύκλωση των απορριμμάτων)

- μόλις προσδιοριστεί ένας κίνδυνος, η διαδικασία της εκτίμησης οφείλει να ξεκινήσει από τις βασικές αρχές της, εξετάζοντας καταρχάς εάν μπορεί να εξαλειφθεί εντελώς.

Οι κατευθυντήριες γραμμές της ΕΕ σχετικά με την εκτίμηση κινδύνου στην εργασία προτείνουν μια σταδιακή προσέγγιση που βασίζεται σε μια σειρά βημάτων. Δεν πρόκειται για τη μοναδική μέθοδο διεξαγωγής της εκτίμησης κινδύνου· υπάρχουν πολλές διαφορετικές μεθοδολογίες για την επίτευξη του ίδιου σκοπού. Δεν υπάρχει μόνο ένας «σωστός» τρόπος για την εκτέλεση μιας εκτίμησης κινδύνου καθώς διαφορετικές προσεγγίσεις μπορούν να αποδώσουν σε διαφορετικές περιστάσεις.

Η διαδικασία εκτίμησης κινδύνου (με την ενσωμάτωση στοιχείων διαχείρισης κινδύνου) μπορεί να περιγραφεί αναλυτικά με τα παρακάτω βήματα.

1) Καθιέρωση ενός προγράμματος εκτίμησης κινδύνου στην εργασία
2) Διάρθρωση της εκτίμησης (λήψη αποφάσεων σχετικά με την προσέγγιση: γεωγραφική/λειτουργική/διαδικασίας/ροής)
3) Συλλογή πληροφοριών
4) Προσδιορισμός πηγών κινδύνου
5) Προσδιορισμός των ατόμων που απειλούνται από τις πηγές κινδύνου
6) Προσδιορισμός των τύπων έκθεσης των ατόμων που απειλούνται από τις πηγές κινδύνου
7) Αξιολόγηση των κινδύνων (πιθανότητες πρόκλησης βλάβης/η σοβαρότητα βλάβης υπό πραγματικές συνθήκες)
8) Εξέταση των επιλογών για την εξάλειψη ή τον έλεγχο των κινδύνων

9) Καθορισμός προτεραιοτήτων για την ανάληψη δράσης και λήψη αποφάσεων σχετικά με τα μέτρα ελέγχου
10) Εφαρμογή ελέγχων
11) Καταγραφή της εκτίμησης
12) Μέτρηση αποτελεσματικότητας της δράσης
13) Αναθεώρηση (σε περίπτωση αλλαγών ή σε τακτά χρονικά διαστήματα)
14) Παρακολούθηση του προγράμματος εκτίμησης κινδύνου

Στις περισσότερες επιχειρήσεις, κυρίως στις μικρές και μικρομεσαίες επιχειρήσεις, μια απλή προσέγγιση της εκτίμησης κινδύνου, με πέντε βήματα, είναι συνήθως επιτυχής.

Βήμα 1. Προσδιορισμός των πηγών κινδύνων καθώς και των ατόμων που απειλούνται από αυτές
Αναζήτηση στον εργασιακό χώρο των παραγόντων εκείνων οι οποίοι θα μπορούσαν να προκαλέσουν βλάβη και προσδιορισμός των εργαζομένων οι οποίοι μπορεί να εκτίθενται σε κάποια πηγή κινδύνου.

Βήμα 2. Εκτίμηση των κινδύνων και καθορισμός προτεραιοτήτων
Υπολογισμός των πηγών κινδύνου (της σοβαρότητας και της πιθανότητας πρόκλησης βλάβης…) και καθορισμός προτεραιοτήτων με βάση τη σοβαρότητα του κάθε κινδύνου.

Βήμα 3. Λήψη αποφάσεων σχετικά με προληπτική δράση
Προσδιορισμός των κατάλληλων μέτρων ώστε οι κίνδυνοι να εξαλειφθούν ή να τεθούν υπό έλεγχο.

Βήμα 4. Ανάληψη δράσης
Θέσπιση μέτρων πρόληψης και προστασίας μέσω ενός σχεδίου που θα καθορίζει προτεραιότητες.

Βήμα 5. Παρακολούθηση και αναθεώρηση
Η εκτίμηση πρέπει να αναθεωρείται ανά τακτά διαστήματα, ώστε να διασφαλίζεται η ενημερότητα της.

Ωστόσο, είναι σημαντικό να γνωρίζουμε ότι υπάρχουν και άλλες μέθοδοι οι οποίες λειτουργούν εξίσου καλά, ιδιαίτερα για πιο περίπλοκους κινδύνους και συνθήκες. Η επιλογή της προσέγγισης της εκτίμησης εξαρτάται από:

- τη φύση του χώρου εργασίας (π.χ. μόνιμες ή προσωρινές εγκαταστάσεις)

- το είδος της διαδικασίας (π.χ. επαναλαμβανόμενες λειτουργίες, εξελισσόμενες/μεταβαλλόμενες διαδικασίες, εργασία κατ' αίτηση)
- το είδος της εργασίας που εκτελείται (π.χ. επαναληπτική, περιστασιακή ή υψηλού κινδύνου)
- την τεχνική πολυπλοκότητα.

Σε ορισμένες περιπτώσεις μπορεί να κριθεί κατάλληλη μία ενιαία προσέγγιση που να καλύπτει όλους τους κινδύνους σε ένα χώρο εργασίας ή μια δραστηριότητα. Σε άλλες περιπτώσεις, διαφορετικές προσεγγίσεις μπορεί να κριθούν κατάλληλες για διαφορετικά μέρη ενός χώρου εργασίας.[6]

3.2 Οφέλη της ανάλυσης κινδύνων

Παρακάτω αναφέρονται τα πιο σημαντικά οφέλη που αποκομίζονται από την ανάλυση κινδύνων πληροφοριακών συστημάτων.

Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος
Η ανάλυση κινδύνων βοηθάει στην γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος αναγνωρίζοντας και αντιμετωπίζοντας τους σημαντικότερους κινδύνους που το απειλούν.

Στόχευση της ασφάλειας
Η ασφάλεια πρέπει να στοχεύει κατάλληλα και άμεσα στις πιθανές επιπτώσεις, απειλές και υπάρχουσες ευπάθειες. Η αποτυχία να γίνει αυτό μπορεί να οδηγήσει σε υπερβολικές και μη αναγκαίες δαπάνες. Η ανάλυση κινδύνων προάγει πολύ καλύτερη στόχευση που βοηθά στην εξάλειψη των άσκοπων δαπανών και στην πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφαλείας.

Βελτίωση της κατανόησης του συστήματος
Κατά την διαδικασία της ανάλυσης κινδύνων βελτιώνεται η γνώση και η κατανόηση του συστήματος ως προς θέματα ασφαλείας. Καταρχάς αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειες του. Επίσης κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.

Κατανόηση της αναγκαιότητας της ασφάλειας
Η συμμετοχή στην διαδικασία της ανάλυσης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με αυτό τον τρόπο επιτυγχάνεται καλύτερη επιλογή αντιμέτρων αλλά και μεγαλύτερη αποδοχή των αντιμέτρων που προτείνονται από τους

χρήστες. Η κατανόηση της αναγκαιότητας της ασφάλειας έχει ως αποτέλεσμα την αντιμετώπιση των θεμάτων ασφαλείας με την σοβαρότητα που τους αρμόζει.

Δικαιολόγηση δαπανών για την ασφάλεια
Η εισαγωγή ασφάλειας σε ένα πληροφοριακό σύστημα σχεδόν πάντα σημαίνει επιπλέον κόστος. Επειδή όμως δεν οδηγεί άμεσα σε αύξηση των κερδών μιας επιχείρησης, πρέπει να δικαιολογείται οικονομικά. Η ανάλυση κινδύνων δημιουργεί την κατάλληλη δικαιολόγηση για την αναγκαιότητα της ασφάλειας που προτείνεται και του κόστους που αυτή προσθέτει.[7],[8]

3.3 Εργαλεία Ανάλυσης Κινδύνων [9], [10]

Η ανάλυση κινδύνων είναι μια συνθέτη διαδικασία, και η διαχείριση των Πληροφοριών που συλλέγονται είναι ανάλογη με το εύρος της. Για τη διευκόλυνση της ανάλυσης κίνδυνων, ορισμένες εταιρίες ανέπτυξαν η κάθε μια τις δίκες τις μεθόδους. Αυτό ήταν ένα σημαντικό βήμα για να ελαχιστοποιηθεί η παρέμβαση εξωτερικών ειδικών συνεργατών στα εσωτερικά μίας εταιρείας ή ενός οργανισμού. Αρχικά τα προγράμματα που σχεδιάστηκαν ήταν απλά και περιορίζονταν σε απλούς υπολογισμούς. Στην συνέχεια όμως, λόγω της αύξησης της πολυπλοκότητας των πληροφοριακών συστημάτων καθώς και των προβλημάτων ασφαλείας, τα προγράμματα για ανάλυση κινδύνων έλαβαν πιο ενεργό ρόλο αναλαμβάνοντας την διευκόλυνση του συνόλου της ανάλυσης κινδύνων με πολλά διαφορετικά εργαλεία. Μάλιστα κατά την δεκαετία του ’90 που τέτοια προγράμματα βγήκαν στην ελεύθερη αγορά, ο ανταγωνισμός οδήγησε τις εταιρίες ανάπτυξης τους να προσθέσουν νέα χαρακτηριστικά ώστε τελικά να καταλήξουν σε μεγάλα πακέτα εφαρμογών. Παρακάτω περιγράφονται οι δυνατότητες, τα χαρακτηριστικά και τα εργαλεία που έχουν αναπτυχθεί όλα αυτά τα χρόνια για το λογισμικό ανάλυσης κινδύνων.

3.3.1 *Callio Secura 17799*
Το Callio Secura 17799 είναι ένα σύστημα διαχείρισης ασφάλειας πληροφοριακών συστημάτων με έμφαση την συμμόρφωση με το διεθνές στάνταρ BS7799 / ISO 17799. Βασίζεται σε μια δική του μέθοδο για την ανάλυση κινδύνων που είναι σχετικά απλή, βήμα προς βήμα, ώστε να γίνεται εύκολα κατανοητή και να μην απαιτεί ειδικευμένο προσωπικό για την χρήση του. Ανήκει δε στην κατηγορία των ποιοτικών μεθόδων. Ιδρύθηκε το 2001 στον Καναδά.
Το πρόγραμμα δημιουργεί ένα web site στο οποίο μπορούν να έχουν πρόσβαση από παντού όσοι συμμετέχουν στην ανάλυση κινδύνων και χρησιμοποιείται επίσης για την ενημέρωση και εκπαίδευση του προσωπικού για τα θέματα ασφαλείας, τις υπάρχουσες πολιτικές ασφαλείας, τις διαδικασίες κτλ. Περιέχει

όλα εκείνα τα εργαλεία που χρειάζονται για την συνεχή διαχείριση και βελτίωση όλων των εγγράφων ασφαλείας του οργανισμού (πχ. version control). [14]

3.3.2 ***MEHARI*** *(Méthode Harmonisée d'Analyse de Risques Informatiques)*

Σχεδιάστηκε από ειδικούς ασφάλειας του CLUSIF (Club de la Sécurité Informatique Français) και αντικατέστησε τις προηγούμενες μεθόδους MARION και MELISA. Ανακοινώθηκε το 1996. Παρέχει ένα μοντέλο αποτίμησης επικινδυνότητας και αρθρωτά συστατικά και διαδικασίες. Περιέχει τύπους που διευκολύνουν την αναγνώριση και χαρακτηρισμό των απειλών και τη βέλτιστη επιλογή διορθωτικών μέτρων. Έχει λίστα σημείων ευπαθειών που πρέπει να ελεγχθούν. Είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 13335 .

3.3.3 ***OCTAVE*** *(Operationally Critical Threat, Asset, and Vulnerability Evaluation)*

Ανακοινώθηκε το 1999, από το Software Engineering Institute του Carnegie-Mellon University. Η OCTAVE είναι αυτοκατευθυνόμενη, με την έννοια ότι μια μικρή ομάδα ατόμων από τις επιχειρησιακές μονάδες και τη Δ/νση Πληροφορικής εργάζονται μαζί για να ικανοποιήσουν τις ανάγκες ασφάλειας του οργανισμού. Η OCTAVE-S είναι μια παραλλαγή της μεθόδου για μικρούς (λιγότερα από 100 άτομα) οργανισμούς. Το Octave Automated Tool αναπτύχθηκε από το Advanced Technology Institute (ATI) προκειμένου να υποστηρίζει τους χρήστες της OCTAVE

3.3.4 ***COBRA***

"Ένα από τα πλεονεκτήματα του είναι η αυτόματη προσαρμογή της ανάλυσης στις ανάγκες της εκάστοτε εταιρείας, καθώς χρησιμοποιεί τη δίκη του μέθοδο για να επιτευχθεί η αρμονία με το διεθνές στάνταρ ISO/IEC 17799. Παρ'όλο ότι είναι ένα από τα πιο παλιά προγράμματα που έχουν κυκλοφορήσει, έχει το πλεονέκτημα της αυτόματης προσαρμογής της ανάλυσης κινδύνων στα προβλήματα της εκάστοτε εταιρείας. Έχει την δυνατότητα, επίσης, για την δημιουργία αναφορών επαγγελματικού επιπέδου είτε για την διοίκηση της εταιρείας, είτε για το τεχνικό προσωπικό. Τρέχει σε λειτουργικό σύστημα Windows με κάποιο UI. Επίσης, για πιο απαιτητικές αναλύσεις επιτρέπεται η πλήρη παραμετροποίηση των γνωσιακών βάσεων που περιέχει (knowledge bases). Περιλαμβάνεται επιπλέον και η λεγόμενη «What if» ανάλυση, κατά την οποία ελέγχονται υποθετικά σενάρια ώστε να διαπιστωθεί δυναμικά η επίδραση που θα έχουν συγκεκριμένα αντίμετρα στους βαθμούς κινδύνου. Έχει σχεδιαστεί από την εταιρεία C&A System Security Ltd. Μετρά το βαθμό επικινδυνότητας για κάθε περιοχή ενός συστήματος και τον συνδέει με τη πιθανή επιχειρησιακή επίπτωση. Προσφέρει λεπτομερείς λύσεις και συστάσεις μείωσης της επικινδυνότητας.

3.3.5 *IT-Grundschutz*

Ανακοινώθηκε το 1994. Περιέχει και γενικές συστάσεις για την δημιουργία μιας εφαρμόσιμης διαδικασίας ασφάλειας και λεπτομερείς τεχνικές οδηγίες για την επίτευξη του απαραίτητου επιπέδου ασφάλειας σε συγκεκριμένα πεδία. Η διαδικασία ασφάλειας που προβλέπει η IT-Grundschutz αποτελείται από τα εξής βήματα: αρχικοποίηση της διαδικασίας, καθορισμός στόχων ασφάλειας και επιχειρησιακού περιβάλλοντος, καθιέρωση οργανωτικής δομής για την ασφάλεια, παροχή των απαραίτητων πόρων, δημιουργία της έννοιας της ασφάλειας, ανάλυση της πληροφοριακής υποδομής, αποτίμηση απαιτήσεων προστασίας, μοντελοποίηση, έλεγχος ασφάλειας, συμπληρωματική ανάλυση ασφάλειας, σχεδιασμός υλοποίησης και υλοποίηση, συντήρηση, παρακολούθηση και βελτίωση της διαδικασίας και πιστοποίηση (προαιρετικά). Η IT-Grundschutz υποστηρίζεται από το εργαλείο Gstool που αναπτύχθηκε από το Federal Office for Information Security (BSI). Η μέθοδος είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001

3.3.6 *EBIOS*

Αναπτύχθηκε το 1995 από την DCSSI (Direction Centrale de la Sécurité des Systèmes d' Information) της Γαλλικής κυβέρνησης. Λαμβάνει υπόψη τόσο τεχνικές όσο και μη τεχνικές οντότητες. Επιτρέπει σε όλο το προσωπικό που χρησιμοποιεί το ΠΣ να εμπλακεί στα θέματα ασφάλειας και προσφέρει μια δυναμική προσέγγιση που ενθαρρύνει τη διάδραση ανάμεσα στις διάφορες λειτουργίες του οργανισμού, εξετάζοντας το συνολικό κύκλο ζωής του συστήματος.
Η EBIOS είναι συμβατή με τα πρότυπα ISO/IEC 27001, ISO/IEC 13335 (GMITS), ISO/IEC 15408 (Common Criteria), ISO/IEC 17799 και ISO/IEC 21827.
Το 2002, διεθνείς συγκρίσεις τοποθετούν την EBIOS μεταξύ των τριών καλύτερων μεθόδων για την ανάλυση πληροφοριακών κινδύνων. Πολλές οργανώσεις του δημόσιου και του ιδιωτικού τομέα χρησιμοποιούν τη μέθοδο για να πραγματοποιούν τις δικές τους αναλύσεις πληροφοριακού κινδύνου

3.3.7 *CounterMeasures*

Προϊόν της Allion για διαχείριση επικινδυνότητας βασισμένο στις σειρές αμερικανικών προτύπων US-NIST 800 και OMB Circular A-130. Ο χρήστης αρχικοποιεί τα κριτήρια αξιολόγησης και, χρησιμοποιώντας μια "tailor-made" λίστα ελέγχου αποτίμησης, το software παρέχει αντικειμενικά κριτήρια αξιολόγησης για να αποφασίσει για το βαθμό ασφάλειας και συμμόρφωσης με τα πρότυπα.

3.3.8 *PROTEUS*

Είναι σύνολο προϊόντων της Infogov, που ανακοινώθηκε το 1999. Επιτρέπει τη διεξαγωγή ανάλυσης κενών στη συμμόρφωση με πρότυπα όπως το ISO 17799 ή τη δημιουργία και διαχείριση ενός ISMS σύμφωνα με το πρότυπο ISO 27001 (BS 7799-2). Το Proteus Enterprise είναι πλήρως ολοκληρωμένη Web-based εφαρμογή για διαχείριση επικινδυνότητας για μεγάλες επιχειρήσεις. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001.

3.3.9 *RA2 Art of Risk*

Είναι εργαλείο της AEXIS, που αντικατέστησε το RA Software Tool και ανακοινώθηκε το 2000. Είναι σχεδιασμένο για να βοηθήσει τις επιχειρήσεις να αναπτύξουν ένα ISMS συμβατό με το πρότυπο ISO/IEC 27001:2005 (προηγουμένως BS 7799 Part 2:2002) και τον κώδικα πρακτικής ISO/IEC 27002. Το RA2 Information Collection Device, ένα συστατικό που διανέμεται μαζί με το εργαλείο, μπορεί να εγκατασταθεί οπουδήποτε στον οργανισμό υπάρχει ανάγκη για συλλογή πληροφορίας προς χρήση από τη διαδικασία αποτίμησης επικινδυνότητας. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001

3.3.10 *CRAMM*

Το CRAMM είναι ένα εργαλείο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το CCTA (Central Computer and Telecommunications Agency) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Το πρόγραμμα, το οποίο έχει υποστεί σημαντικές αναθεωρήσεις και βρίσκεται σήμερα στην έκδοση 5, συνεχίζει να αναπτύσσεται πλέον από την εμπορική εταιρία Insight Consulting που έχει έδρα στην Αγγλία. Το CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του ΝΑΤΟ. Το πρόγραμμα ακολουθεί την δική του μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές στάνταρ ISO17799/BS7799. Τα βασικά χαρακτηριστικά του προγράμματος είναι:

- Μεγάλη βάση αντιμέτρων που ανανεώνεται συνεχώς και καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριακών συστημάτων.

- «What if» ανάλυση

- Εργαλεία για την δημιουργία σχεδίων «Business Continuity»

- Οδηγούς για την δημιουργία πολιτικών ασφαλείας

- Οδηγούς για την δημιουργία αναφορών

- Σχετικά σύγχρονο περιβάλλον σε πλατφόρμα MS Windows

- Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού (σε συνεννόηση με την εταιρία)

Υπάρχει και η έκδοση CRAMM Express η οποία δεν περιλαμβάνει όλα τα εργαλεία σαν την κανονική έκδοση αλλά είναι πιο απλή στην χρήση και οδηγεί σε πιο γρήγορα αλλά λιγότερο αναλυτικά αποτελέσματα.[15]

3.3.11 *Ezrisk*

Το Ezrisk είναι ένα προϊόν που σχεδιάστηκε από την εταιρία Ezrisk Limited και στοχεύει κυρίως στις μικρομεσαίες επιχειρήσεις. Οι επιχειρήσεις αυτές συνήθως δεν έχουν ειδικούς για να διεξάγουν τις δικές τους αναλύσεις κινδύνων και ούτε έχουν τους πόρους για να αγοράσουν ανάλογες υπηρεσίες. Το πρόγραμμα Ezrisk είναι φθηνό και εξαιρετικά απλό, ώστε να μην χρειάζεται ειδική εκπαίδευση για την χρήση του. Περιέχει αλγορίθμους που ελέγχουν τα δεδομένα που εισάγει ο χρήστης, αναγνωρίζουν τυχόν σφάλματα ή αντιφάσεις και βοηθούν στην επίλυση τους. Είναι συμβατό με το διεθνές στάνταρ ISO17799/BS7799 και βοηθάει στην επίτευξη συμμόρφωσης με αυτό. Μπορεί να παράγει αναφορές σε απλή και κατανοητή μορφή, εξηγώντας τους κινδύνους και τα αντίμετρα που προτείνονται σε κάθε περίπτωση. Τέλος, δημιουργεί σχέδιο δράσης που δείχνει τα βήματα που πρέπει να ακολουθηθούν μέχρι την επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799, βάση της προτεραιότητας τους.

3.3.12 *RiskWatch for Information Systems & ISO 17799*

Η εταιρία RiskWatch ειδικεύεται στην δημιουργία προγραμμάτων ανάλυσης κινδύνων για πολλούς τομείς, μεταξύ των οποίων και ο τομέας της ασφάλειας πληροφοριακών συστημάτων. Η κύρια διαφορά του σε σχέση με τα περισσότερα προγράμματα του ανταγωνισμού είναι η χρήση ποσοτικής μεθόδου ανάλυσης κινδύνων. Το πρόγραμμα περιέχει χρόνια δεδομένων ποσοτικής ανάλυσης που χρησιμοποιούνται έτοιμα για την εξοικονόμηση χρόνου και προσπάθειας. Εναι ιδιαίτερα δημοφιλής στις ΗΠΑ και έχει μεγάλο κύρος καθώς χρησιμοποιείται σε πολλές κυβερνητικές υπηρεσίες και μεγάλους ιδιωτικούς οργανισμούς. Μερικοί από αυτούς είναι: Υπουργείο Αμύνης των ΗΠΑ, Πεντάγωνο, NSA (National Security Agency), AT&T και Vodafone [16]

3.3.13 *Security by Analysis (SBA)*

Αναπτύχθηκε στη Σουηδία στις αρχές του ‘80. Χρησιμοποιείται έκτοτε με επιτυχία σχεδόν αποκλειστικά στις Σκανδιναβικές χώρες. Δέχεται ότι οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία του Π.Σ. έχουν τις περισσότερες πιθανότητες να εντοπίσουν τα προβλήματα και να προτείνουν λύσεις. Αποτελείται από ένα σύνολο μεθόδων με κυριότερες τις SBA Check και SBA Scenario. Η SBA Check προσφέρει ταχεία αποτίμηση του επιπέδου ασφάλειας του Π.Σ., στηρίζεται σε ερωτηματολόγια, εχει ως σημείο αναφοράς το ISO/IEC 17799 και υποστηρίζεται από ειδικό λογισμικό.

3.3.14 *CYSM*

Το εργαλείο CYSM στοχεύει στην ασφάλεια των λιμένων. Σκοπός του είναι να προσφέρει στα λιμάνια την δυνατότητα να βελτιώσουν την τρέχουσα ασφάλεια τους και το επίπεδο ασφάλειας , παρέχοντάς τους καινοτόμες , φιλικές προς το χρήστη , εξατομικευμένες υπηρεσίες διαχείρισης της ασφάλειας, που μπορούν να τους βοηθήσουν να λύσουν προβλήματα στον κυβερνοχώρο ή στην φυσική υποδομή τους.
Το εργαλείο αυτό, καθώς και το εργαλείο Medusa που αποτελεί προέκταση του, είναι ένα καινοτόμο συνεργατικό και ολοκληρωμένο εργαλείο με σκοπό την συνεχή αναγνώριση (identification), αξιολόγηση (assessment) και “θεραπεία” (treatment) των κινδύνων που επικρατούν στα λιμάνια [27]

Κεφάλαιο 4

4.1 Medusa

Για τις ανάγκες της παρούσας διπλωματικής εργασίας, σχεδιάστηκε ένα εργαλείο για την αξιολόγηση των κίνδυνων
Το εργαλείο Medusa έχει δημιουργηθεί στα πλαίσια ενός ευρωπαϊκού προγράμματος και αποτελεί μια προέκταση του εργαλείου CYSM και όπως και εκείνο, στοχεύει στην ασφάλεια των λιμενικών εγκαταστάσεων. Προσφέρει στα λιμάνια την δυνατότητα να βελτιώσουν την τρέχουσα ασφάλεια τους στον κυβερνοχώρο ή στην φυσική υποδομή τους.

Το εργαλείο Medusa (Multi-order Dependency approaches for managing cascading effects in port's global supply chain and their integration in risk assessment frameworks) σκοπεύει να προτείνει μια στοχευμένη προσέγγιση εκτίμησης κινδύνων που στοχεύει στην ενίσχυση της προστασίας και της ασφάλειας της εφοδιαστικής αλυσίδας των θαλασσών και εγγυώνται τη λειτουργία και την ανάπτυξη των θαλάσσιων μεταφορών. Η προτεινόμενη προσέγγιση θα παράγει τις πληροφορίες που απαιτούνται για την αξιολόγηση και τον μετριασμό της εφοδιαστικής αλυσίδας των θαλασσών με συναφείς κινδύνους και απειλές.
Για το σκοπό αυτό,θα αναπτυχθεί ένα αποτελεσματικό, συνεργατικό, εργαλείο διαχείρισης του κινδύνου, βασισμένο σε πρότυπα, που θα εφαρμόσει την προτεινόμενη προσέγγιση. Αυτό το εργαλείο εξετάζει όλες τις απειλές που προκύπτουν από την παγκόσμια αλυσίδα εφοδιασμού, συμπεριλαμβανομένων των απειλών που συνδέονται με τα λιμάνια των αλληλεξαρτήσεων και των συναφών επιπτώσεων.

4.2 Λειτουργικές απαιτήσεις:

1. **Η συμμόρφωση με τα πρότυπα ασφαλείας και διαχείρισης κινδύνων .**
   Το Medusa πρέπει να είναι συμβατό με τα γνωστά και de facto πρότυπα που σχετίζονται με τη διαχείριση της ασφάλειας και της διαχείρισης των κινδύνων.

2. **Η συμμόρφωση με συγκεκριμένο πλαίσιο κανόνων .**
   Το εργαλείο Medusa πρέπει να είναι συμβατό με ένα φάσμα υφιστάμενων προτύπων που σχετίζονται με την ασφάλεια του τομέα της ναυτιλίας , καθώς και τη διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας.

   Περιλαμβάνει αλλά δεν περιορίζεται σε :

- αξιολόγηση ασφάλειας λιμενικών εγκαταστάσεων θαλάσσιου χώρου του λιμένα και την ανάπτυξη προτύπων σχεδίου ασφάλειας. Το προτυπο ISO 20858

έχει σχεδιαστεί για να βοηθήσει στην ομοιόμορφη εφαρμογή της βιομηχανίας του Κώδικα ISPS .

- πρότυπα αξιολόγησης των κινδύνων της εφοδιαστικής αλυσίδας. Το Medusa θα πρέπει να είναι πλήρως συμβατό με την οικογένεια προτύπων 28000, δεδομένου ότι προσδιορίζουν τις βέλτιστες πρακτικές για την εφαρμογή της ασφάλειας της εφοδιαστικής αλυσίδας , τις εκτιμήσεις και τα σχέδια .

3. **Ολιστική άποψη της εφοδιαστικής αλυσίδας .**

Η κύρια λειτουργική απαίτηση της μεθοδολογίας Medusa είναι να εντοπίζει και να διαχειρίζεται τις κλιμακωτές απειλές στην αλυσίδα εφοδιασμού του λιμανιού , αναλύοντας τις αλλιλεξαρτήσεις εντός της εφοδιαστικής αλυσίδας . Ως εκ τούτου το εργαλείο πρέπει να ενσωματώνει μια ολιστική άποψη της εφοδιαστικής αλυσίδας και των σχέσεων (εξαρτήσεις) μεταξύ των συμμετεχόντων που έχουν βασικό ρόλο στη μεθοδολογία .

4. **Η υποστήριξη για τη συνεργατική διαχείριση του κινδύνου** .

Όπως συζητήθηκε στις τεχνικές προδιαγραφές , το Medusa πρέπει να υποστηρίζει ένα συνεργατικό - προσανατολισμένο σχεδιασμό . Όσον αφορά τις λειτουργικές απαιτήσεις της μεθοδολογίας , θα πρέπει να υποστηρίζει τη συνεργατική συγκέντρωση γνώσεων , καθώς και την ομαδική διαδικασία λήψης αποφάσεων . Το αποτέλεσμα της εκτίμησης των κινδύνων της εφοδιαστικής αλυσίδας θα πρέπει να βασίζεται σε μια ομαδική και προσεγγιστική λήψη αποφάσεων , όπου όλοι οι συμμετέχοντες θα είναι σε θέση να παρέχουν την άποψή τους σχετικά με τη διαδικασία αξιολόγησης του κινδύνου με αποτελεσματικό τρόπο .

5. **Ελαχιστοποίηση της προσπάθειας των συμμετεχόντων**

Αν μια μεθοδολογία εκτίμησης κινδύνων της εφοδιαστικής αλυσίδας τοποθετεί μια πρόσθετη επιβάρυνση για τους συμμετέχοντες , είναι εξαιρετικά απίθανο η μεθοδολογία αυτή να υιοθετηθεί ευρέως. Το Medusa στοχεύει στην ελαχιστοποίηση του απαιτούμενου χρόνου και προσπάθειας του κάθε συμμετέχοντα για την αξιολόγηση των κινδύνων της εφοδιαστικής αλυσίδας . Όταν είναι δυνατόν , πρέπει να χρησιμοποιούνται τα αποτελέσματα της εκτίμησης κινδύνου από μια υφιστάμενα οργάνωση. Επιπλέον , όταν αυτό είναι δυνατόν , μια είσοδος που απαιτείται από τη μεθοδολογία στα αρχικά στάδια της, θα πρέπει να καθοριστεί σαφώς με σκοπό την επαναχρησιμοποίησης της στα επόμενα βήματα της μεθοδολογίας . Για παράδειγμα, κατά τον υπολογισμό πολλαπλών επιπτώσεων, στοιχεία που παρασχέθηκαν κατά τη διάρκεια της αρχικής εκτίμησης των κινδύνων της εφοδιαστικής αλυσίδας, θα πρέπει να επαναχρησιμοποιείται .

6. **Προώθηση της επέκτασης της μεθοδολογίας.**
Όταν είναι δυνατόν , το Medusa θα πρέπει να σχεδιαστεί έχοντας κατά νου την επεκτασιμότητα και την προσαρμοστικότητα στις μελλοντικές αλλαγές . Για παράδειγμα , το εργαλείο θα πρέπει να υποστηρίζει την προσθήκη νέων απειλών για την ασφάλεια ή την έγκρισή της σε άλλα περιβάλλοντα της εφοδιαστικής αλυσίδας .

4.3 Μη λειτουργικές απαιτήσεις

Η μη λειτουργική απαίτηση καθορίζει τα κριτήρια που μπορούν να χρησιμοποιηθούν για να κριθεί σωστά η λειτουργία ενός συστήματος, σε αντίθεση με τις λειτουργικές απαιτήσεις που ορίζουν συγκεκριμένη συμπεριφορά ή λειτουργίες

1. Λειτουργικότητα
   Μια σειρά από χαρακτηριστικά σχετικά με την ύπαρξη ενός συνόλου λειτουργιών και καθορισμένες ιδιότητες.

- Καταλληλότητα (Suitability)
- Ακρίβεια (Accuracy)
- Διαλειτουργικότητα (Interoperability)
- Ασφάλεια (Security)
- Συμμόρφωση Λειτουργικότητας (Functionality Compliance)

2. Αξιοπιστία
   Μια σειρά από χαρακτηριστικά που φέρουν την ικανότητα του λογισμικού να διατηρήσει το επίπεδο της απόδοσης κάτω από καθορισμένες συνθήκες και για δεδομένη χρονική περίοδο .

- Ωριμότητα (Maturity)
- Ανοχή σφαλμάτων (Fault Tolerance)
- Δυνατότητα Ανάκαμψης (Recoverability)
- Συμμόρφωση Αξιοπιστίας (Reliability Compliance)

3. Ευχρηστία

Μια σειρά από χαρακτηριστικά σχετικά με την προσπάθεια που απαιτείται για τη χρήση του λογισμικού

- Κατανοητότητα (Understandability)
- Ευκολία εκμάθησης (learnability)
- Λειτουργικότητα (Operability)
- Ελκυστικότητα (Attractiveness)
- Συμμόρφωση Ευχρηστίας (Usability Compliance)

4. Αποτελεσματικότητα

Ένα σύνολο από χαρακτηριστικά για τη σχέση μεταξύ του επιπέδου της απόδοσης του λογισμικού και την ποσοτητα των πόρων που χρησιμοποιούνται , υπό καθορισμένες συνθήκες .

- Συμπεριφορά σύμφωνα με την ωρα (Time Behaviour)
- Αξιοποίηση των πόρων (Resource Utilization)
- Συμμόρφωση Αποδοτικότητας (Efficiency Compliance)

5. Δυνατότητα συντήρησης

Μια σειρά από χαρακτηριστικά σχετικα με την προσπάθεια που απαιτείται για να κάνουν συγκεκριμένες τροποποιήσεις .

- Δυνατότητα Ανάλυσης (Analyzability)
- Εναλλαξιμότητα (Changeability)
- Σταθερότητα (Stability)
- Δυνατότητα Δοκιμών (Testability)
- Συμμόρφωση στην συντήρηση (Maintainability Compliance)

6. Φορητότητα

Μια σειρά από χαρακτηριστικά σχετικά με την ικανότητα του λογισμικού να μεταφέρονται σε πολλές πλατφόρμες.

- Προσαρμοστικότητα (Adaptability)
- Δυνατότητα εγκατάστασης (Installability)
- Συνύπαρξη (Co-Existence)
- Δυνατότητα αντικατάστασης (Replaceability)
- Συμμόρφωση Φορητότητας (Portability Compliance)

Αυτή η ενότητα παρέχει μια επισκόπηση του εργαλείου διαχείρισης κινδύνων Medusa. Το συγκεκριμένο εργαλείο θα χρησιμοποιηθεί για να συλλάβει τις πολλαπλές επιπτώσεις στις που μπορούν να υπάρξουν στις διαδικασίες της εφοδιαστικής αλυσίδας ενός λιμανιού. Ο πρώτος στόχος του εργαλείου διαχείρισης κινδύνων Medusa είναι να διευκολύνει τον καθορισμό των αλυσίδων εφοδιασμού σε γραφικό / διαισθητικό τρόπο. Μια αλυσίδα εφοδιασμού είναι μια μαθηματική γραφική παράσταση που καταγράφει τις εξαρτήσεις μεταξύ των διαφόρων «παραγόντων» της αλυσίδας εφοδιασμού. Αυτοί οι παράγοντες δεν είναι από τους επιχειρηματικούς εταίρους.

Ένα γράφημα (που αντιπροσωπεύει μια αλυσίδα εφοδιασμού) μπορεί να είναι «αφηρημένο» ή «γειωμένο». Μια αφηρημένη γραφική παράσταση αντιπροσωπεύει τις εξαρτήσεις μεταξύ των επιχειρηματικών εταίρων, χωρίς να προσδιορίζεται ποια εταιρεία ή πρόσωπο αντιπροσωπεύει αυτόν τον εταίρο. Με άλλα λόγια, μια αφηρημένη αλυσίδα εφοδιασμού είναι ένα γράφημα εξάρτησης που μπορεί να επαναχρησιμοποιηθεί από πολλούς λιμένες, που αυτοί με την σειρά τους θα εκτελέσουν τη δική τους διαδικασία “γείωσης” δηλαδή την χαρτογράφηση των πραγματικών οντοτήτων (επιχειρηματικούς εταίρους) που αντιστοιχούν στον εκάστοτε λιμένα. Οι οντότητες που εμπλέκονται σε μια «γειωμένη» αλυσίδα εφοδιασμού θα πρέπει να αντιμετωπιστούν ως ενδιαφερόμενοι φορείς (Stakeholders).

Οι επιχειρηματικοί εταίροι (και ως εκ τούτου, οι ενδιαφερόμενοι φορείς) συνδέονται μεταξύ τους με έναν συγκεκριμένο τύπο εξάρτησης, που μπορεί να είναι φυσικός, στον κυβερνοχώρο κ.α. Κάθε ενδιαφερόμενος φορέας που έχει αντιστοιχηθεί σε ένα συγκεκριμένο τμήμα του γραφήματος, περιέχει έναν αντιπρόσωπο ο οποίος είναι ένα πρόσωπο που θα χρησιμοποιηθεί για να αλληλεπιδράσει με το εργαλείο διαχείρισης κινδύνου Medusa. Ο αντιπρόσωπος θα συνδεθεί στο εργαλείο, προκειμένου να παρέχει πληροφορίες σχετικά με τις απειλές, την ευπάθεια και τους έλεγχους που θα ανήκουν στην περιοχή ευθύνης του / της.

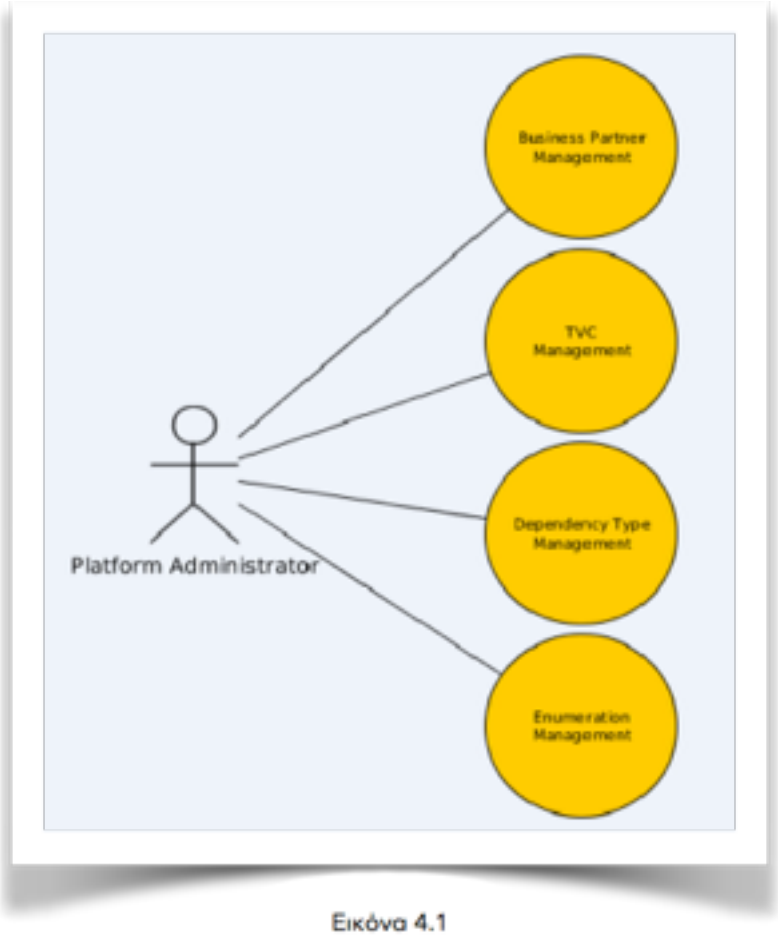
Το εργαλείο που θα δημιουργηθεί θα αξιολογεί την αναφορά του κάθε εκπροσώπου, και θα την αξιολογήσει σχετικά με τις κλιμακωτές επιπτώσεις βάσει συγκεκριμένων σεναρίων.

4.4 Οι εμπλεκόμενοι ρόλοι του Medusa

Οι ακόλουθοι ρόλοι που προσδιορίζονται στο οικοσύστημα Μέδουσα είναι:
• Ο διαχειριστής της πλατφόρμας
• Ο σχεδιαστής της Εφοδιαστικής Αλυσίδας
• Οντότητες ενδιαφερομένων Εκπρόσωπων

4.4.1 Διαχειριστής πλατφόρμας

Ο πρώτος ρόλος είναι ο διαχειριστής της πλατφόρμας.



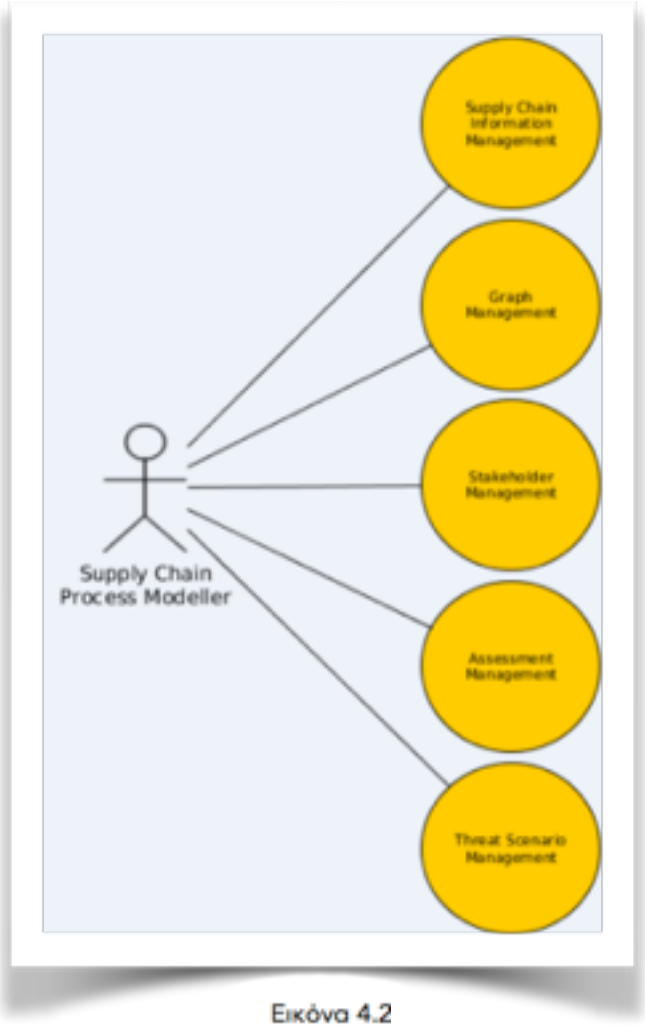
Εικόνα 4.1

Ο σκοπός του διαχειριστή της πλατφόρμας είναι να προετοιμάσει το σύστημα με τις πληροφορίες που θα πρέπει να είναι διαθέσιμες σε παγκόσμιο επίπεδο με τους άλλους δύο ρόλους. Οι αρμοδιότητες αυτού του ρόλου είναι:

α) να παρέχει ένα λεξιλόγιο των διαθέσιμων Business Partners που θα χρησιμοποιηθεί προκειμένου να σχεδιάσει τη γραφική παράσταση της εξάρτησης
β) να εκτελεί την διαδικασία Δημιουργίας (Create)-Ανάκτησης(Retrive)-Ενημέρωσης(Update)-Διαγραφής(Delete) (γνωστή και ως CRUD) για πράξεις σχετικά με τις θεμελιώδεις απειλές, τρωτά σημεία και τους ελέγχους (aka TVC). Είναι εξαιρετικά σημαντικό για τη συνοχή του εργαλείου,οι διαδικασίες CRUD να γίνονται σε κεντρικό επίπεδο.
γ) παρέχει όλα τα είδη των απαριθμήσεις όπως DependencyType (π.χ. στον κυβερνοχώρο), ConcequencyLevel (π.χ. υψηλή), ConcequencyType (π.χ. οικονομικά) κλπ που θα χρησιμοποιηθούν από των άλλους ρόλους.

4.4.2 Σχεδιαστής της εφοδιαστικής αλυσίδας

Ο δεύτερος ρόλος του Εργαλείου Διαχείρισης Κινδύνων Medusa είναι ο μοντελιστής/σχεδιαστής της εφοδιαστικής αλυσίδας .



Εικόνα 4.2

Οι κύριες αρμοδιότητες περιλαμβάνουν:
α) Τον ορισμό και την επεξεργασία των “αφηρημένων” (abstract) γραφημάτων της εφοδιαστικής αλυσίδας. Αυτά τα γραφήματα βασίζονται αποκλειστικά στους επιχειρηματικούς εταίρους (Business Partners), δεδομένου ότι, όπως έχει ήδη εξηγηθεί, δεν περιέχουν καμία πληροφορία για τους ενδιαφερόμενους φορείς (Stakeholders).

β) Πέραν του ορισμού των αφηρημένων γραφημάτων, είναι υπεύθυνος για την παροχή του καταλόγου με τα ενδιαφερόμενα μέλη που αντιστοιχούν σε συγκεκριμένους επιχειρηματικούς εταίρους (που έχουν ήδη καθοριστεί από τον διαχειριστή της πλατφόρμας) λαμβάνοντας υπ 'όψιν το επιχειρηματικό οικοσύστημα της

γ) είναι υπεύθυνος για την εκτέλεση της "γείωσης", δηλαδή να παρέχει συσχέτιση ενός πραγματικού ενδιαφερόμενου (Stakeholder) με μια επιχειρηματική οντότητα (Business partner) για ένα συγκεκριμένο κόμβο γράφημα (Graph node).

δ) Μια άλλη αρμοδιότητα, ίσως και η πιο κρίσιμη, είναι το “Assessment Management”. Σύμφωνα με αυτή την περίπτωση, μετά την προσάραξη της εφοδιαστικής αλυσίδας από τον μοντελιστή/σχεδιαστή, δίνει το προβάδισμα στους εκπροσώπους προκειμένου να παρέχουν πληροφορίες σχετικά με θέματα ευπάθειας και ελέγχων που είναι υπεύθυνοι για αυτά.

ε) Η τελευταία ευθύνη του, είναι η διαχείριση του σεναρίου σύμφωνα με το οποίο, συγκεκριμένες επιπτώσεις μπορούν να συναχθούν με βάση τις πληροφορίες που παρέχονται από τους αντιπροσώπους.

4.4.3 Υπεύθυνος Ασφαλείας

Τέλος , ο Υπεύθυνος Ασφαλείας.
Ο Υπεύθυνος Ασφαλείας είναι αρμόδιος για την επικύρωση του γραφήματος , αφού συνδεθεί στο σύστημα (με τις πιστοποιήσεις που έχουν δοθεί από τον υπεύθυνο ασφαλείας).
Από εκεί και πέρα ,είναι ο ίδιος υπεύθυνος για την παροχή των απειλών, ευπαθειών και των ελέγχων που εφαρμόζονται στη ζώνη της ευθύνης του

Εικόνα 4.3

4.5 Οι βασικές αρχές σχεδιασμού

Μια σειρά από βασικές αρχές σχεδιασμού θα πρέπει να θεσπισθούν προκειμένου να αναπτύξουν και να παρέχουν μια συνεπή και προηγμένη τεχνολογική αρχιτεκτονική, ικανή για τις καθορισμένες απαιτήσεις των χρηστών, καθώς και την ανάγκη να είναι εύκολα προσαρμόσιμο και επεκτάσιμο.
Αυτές οι αρχές σχεδιασμού είναι:

Επεκτασιμότητα (Modularity): Κάθε μονάδα θα πρέπει να είναι ένα συστατικό ενός μεγαλύτερου συστήματος , και να λειτουργεί στο πλαίσιο του συστήματος αυτού, ανεξάρτητα. Ως εκ τούτου, στο ολοκληρωμένο σύστημα, θα είναι εύκολο να διαιρεθεί ένα πρόβλημα λειτουργίας σε μικρότερα, τα οποία συνήθως συνδέονται με μια απλή δομή , και είναι αρκετά ανεξάρτητα μεταξύ τους.

Διαλειτουργικότητα (Interoperability): Η διασύνδεση πολλών κατανεμημένων και ετερογενών συστημάτων, είναι ένα δύσκολο έργο, που απαιτεί να αναγνωρίζονται εύκολα υπηρεσίες αξιολόγησης και διαχείρισης. Η διαλειτουργικότητα μεταξύ των βασικών συνιστωσών του Medusa, καθώς και με κάθε άλλο εξωτερικό σύστημα, επιτυγχάνεται με την υιοθέτηση Web Services ως τον βασικό πρωτόκολλο επικοινωνίας.

Δυνατότητα κλιμάκωσης & Επεκτασιμότητα (Scalability & Extensibility):
Η Δυνατότητα κλιμάκωσης και η επεκτασιμότητα εξαρταται σε μεγάλο βαθμό από την υιοθέτηση του Web Services ως τον πυρήνα πρωτόκολλο επικοινωνίας, και τις προηγμένες τεχνολογίες που βασίζονται σε XML.

Ασφάλεια (Security): Η ασφάλεια παραμένει μια από τις κύριες προκλήσεις. Η βιβλιογραφία έχει αποδειχθεί ότι οι απειλές αλλάζουν συνεχώς και τα υπολογιστικά συστήματα και συστήματα εφαρμογών Web υπόκεινται σε νέες σοβαρές, επίμονες και έντονες κυβερνο-επιθέσεις. Στο πλαίσιο αυτό, το εργαλείο Medusa έχει να αντιμετωπίσει μια σειρά από κρίσιμες απαιτήσεις ασφάλειας (π.χ. έλεγχος ταυτότητας, ακεραιότητα, μη άρνηση, και τη διαθεσιμότητα). Το Medusa θα πληρεί τις απαιτήσεις ασφαλείας κάνοντας χρήση του συνόλου των μηχανισμών ασφαλείας και μια σειρά από υπηρεσίες ασφαλείας.

Προστασία Προσωπικών Δεδομένων (Privacy): Προστασία Προσωπικών Δεδομένων σε μαζικά διασυνδεδεμένα περιβάλλοντα είναι μια κοινωνική αποδοχή από τους τελικούς χρήστες που απαιτούν εντελώς νέες προσεγγίσεις για την ταυτότητα και τη διαχείριση της ιδιωτικής ζωής. Επιπλέον, σε συνεργατικά περιβάλλοντα, όπως το σύστημα του Medusa, απαιτείται πρόσθετη προστασία, λόγω των μηχανισμών επεξεργασίας και των εργαλείων που χρησιμοποιούνται. Αξίζει να σημειωθεί ότι, προστασία της ιδιωτικής ζωής των χρηστών εξαρτάται σε μεγάλο βαθμό από τα κίνητρα των άλλων χρηστών.

Επαναχρησιμοποίηση (Reusability): Οι στόχοι πίσω από την επαναχρησιμοποίηση των υπηρεσιών συνδέονται άμεσα με μερικούς από τους πιο στρατηγικούς στόχους του service-oriented υπολογιστών, και θα πρέπει να υποστηρίζονται σθεναρά από το Medusa. Αντί για την ενσωμάτωση λειτουργιών που θα πρέπει να αναπτυχθούν για κάθε συγκεκριμένη υπηρεσία, το εργαλείο Medusa θα πρέπει να προσφέρει στους προγραμματιστές, προηγμένες και επαναχρησιμοποιήσιμες τεχνολογίες ασφάλειας, διεπαφές αποθήκευσης και Web Services για να επεκτείνεται εύκολα η λειτουργικότητα τους και να αξιοποιείται σωστά.

Είναι ένα συνεργατικό εργαλείο, καθώς μπορεί να γίνεται αξιολόγηση από πολλούς χρήστες ταυτόχρονα.

4.5.1 Τεχνολογίες και γλώσσα προγραμματισμού.

Οι τεχνολογίες για την κατασκευή αυτού του εργαλείου, την αλληλεπίδραση του χρήστη με το Web Περιβαλλον είναι:
HTML, CSS, ANGULAR JS, JavaScript.

Η HyperText Markup Language (HTML) είναι γλώσσα υπολογιστών για τη σύνταξη ιστοσελίδων. Δηλαδή, οι WEB σελίδες είναι HTML έγγραφα που αποτελούνται από κείμενο και κωδικούς της γλώσσας. Το όνομα του αρχείου έχει επέκταση .html ή .htm (π.χ. index.html).
Ο αναγνώστης (browser) ιστοσελίδων διαβάζει/μεταφράζει τους κωδικούς του εγγράφου και εμφανίζει το έγγραφο ως WEB σελίδα. Η διαδικασία αυτή είναι ανεξάρτητη από τη πλατφόρμα του υπολογιστή (UNIX, Windows ή Macintosh). [11]
Το CSS είναι μια απλή γλώσσα που μας βοηθάει να ορίσουμε με σαφήνεια και ιδιαίτερη ευελιξία τον τρόπο με τον οποίο θα εμφανίζονται τα διάφορα στοιχεία στην ιστοσελίδα μας.[12]

Η JavaScript (JS) είναι διερμηνευμένη γλώσσα προγραμματισμού για ηλεκτρονικούς υπολογιστές.[1] Αρχικά αποτέλεσε μέρος της υλοποίησης των περιηγητών ιστού, ώστε να είναι σε θέση να ανταλλάσσουν δεδομένα ασύγχρονα και να αλλάζουν δυναμικά το περιεχόμενο του εγγράφου που εμφανίζεται δημιουργώντας effects και animations

Κύριο στοιχείο για την υλοποίηση το frontend εργαλείου ειναι το AngularJS.

AngularJS είναι ένα δομικό πλαίσιο για ανάπτυξη δυναμικών web εφαρμογών. Επιτρέπει την χρήση της HTML ως ένα πρότυπο γλώσσας προγραμματισμού με σκοπό να επεκτείνει τη σύνταξη της HTML για να εκφράσει τα συστατικά μιας web εφαρμογής με συντομία και σαφήνεια .Με την χρήση της AngularJS εξαλείφεται ένα μεγάλο μέρος του κώδικα που διαφορετικά θα έπρεπε να γράφει, ώστε να υπάρχει η ίδια λειτουργικότητα.

4.6 Οι κύριοι φορείς στην αλυσίδα εφοδιασμού

Η προσέγγιση Διαχείρισης Εμπορευματοκιβωτίων αποτελεί περίπου το 70 % του συνόλου των εμπορευμάτων που μεταφέρονται δια μέσω των φορτηγών πλοίων (containers) στην ναυτιλία . Την ασφάλεια των εμπορευματοκιβωτίων αφορούν θέματα όπως οι τρομοκρατικές απειλές , κλοπή και το λαθρεμπόριο και αποτελεί σημαντικό παράγοντα για τη συνολική ευρωπαϊκή ασφάλεια διασυνοριακά και για θέματα της βελτιστοποίησης των αλυσίδων εφοδιασμού .
Είναι σημαντικό να σημειωθεί ότι οι έννοιες της εξαγωγής και της εισαγωγής χρησιμοποιούνται σε μια πιο ευρεία έννοια. 'Ετσι η εξαγωγή είναι η διαδικασία κατά την οποία εισέρχεται το εμπόρευμα μέσα στο τερματικό από την ξηρά προς το πλοίο, ενώ την εισαγωγή σημαίνει ότι το εμπόρευμα καταφτάνει από τη θάλασσα για να εκφορτωθεί στην ξηρά.

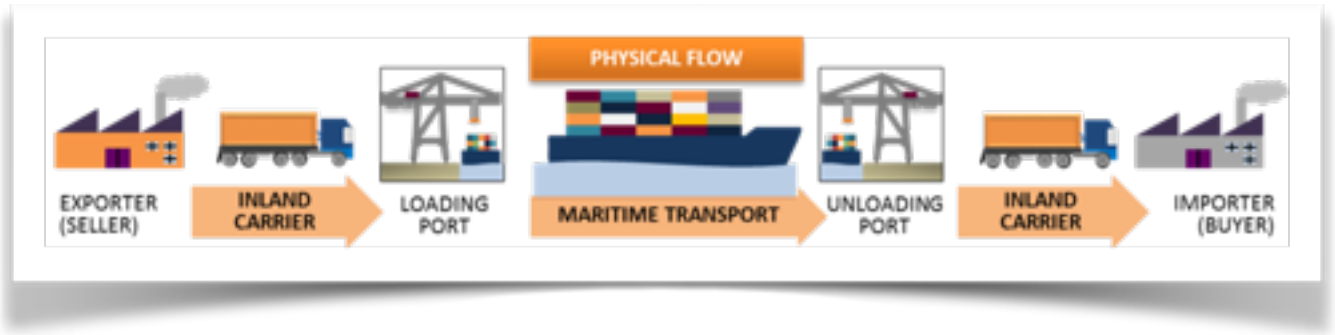
Οι κύριοι φορείς που εμπλέκονται στην αλυσίδα εφοδιασμού των εμπορευματοκιβωτίων είναι :

- Λιμεναρχεία (Port Authorities)
- Ναυτικοί πράκτορες (Ship's Agents)
- Ναυτιλιακές εταιρείες (Shipping Lines)
- Εταιρείες μεταφορών (Land Transport Companies)
- Αποθήκες εμπορευματοκιβωτίων (Empty Container Depots)
- Εμπορευματικά Κέντρα (Logistic Centers)
- φορτωτές και δέκτες (Shippers and Receivers)
- Πάροχοι των φορτοεκφορτωτών και των Τελωνείων (Provider of Dockers and Customs.)

Η διαδικασία της μεταφοράς των αγαθών μέσω εμπορευματοκιβωτίων έχει ως εξής :

Πρώτον , τα εμπορεύματα φορτώνονται στο containers και μεταφέρονται σε ένα τερματικό εμπορευματοκιβωτίων , όπου με την σειρά τους φορτώνονται στο το πλοίο. Το πλοίο αυτό, ταξιδεύει στο λιμάνι προορισμού και έπειτα και μια άλλη μεταφορική εταιρεία μεταφέρει το εμπόρευμα στην αποθήκη του δέκτη/πελάτη

Η αλυσίδα εφοδιασμού των container, συνοψίζεται έχοντας υπόψη μόνο τους φορείς που εμπλέκονται μεταξύ του κατασκευαστή των εξαγωγών (πωλητή) στον εισαγωγέα (αγοραστή) [FundaciónValenciaport, 2012]



Αλυσίδα εφοδιασμού

Η αλυσίδα εφοδιασμού των container αποτελείται από επτά πτυχές :
1. Τοποθέτηση των εμπορευμάτων σε containers σε ένα εργοστάσιο
2. Χερσαίες φορέα από το εργοστάσιο στο λιμάνι φόρτωσης
3. Παραλαβή και αποθήκευση σε ένα τερματικό σταθμό εμπορευματοκιβωτίων και την φόρτωση στο πλοίο
4. θαλάσσιες μεταφορές από το λιμένα φόρτωσης στον λιμένα εκφόρτωσης
5. Η εκφόρτωση από το πλοίο , την αποθήκευση σε ένα τερματικό σταθμό εμπορευματοκιβωτίων και παράδοση σε χερσαίο μεταφορέα
6. Μεταφορά του εμπορεύματος (container) κατά την εκφόρτωση του πλοίου στην αποθήκη (αγοραστή)
7. Η εκφόρτωση των εμπορευματοκιβωτίων / εμπορευμάτων στην αποθήκη του αγοραστή

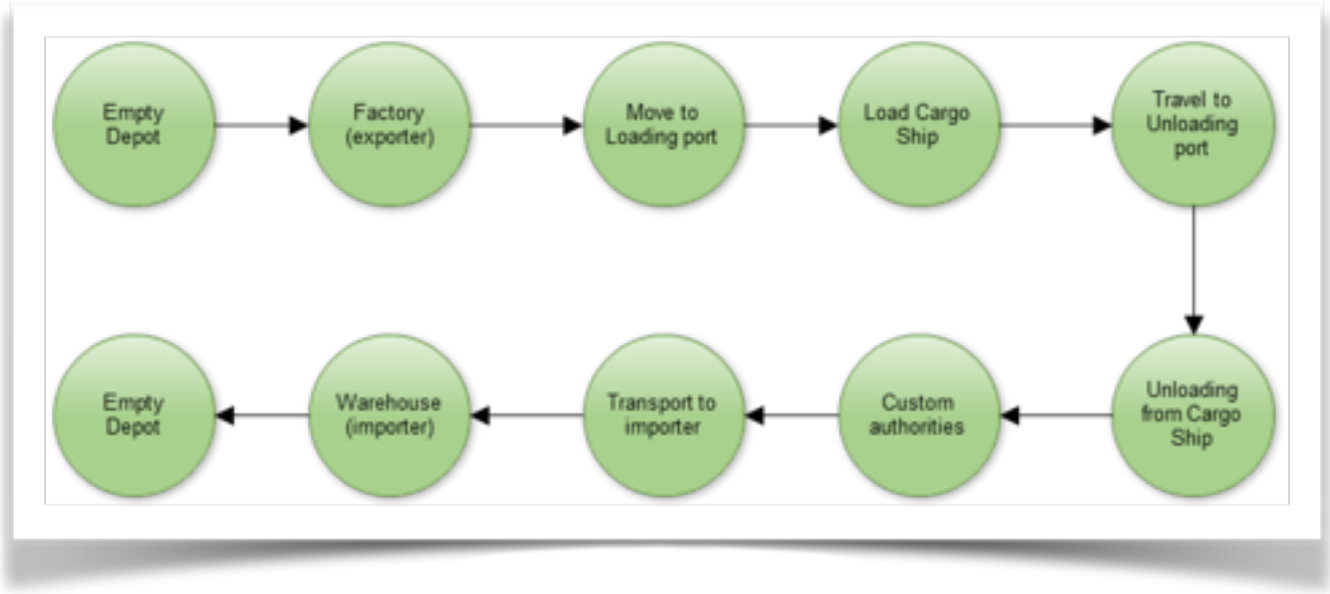
4.7 Οι ροές της αλυσίδας εφοδιασμού

Θα εξετάσουμε τρία είδη ροών στην αλυσίδα εφοδιασμού των λιμένων

1) Φυσική ροή
2) Ροή στον κυβερνοχώρο
4) Συνδυασμένη ροή

4.7.1 **Φυσική ροή** (The Physical Flow Use Case)

Σε αυτή τη περίπτωση εξετάζεται μόνο η ροή φορτίου (φυσικό επίπεδο) . Η ροή αυτή ξεκινά από το εργοστάσιο του κατασκευαστή στην ενδοχώρα του λιμένα φόρτωσης και τελειώνει με την αποθήκη του αγοραστή στην ενδοχώρα του λιμένα εκφόρτωσης . Σκοπός του είναι να εξετάσει, πώς διάφορες απειλές μπορούν να επηρεάσουν τη φυσιολογική ροή του φορτίου.

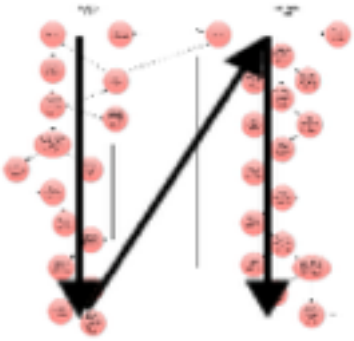


Physical Flow Use Case in Container Chain

4.7.2 **Ροή στον κυβερνοχώρο** (The Cyber Flow Use Case)

Σε αυτή τη περίπτωση εξετάζεται μόνο η ροή των πληροφοριών και εγγράφων (επίπεδο στον κυβερνοχώρο) στην συμμετοχή όλων των φορέων μεταξύ του εξαγωγέα και του εισαγωγέα .
Η ροή στον κυβερνοχώρο δεν είναι πάντα μια ευθεία γραμμή (συνεχούς ροής). Αυτό σημαίνει ότι παρόλο του υψηλού βαθμού πολυπλοκότητας της αλυσίδας εμπορευματοκιβωτίων, υπάρχουν πολλές επικοινωνίες μεταξύ των διαφόρων παραγόντων στο λιμάνι φόρτωσης και εκφόρτωσης.

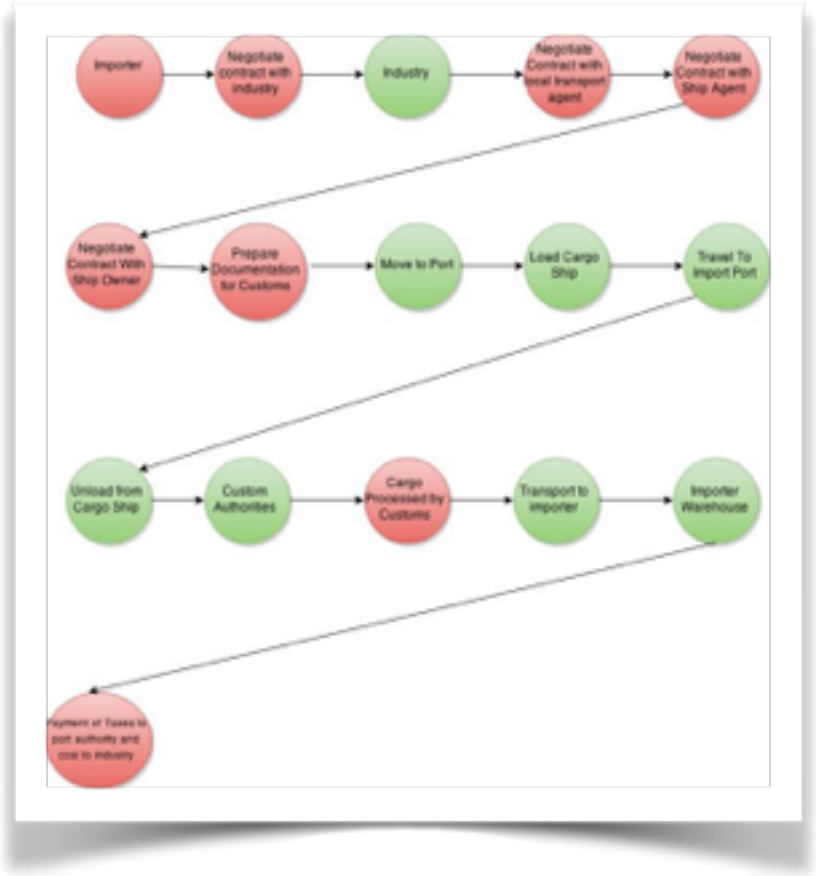
Έτσι για να καταλάβουμε τη ροή , είναι σημαντικό να παρατηρήσουμε ότι : στην αριστερή πλευρά του σχήματος , απεικονίζονται οι επικοινωνίες των φορέων που ανήκουν στον λιμένα φόρτωσης , και στο δεξί μέρος αυτοί που ανήκουν στον λιμένα εκφόρτωσης. Αν και η ροή των πληροφοριών ξεκινά με τον εισαγωγέα (δεξιά) η χρονική ακολουθία της ροής πηγαίνει από αριστερά προς τα κάτω και συνεχίζει από το δεξί μέρος προς τα κάτω. Ο σκοπός αυτής της τεχνικης είναι να εξετάσει πώς διάφορες απειλές να επηρεάσουν την κανονική ενημέρωση / ροή εγγράφων .



Cyber Flow Use Case in Container Chain

4.7.3 **Συνδυασμένη ροή** (Combined Use Case)

Σε αυτή τη περίπτωση εξετάζεται τόσο το φορτίο όσο και η ροή πληροφοριών/ εγγράφων (τόσο στον κυβερνοχώρο όσο και το φυσικό επίπεδο), που ξεκινά από μια βιομηχανία και τελειώνει με την παραλαβή του φορτίου από τον εισαγωγέα. Σκοπός του είναι να εξετάσει πώς διάφορες απειλές μπορουν να επηρεάσουν την κανονική ροή ολόκληρης της εφοδιαστικής αλυσίδας της



Combined of Vehicles Transport Use Case

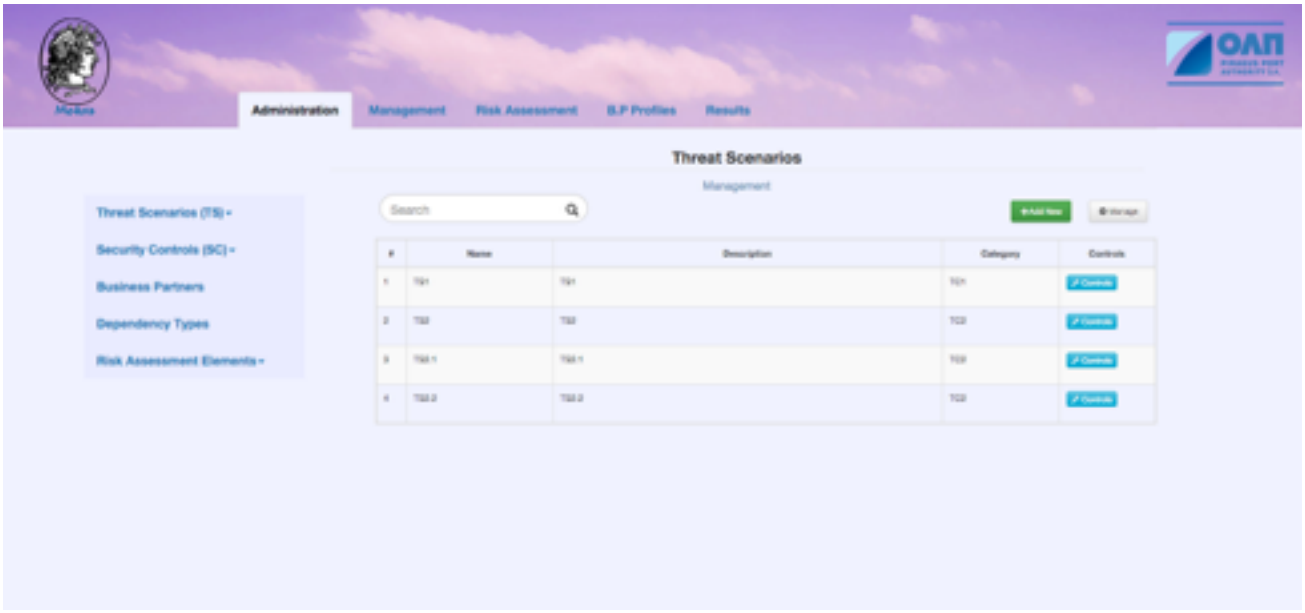
4.8 Το γραφικό περιβάλλον

Το εργαλείο Medusa, όπως και κάθε άλλο εργαλείο ανάλυσης κίνδυνων, συνεχώς ανανεώνεται, βελτιώνεται και αναβαθμίζεται, τόσο στις δυνατότητες που παρέχει στους χρήστες του, όσο και στις πληροφορίες της βάσης δεδομένων που αφορούν τις απειλές τα αντίμετρα, υποδομή κ.α

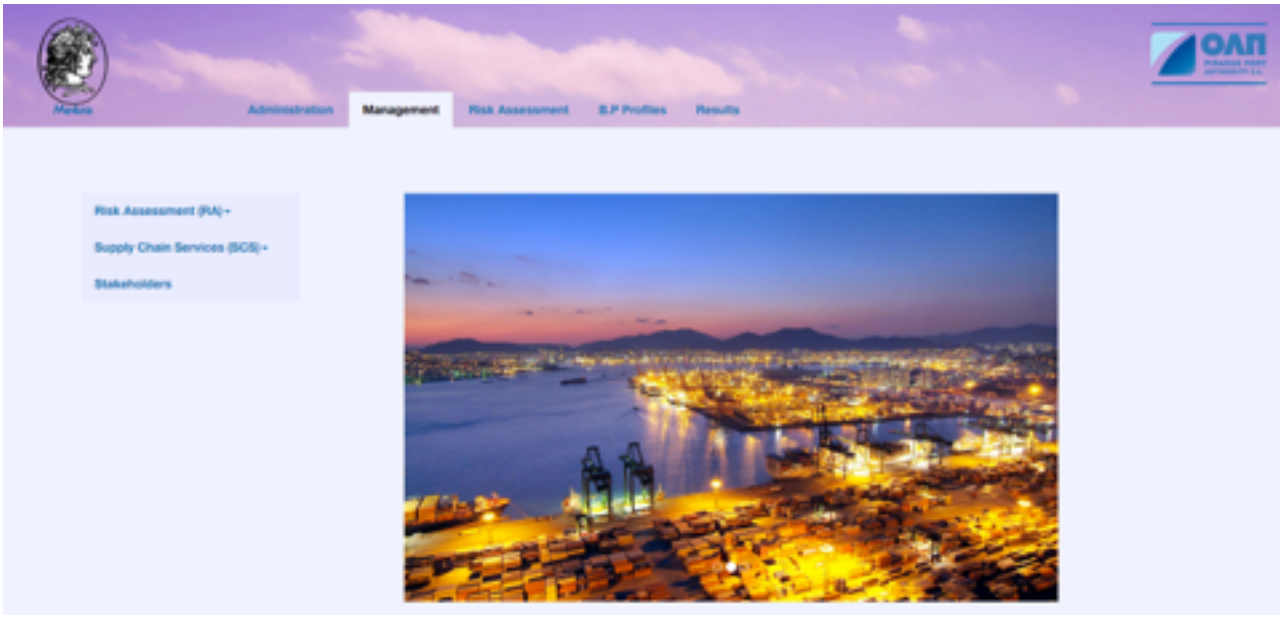
Το εργαλείο, σχεδιάστηκε να είναι όσο πιο φιλικό γίνεται στους τελικούς χρήστες, με ένα απλό γραφικό περιβάλλον για την καλύτερη κατανόηση και χρήση των υπηρεσιών του. Θα ενσωματώνει στοιχεία που έλειπαν από τον προκάτοχο του (CYSM), παρόλα αυτά θα είναι άρρητα συνδεδεμένο μαζί του. Κάποιος χρήστης θα πρέπει πρώτα να συνδεθεί στο εργαλείο CYSM, να αυθεντικοποιηθεί, και στην συνέχεια να είναι σε θέση να χρησιμοποιήσει το περιβάλλον του Medusa

Σημείωση:

Επειδή το εργαλείο είναι σε φάση προγραμματισμού και σχεδιασμού ακόμα, ορισμένα UIs ενδέχεται να αλλάξουν κατά την πορεία. Οι τιμές των πινάκων δεν έχουν ενδεικτικά και σωστά δεδομένα όπως θα είναι στην πραγματικότητα αλλά περιέχουν dummy τιμές καθώς βρισκόμαστε σε επίπεδο δοκίμων και εκτίμησης της συνολικής υπηρεσίας και η χρήση πραγματικών τιμών θα ήταν χρονοβόρα και μη πρακτική.



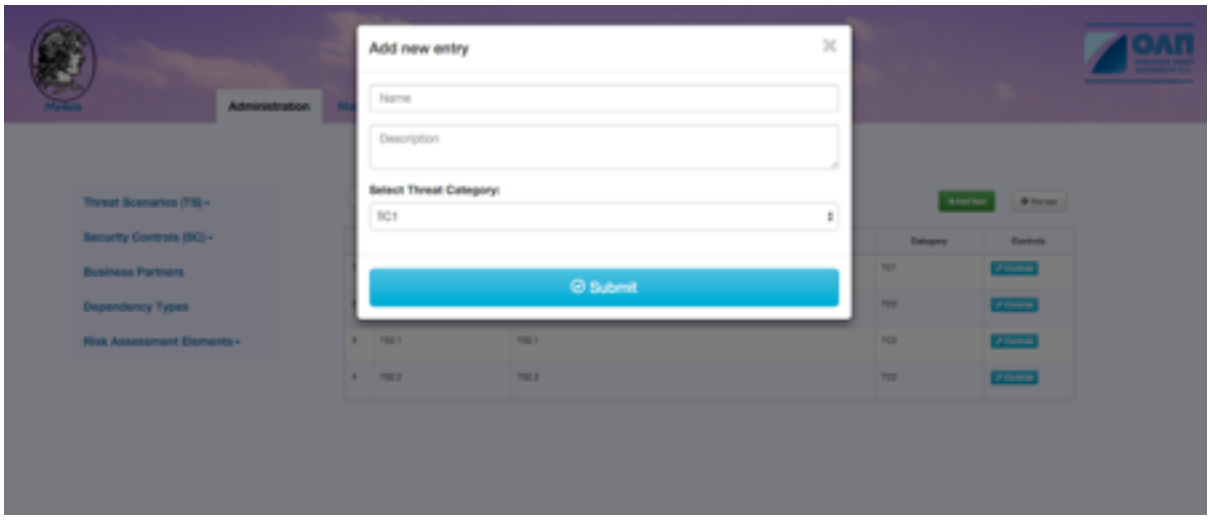
Κατηγορία Administration:
Εδώ εισάγονται οι κατηγορίες καθώς και τα threat scenarios και security controls αυτά καθαυτά. Εισάγονται επίσης οι επιχειρηματικές οντότητες (business partners) καθώς και η αρχικοποίηση των απαραίτητων στοιχείων για την διεξαγωγή της ανάλυσης κίνδυνου



Κατηγορία Management:
Εδώ γίνεται η αρχικοποίηση των αλυσίδων εφοδιασμού και των συνεργατών/ κόμβων, καθώς επίσης η αρχικοποίηση μιας νέας αξιολόγησης κινδύνου με όλους τους ενδιαφερόμενους και τα “βάρη" που έχουν κατά την αξιολόγηση

Στις κατηγορίες Risk Assessment και B.P Profiles γίνεται ο προσδιορισμός των threat scenarios και security controls ως προς το επίπεδο της εφαρμογής τους στον λιμένα που εξετάζεται.

Η εισαγωγή νέων στοιχείων γίνεται με την χρήση modal για την ευκολία του τελικού χρήστη



Δεν αντιμετωπίστηκαν σημαντικές δυσκολίες στην κατασκευή του εργαλείου Medusa. Ωστόσο έμφαση θα πρέπει να δοθεί στην προστασία και την θωράκιση του εργαλείου από όλες της γνωστές επιθέσεις web based εφαρμογών, για την προστασία των δεδομένων και την ιδιωτικότητα των χρηστών της. Η συνεχής βελτίωση των υπηρεσιών του εργαλείου, θα προσφέρει καλύτερη ασφάλεια σε ενδεχόμενες επιθέσεις, καθώς και την καλύτερη εμπειρία χρήσης των ατόμων που το χρησιμοποιούν.

Συμπεράσματα

Σε αυτήν την εργασία έγινε μία προσπάθεια να προσεγγισθεί ολιστικά το θέμα της ασφάλειας στους εμπορικούς λιμένες. Αρχικά περιγράφηκε το φυσικό περιβάλλον και οι εγκαταστάσεις ενός εμπορικού λιμένα, έπειτα προχωρήσαμε στον ορισμό του ΤΠΕ περιβαλλοντός του, αναλύοντας την αρχιτεκτονική αυτού, τα στρώματα που το αποτελούν, τις υπηρεσίες που προσφέρει και τους χρήστες του. Η εργασία συνεχίζεται με την καταγραφή των σημαντικότερων παγκόσμιων, ευρωπαικών και εθνικών οργανισμών και φορέων που δραστηριοποιούνται στον τομέα της ασφάλειας, όλων των βασικών σχετικών νομοθετικών πλαισίων, των υφιστάμενων σχεδίων ασφάλειας και των σημαντικότερων αντίστοιχων προτύπων που υπάρχουν. Στη συνέχεια παρουσιάζεται συνοπτικά ορισμένα άλλα εργαλεία και έπειτα το εργαλείο που αναπτύχθηκε.

Παρατηρείται πως οι περισσότεροι κανονισμοί που σχετίζονται με την ασφάλεια των λιμένων περιλαμβάνουν διατάξεις μόνο για την φυσική ασφάλεια και δεν θεωρούν της επιθέσεις στον κυβερνοχώρο πιθανές απειλές από σκόπιμες παράνομες πράξεις, παραλείποντας εντελώς από τις διατάξεις τους την ασφάλεια του Κυβερνοχώρου των λιμενικών εγκαταστάσεων.

Ενώ πολλά λιμάνια εφαρμόζουν κάποια χαμηλού επιπέδου μέτρα προστασίας που αφορούν την ασφάλεια δεδομένων και τοπικών δικτύων δεν έχουν υπό έλεγχο όλα τα πληροφοριακά συστήματα που είναι εξαρτόμενα από τα λιμενικά συστήματα παραβλέποντας την πολυπλοκότητα των ΤΠΕ λιμενικών συστημάτων. Τα περισσότερα λιμάνια επιδεικνύουν χαμηλά επίπεδα γνώσης αναφορικά με την ασφάλεια στον κυβερνοχώρο. Το πρόβλημα αυτό μπορεί να επιλυθεί με την οργάνωση παγκόσμιων, ευρωπαϊκών και εθνικών εκστρατειών επιμόρφωσης επί του θέματος. Η παρούσα εργασία θα μπορούσε να χρησιμοποιηθεί για να εισάγει τις βάσεις μίας τέτοιας εκστρατείας.

Άλλο σημαντικό συμπέρασμα είναι πως υπάρχει έλλειψη τυποποίησης της ΤΠΕ ασφάλειας των εμπορικών λιμένων με αποτέλεσμα οι εμπλεκόμενοι φορείς να μην γνωρίζουν τα υπάρχοντα μέτρα ασφάλειας που θα μπορούσαν να υλοποιήσουν για να διασφαλίσουν την ασφάλεια των ΤΠΕ συστημάτων τους. Επιπλέον, οι λιμένες εφόσον για την λειτουργία τους στηρίζονται σε ΤΠΕ συστήματα θα έπρεπε να θεωρούνται Κρίσιμες Υποδομές και να προστατεύονται από τους αντίστοιχους κανονισμούς και πρότυπα. Σε αυτήν την περίπτωση θα μπορούσε να χρησιμοποιηθεί για την τυποποίηση της ασφάλειάς τους ένας συνδυασμός των υφιστάμενων ΤΠΕ προτύπων και προτύπων προστασίας πληροφοριακών υποδομών ζωτικής σημασίας (CIIP standards).

Ενώ υπάρχουν διάφοροι οργανισμοί που ασχολούνται με την ασφάλεια δεν προκύπτει από κάπου πως αυτοί συντονίζουν τις προσπάθειες τους για να αντιμετωπίσουν τις προκλήσεις ασφάλειας που συναντά ένας εμπορικός λιμένας στην εποχή της πληροφορίας και της τεχνολογίας. Κρίνεται επιτακτική η ανάγκη ύπαρξης ενός συγκεκριμένου φορέα επιφορτισμένου με αυτή την ιδιότητα και με γενικότερες ευθύνες για την ασφάλεια στον κυβερνοχώρο των λιμένων. Η συγκεκριμένη μελέτη θα μπορούσε να χρησιμοποιηθεί ως σημείο αναφοράς για τις ευθύνες που θα μπορούσε να έχει ένας τέτοιος φορέας.

Από την μελέτη προκύπτει, η ανάγκη για μία μέθοδο ή έναν τρόπο που αξιολογεί ολιστικά την ασφάλεια ενός εμπορικού λιμένα. Για να καλύψουμε αυτήν την ανάγκη, δημιουργήθηκε το εργαλείο Medusa ως διαδικτυακή εφαρμογή. Η εφαρμογή του, σε έναν εμπορικό λιμένα, μπορεί να αξιολογήσει το επίπεδο της ασφάλειάς του και να ελέγξει την συμμόρφωσή του τόσο με των διεθνή κώδικα ασφάλειας όσο και με πρότυπο τυποποίησης. Η εφαρμογή δίνει στον χρήστη, ο οποίος μπορεί να είναι ένας υπάλληλος ασφάλειας του λιμένα ή ένας διαπιστευμένος ελεγκτής ασφάλειας, την δυνατότητα να εκτελέσει μια μεθοδολογία για την εκτίμηση των κινδύνων.

Τέλος, η αποστολή της διασφάλισης της ‘κυβερνοασφάλειας’ είναι η πιο σημαντική πρόκληση της δεκαετίας για την ασφάλεια των θαλάσσιων λιμένων και είναι σημαντικό όλοι οι εμπλεκόμενοι φορείς να συντονίσουν τις προσπάθειές τους για την εξονυχιστική διερεύνηση και την επίτευξή της.

Βιβλιογραφία

[0] Σ. Κάτσικας, "Ο ΔΕΚΑΛΟΓΟΣ...για θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων στο Ηλεκτρονικό Επιχειρείν"

[1] Δικτυακός τόπος: http://www.hcg.gr/node/65

[2] Εφαρμογή του Κώδικα ISP, Δικτυακός τόπος: http://www.econews.gr/2004/06/23/code-isps/

[3] Δικτυακός τόπος: http://blogthea.gr/internet/6648-χάρτης-πλοίων-πραγματικού-χρόνου-από-δορυφόρο-ais.html

[4] Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών
Δικτυακός τόπος: http://www.tuv-nord.com/gr/el/information-technology/iso-27001-2008-444.htm

[5] Δικτυακός τόπος: http://www.insilico.gr/index.php?option=com_content&view=category&id=80&Itemid=472

[6] Ευρωπαικος οργανισμος για την ασφαλεια και υγεια στην εργασια
Δικτυακός τόπος: https://osha.europa.eu/el/topics/riskassessment/index_html/carry_out

[7] Γεώργιος Νικήτας, "Αναλυση κινδυνων πληροφοριακων συστηματων"

[8] ENISA, Δικτυακός τόπος: http://rm-inv.enisa.europa.eu/methods/m_cramm.html

[9] Ιωάννης Καλογερόπουλος, " Ανάλυση Επικινδυνότητας του Πληροφοριακού Συστήματος Ασφαλιστικής Εταιρίας Πιστώσεων με τη χρήση του Ebios"

[10] Ευτυχία Χαλβατζή, "Συγκριτική Μελέτη Ανάλυσης Επικινδυνότητας"

[11] Δικτυακός τόπος: http://www.physics.ntua.gr/~zamarias/nees_tech/what_is_HTML.html

[12] Δικτυακός τόπος: http://pages.cs.aueb.gr/courses/epl131/files/CSS_notes.pdf

[13] Γιώργος Καμπουράκης, "Εισαγωγή στην ασφάλεια Πληροφοριακών και

Επικοινωνιακών Συστημάτων"

[14] Δικτυακός τόπος CALLIO: www.callio.com

[15] Δικτυακός τόπος CRAMM: www.cramm.com

[16] Δικτυακός τόπος Risk Watch: www.riskwatch.com

[17] Παρδάλη Αγγελική. Η λιμενική βιομηχανία. Αθήνα: Σταμούλης, 2001

[18] Εφημερίδα της Κυβερνήσεως, Τεύχος Πρώτο, Αρ. Φύλλου 281. ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3622. Ενίσχυση της ασφάλειας πλοίων, λιμενικών εγκαταστάσεων και λιμένων και άλλες διατάξεις. 20 Δεκεμβρίου 2007

[19] International Maritime Organization. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). Δικτυακός τόπος: http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for-Seafarers-(STCW).aspx

[20] International Maritime Organization. International Convention on Maritime Search and Rescue (SAR). Δικτυακός τόπος: http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-on-Maritime-Search-and-Rescue-(SAR).aspx

[21] Paris MoU. A short history of the Paris MoU on PSC. Δικτυακός τόπος: https://www.parismou.org/about-us/history

[22] European Maritime Safety Agency (EMSA). Maritime Security Overview. Δικτυακός τόπος: http://emsa.europa.eu/implementation-tasks/visits-and-inspections/maritime-security.html

[23] European Commission. EU legislation on Maritime Security. [online] Δικτυακός τόπος: http://ec.europa.eu/transport/modes/maritime/security/doc/legislation_maritime_security.pdf

[24] European Union Agency for Network and Information Security (enisa), 2011. Maritime Cyber Security Workshop in Brussels Δικτυακός τόπος: https://www.enisa.europa.eu/media/news-items/cyber-security-in-the-maritime-sector-workshop-in-brussels

[25] Europa (Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης), 2002. Θαλάσσια ασφάλεια: Ευρωπαϊκός Οργανισμός για την ασφάλεια στη θάλασσα. Δικτυακός τόπος:
http://europa.eu/legislation_summaries/institutional_affairs/institutions_bodies_and_agencies/l24245_el.htm

[26] Υπουργείο Ναυτιλίας και Αιγαίου. Νομοθεσία, Νόμοι - ΠΔ. Δικτυακός τόπος:
http://www.yen.gr/wide/yen.chtm?prnbr=24729

[27] CYSM. Collaborative Cyber/Physical Security Management System. Δικτυακός τόπος:
http://www.cysm.eu/index.php/en/