Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.
Σχολή Τεχνολογικών Εφαρμογών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Διαχείριση Ασφάλειας των Τεχνολογιών Πληροφορικής και Επικοινωνιών συστήματα λιμένων (PICT)

Επιβλέπων Καθηγητής: .....

Φοιτητής: Καπαρέλος Χρήστος

Ονοματεπώνυμο *ΑΜ: 2009050*

Σπάρτη, Μάιος 2014

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ **ΥΠΟΓΡΑΦΕΣ**

1.

2.

3.

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής Τ.Ε. του Τ.Ε.Ι. Πελοποννήσου.

Ο συγγραφέας,

Χρήστος Γ. Καπαρέλος

Ευχαριστίες

Ξεκινώντας αυτή την Πτυχιακή Εργασία θα ήθελα να ευχαριστήσω ιδιαίτερα τον υπεύθυνο καθηγητή της Εργασίας μου κύριο ..... για την πολύτιμη βοήθεια του τόσο σε συμβουλευτικό επίπεδο όσο και για την πληθώρα πληροφοριών που μου παρείχε προκειμένου να καταφέρω να αποπερατώσω την εργασία μου.

Επίσης να ευχαριστήσω όλους τους καθηγητές του τμήματος Μηχανικών Πληροφορικής Τ.Ε. του Τ.Ε.Ι. Πελοποννήσου, τόσο για τις γενικές γνώσεις που μου παρείχαν όσο και για τις χρήσιμες πληροφορίες που μου παρείχαν όταν της ζήτησα.

Τέλος να ευχαριστήσω όσους συναδέρφους – συμφοιτητές με βοήθησαν στην διαδικτιακή αναζήτηση των πληροφοριών με σκοπό την αποπεράτωση αυτής της εργασίας.

Περιεχόμενα

Περιεχόμενα Πινάκων

Περιεχόμενα Σχημάτων

Περίληψη

Το οικοσύστημα στη θάλασσα είναι πολύπλοκο και περιλαμβάνει πολλές οντότητες που αλληλεπιδρούν μεταξύ τους. Παραδείγματα αυτών των φορέων είναι οι λιμένες, τα πλοία, οι λιμενικές αρχές, οι ναυτιλιακές και οι ασφαλιστικές εταιρείες, τα τελωνεία, η βιομηχανία πλοίων, οι τράπεζες, τα υπουργεία, άλλοι πάροχοι εμπορικών και λοιπών υποδομών (π.χ. σιδηρόδρομοι, αεροδρόμια). Όλες αυτές οι αλληλεπιδράσεις υποστηρίζονται από πολύπλοκα και ετερογενή συστήματα τεχνολογίας πληροφοριών και επικοινωνιών (ICT).

Οι εμπορικοί λιμένες συγκαταλέγονται μεταξύ των υποδομών μεταφοράς πληροφοριών ζωτικής σημασίας (CII), δεδομένου ότι πρόκειται για υποδομές μεγάλης κλίμακας, η υποβάθμιση των οποίων, καθώς και η διακοπή ή δυσλειτουργία των συστημάτων τους τύπου ICT έχει σοβαρές συνέπειες για την εθνική ασφάλεια, την υγεία, την ασφάλεια, την οικονομία και την ευημερία των πολιτών και των λαών και χαρακτηρίζεται από την πολλαπλότητα των αλληλεξαρτήσεων με άλλους φορείς, στο ναυτιλιακό οικοσύστημα.

Η κανονική λειτουργία των εμπορικών λιμένων εξαρτάται, σε μεγάλο βαθμό, από την ορθή λειτουργία των συστημάτων τους τύπου ICT. Η μεγάλη ποσότητα των κρίσιμων και ευαίσθητων δεδομένων, των πληροφοριών και των υπηρεσιών που διαχειρίζονται σε καθημερινή βάση, ο μεγάλος αριθμός των φορέων που καλούνται να εξυπηρετηθούν και οι αλληλεξαρτήσεις με άλλες υποδομές απαιτούν αποτελεσματική διαχείριση της ασφάλειας.

Ωστόσο, η ισχύουσα νομοθεσία ναυσιπλοΐας και η τυποποίηση των προσπαθειών και πρακτικών δεν καλύπτουν επαρκώς την ασφάλεια τύπου ICT των εμπορικών λιμένων. Επικεντρώνεται μόνο στην ασφάλεια των λιμένων, αφήνοντας έτσι τα ηλεκτρονικά τους δεδομένα και υπηρεσίες εκτεθιμένες σε καθημερινώς αυξανόμενες απειλές, στον κυβερνοχώρο τους.

Ο ENISA έχει ήδη δημοσιεύσει μια αρχική μελέτη σχετικά με την ασφάλεια στον κυβερνοχώρο, στον τομέα των θαλάσσιων μεταφορών [19], εντοπίζοντας την σημασία της εξέτασης και ενεργώντας, κατόπιν, με βάση τις πτυχές ασφάλειας τύπου

ICT, στον τομέα της ναυτιλίας. Μια από τις βασικές συστάσεις της έκθεσης είναι η ανάγκη μίας ολιστικής, βασισμένης στον κίνδυνο, προσέγγισης, όταν πρόκειται για την αξιολόγηση των απειλών κατά του κυβερνοχώρου, στον τομέα της ναυτιλίας. Η έκθεση αυτή αντανακλά την σύσταση αυτή και διερευνά τις προκλήσεις μιας τέτοιας προσέγγισης. Δεν φιλοδοξεί να προσφέρει νέες λύσεις σε αυτά τα προβλήματα που έχουν ήδη εντοπιστεί, αλλά προσπαθεί να πάει ένα βήμα μπροστά από τον εντοπισμό των κενών στις υφιστάμενες προσπάθειες, αναφορικά με την διαχείριση της ασφάλειας των λιμένων CII, εφιστώντας προτάσεις, ερευνητικές κατευθύνσεις και συστάσεις.

Με βάση την ανασκόπηση της βιβλιογραφίας, έχουμε εντοπίσει τα κενά στους ακόλουθους τομείς:

Ορθές πρακτικές: Οι λιμένες δεν υιοθετούν "καλές πρακτικές ασφαλείας τύπου ICT", δηλαδή δεν αντιμετωπίζουν αποτελεσματικά, με βάση την ασφάλεια τύπου ICT (π.χ. επιθέσεις, μεταμφιεσμένες ταυτότητες, παρακολούθηση της κυκλοφορίας του δικτύου, κλοπή / τροποποίηση των δεδομένων προσωπικού χαρακτήρα), προκαλώντας τεράστια ζημιά και θέτοντας σε κίνδυνο (π.χ. απώλεια φήμης, απώλεια της νομικής συμμόρφωσης, και διακοπή της λειτουργίας των επιχειρήσεων), όχι μόνο τα ίδια συμφέροντα, αλλά το σύνολο των επιχειρήσεων της αλυσίδας. Οι λιμένες πρέπει να βελτιώσουν την κουλτούρα της ασφάλειας, συνειδητοποιώντας την αξία της ασφάλειας των πληροφοριών, ως μέσο υποστήριξης των επιχειρηματικών μοντέλων τους, των τρεχόντων και των μελλοντικών επιχειρηματικών σχεδίων.

Διαλειτουργικότητα και πιστοποίηση: Δυστυχώς, οι συνειδητές υπηρεσίες διασυνοριακής ασφάλειας δεν προσφέρονται από τους λιμένες της ΕΕ -βοηθώντας τους να αυξήσουν την εμπιστοσύνη τους στην ανταγωνιστική, νέα εποχή, τις ψηφιακές θαλάσσιες αγορές και να ενισχύσουν τις επιχειρησιακές τους ευκαιρίες- επειδή τα θέματα πιστοποίησης και της διαλειτουργικότητας δεν έχουν επιλυθεί. Οι διασταυρούμενες αναγνωρισμένες αρχές πιστοποίησης, για τον ναυτιλιακό τομέα πρέπει να είναι εγκατεστημένες στην ΕΕ, ώστε οι ναυτιλιακοί έταιροι να είναι σε θέση να υπογράψουν, με ψηφιακό τρόπο, ηλεκτρονικά κρίσιμα λιμενικά έγγραφα (διασφαλίζοντας την ακεραιότητα και την αυθεντικότητα τους), σε εθνικό και ευρωπαϊκό επίπεδο. Η έλλειψη προστασίας, διαλειτουργικότητας και η

διασταυρούμενη πιστοποίηση είναι τα κύρια εμπόδια στη διασυνοριακή παροχή υπηρεσιών ηλεκτρονικού λιμένος. Οι συνεργατικές δράσεις μεταξύ όλων των φορέων απαιτούνται για την επίλυση αυτών των προβλημάτων.

Μεθοδολογίες διαχείρισης της ασφάλειας: Οι υφιστάμενες μεθοδολογίες διαχείρισης της ναυτιλιακής ασφάλειας και τα εργαλεία δεν αντιμετωπίζουν την διαχείριση της ασφάλειας, στις Τεχνολογίες Πληροφορίας και Επικοινωνίας των λιμένων (PICT). Τα υφιστάμενα πρότυπα ICT και CIIP μπορούν να συνδυαστούν με τα ISPS και να τροποποιηθούν, ώστε να καλύπτουν επαρκώς τη διαχείριση προστασίας PICT, ενώ, την ίδια στιγμή, αποφεύγονται οι χρονοβόρες προσπάθειες, για τη δημιουργία νέων προτύπων ναυτικής ασφάλειας στον κυβερνοχώρο. Μια ολιστική προσέγγιση, για την διαχείριση προστασίας των συστημάτων PICT, που προτείνεται σε αυτή την εργασία είναι η δημιουργία / ενίσχυση των θαλάσσιων στοχευμένων μεθοδολογιών διαχείρισης της προστασίας, οι οποίες είναι συμβατές με: τον κώδικα ISPS, τον τροποποιημένο ICT και τα πρότυπα διαχείρισης προστασίας CCIP. Επιπλέον, έχουμε εντοπίσει βελτιώσεις που απαιτούνται σε:

- *εκτίμηση κρισιμότητας της υπηρεσίας e-port:* Τα συστήματα Τεχνολογίας Πληροφοριας και Επικοινωνίας των λιμένων (PICT) προσφέρουν μια πληθώρα ηλεκτρονικών υπηρεσιών (ηλεκτρονικών λιμενικών υπηρεσιών), οι οποίες: α) ανταλλάσουν και αποθηκεύουν τα ηλεκτρονικά δεδομένα, μέσω περίπλοκων διαδικασιών και β) αλληλεπιδρούν με πολλούς φορείς. Η κρισιμότητα αυτών των υπηρεσιών και των τεχνολογιών που χρησιμοποιούνται (π.χ. οι RFID), πρέπει να αξιολογείται και τα κατάλληλα μέτρα ασφαλείας πρέπει να εφαρμοστούν, προκειμένου να αποφευχθούν οι καταστροφικές συνέπειες (π.χ. εμπορική κατασκοπεία, τρομοκρατικές επιθέσεις στον κυβερνοχώρο), όχι μόνο στο ναυτιλιακό περιβάλλον, αλλά και σε ολόκληρο το ευρωπαϊκό επιχειρηματικό οικοσύστημα.

- *Αυτοματοποιημένα εργαλεία υποστήριξης:* Αυτές οι νέες μέθοδοι θα πρέπει να υποστηρίζονται από καινοτόμα, συνεργατικά, φιλικά προς τον χρήστη εργαλεία, τα οποία η ομάδα ασφάλειας PICT μπορεί να χρησιμοποιήσει εύκολα και αποτελεσματικά, έτσι ώστε να συνεργάζονται και

να παρακολουθούν συνεχώς, να διαχειρίζονται και να ελέγχουν την ασφάλεια των συστημάτων PICT τους.

Η οικονομική κρίση μπορεί να αμφισβητήσει το γεγονός ότι οι λιμένες είναι σε θέση να επενδύσουν στην παροχή ασφαλών, ηλεκτρονικών λιμενικών διασυνοριακών υπηρεσιών. Οι ναυτιλιακές υπηρεσίες νέφους μπορούν να παρέχουν μια λύση για την υπέρβαση αυτού του εμποδίου. Οι ναυτιλιακές υπηρεσίες νέφους, σε εθνικό ή κοινοτικό επίπεδο, θα είναι μια οικονομικά αποδοτική προσέγγιση για την εξασφάλιση των διασυνοριακών, αξιόπιστων υπηρεσιών ηλεκτρονικού λιμένος.

Η έξαρση των κυρίων εμποδίων της ασφάλειας και της διαλειτουργικότητας θα συμβάλει στην υλοποίηση μιας ενοποιημένης ναυτιλιακής πολιτικής στην Ευρώπη. Τα διαθέσιμα μέσα της Ευρωπαϊκή Κοινότητας πρέπει να κινητοποιηθούν, προκειμένου να συμβάλουν προς αυτή την κατεύθυνση. Η ιδιωτικοποίηση των λιμένων της ΕΕ επιβάλλει ακόμη περισσότερο την επείγουσα ανάγκη για την περαιτέρω προστασία των συστημάτων PICT, σύμφωνα με τη νομοθεσία και τον κανονισμό ασφάλειας της ΕΕ, αποφεύγοντας την εμπορική ξένη κατασκοπεία.

Κεφάλαιο 1: Εισαγωγή

Το τραγικό δυστύχημα του Τιτανικού (1912) επέβαλε τη νέα έννοια της "ασφάλειας", στον τομέα της ναυτιλίας. Πολλές νομοθεσίες και οδηγίες που δημοσιεύθηκαν έκτοτε επικεντρώνονται στην φυσική προστασία των πλοίων, του πληρώματος, των επιβατών, του φορτίου και της θάλασσας.

Οι τρομοκρατικές επιθέσεις στη Νέα Υόρκη και την Ουάσιγκτον (2001), την Μαδρίτη (2004) και το Λονδίνο (2005), επέβαλαν την έννοια της *«ασφάλειας»* με πρόσθετες οδηγίες και νομοθεσία (π.χ. ο Διεθνής Κώδικας Προστασίας των Πλοίων και Παροχών Λιμένων ISPS). Παρά το γεγονός ότι αυτές οι νέες προσπάθειες επικεντρώθηκαν στις οργανωτικές και τις πτυχές ελέγχου της φυσικής ασφάλειας των πλοίων, οι ναυτιλιακές εταιρείες και οι εμπορικοί λιμένες δεν έχουν λάβει υπόψη την ICT και τις απειλές, για την ασφάλεια στον κυβερνοχώρο και τους κινδύνους. Το ναυάγιο στην Ιταλία (2012) ήταν μια φυσική συνέπεια αυτής της άγνοιας, δεδομένου ότι διαπιστώθηκε πως η επικοινωνία μεταξύ των λιμένων και των πλοίων δεν ήταν αξιόπιστη, τα συστήματα πλοήγησης και γραμμής ακτών δεν λειτουργούν σωστά και ένα σχέδιο αποκατάστασης των καταστροφών δεν εφαρμόστηκε. Με άλλα λόγια, δεν καλύφθηκαν πολλές πτυχές της ασφάλειας ICT.

Τον Δεκέμβριο του 2011, ο ENISA [19] δημοσίευσε μια έκθεση στην οποία αναλύονται οι προκλήσεις για την ασφάλεια στον κυβερνοχώρο στην Ναυτιλία. Η έκθεση αυτή, που παρουσιάζει τα αποτελέσματα από το εργαστήριο του ENISA [18] για το θέμα αυτό, επικεντρώνεται στην ασφάλεια ICT των λιμένων και, ειδικότερα, στη διαχείριση της ασφάλειας των τεχνολογιών της πληροφορίας και των λιμενικών συστημάτων (PICT). Η εκπληκτική παρατήρηση, όπως αναφέρεται στην έκθεση ήταν ότι *«η ευαισθητοποίηση στον κυβερνοχώρο σχετικά με τις ανάγκες και τις προκλήσεις στον τομέα της ναυτιλίας της ασφάλειας είναι σήμερα χαμηλή έως ανύπαρκτη»*. Παρά το γεγονός ότι οι πτυχές που αφορούν την ασφάλεια (π.χ. φυσική ασφάλεια) θεωρούνται μέσω του κώδικα ISPS, αγνοείται η ασφάλεια PICT. Διάφορες προτάσεις και λύσεις που παρέχονταν στην έκθεση ηταν οι εξής:

"Σας συνιστούμε ότι μια ολιστική προσέγγιση, με βάση τον κίνδυνο, θα απαιτούσε την αξιολόγηση των υφιστάμενων κινδύνων στον κυβερνοχώρο, που σχετίζονται με τις τρέχουσες εφαρμογές συστημάτων ICT, σχετικά με τοη ευρωπαϊκό ναυτιλιακό τομέα, καθώς και την αναγνώριση όλων των κρίσιμων στοιχείων του ενεργητικού, στον τομέα αυτό. Για τους οικονομικούς φορείς της ναυτιλίας και τα ενδιαφερόμενα μέρη, είναι σημαντικό να εφαρμόζονται προληπτικά μέτρα στον κυβερνοχώρο, καθώς και οι αρχές διαχείρισης κινδύνων ασφάλειας πληροφοριών μέσα στους οργανισμούς και το περιβάλλον τους »,

Στην παρούσα εργασία, θα ακολουθήσει η περαιτέρω ανάλυση αυτής της σύστασης. Έχουμε επικεντρωθεί στην "Διαχείρισης Ασφάλειας των Συστημάτων PICT" δεδομένου ότι το ευρωπαϊκό εμπόριο και οι διασυνοριακές συναλλαγές εξαρτώνται, σε μεγάλο βαθμό, από την ασφαλή λειτουργία των εμπορικών λιμένων. Είναι ζωτικής σημασίας υποδομές και σε αυτή την έκθεση θα πρέπει να αντιμετωπίζονται ως τέτοια.

Αυτή η εργασία έχει ως στόχο να βρει τις απαντήσεις στις ακόλουθες ερωτήσεις:

1. Ποιες είναι οι σχετικές προσπάθειες της ναυτιλιακής κοινότητας που σχετίζονται με την ασφάλεια; Ποια είναι τα κενά και ποια τα ανοιχτά ζητήματα;

2. Πώς ορίζεται ένα σύστημα PICT;

3. Ποια πρότυπα διαχείρισης προστασίας και μεθοδολογίες μπορούν να εφαρμοστούν στα συστήματα PICT και ποιές τροποποιήσεις απαιτούνται;

4. Πώς μπορούν τα πρότυπα και οι κατευθύνσεις της Ευρωπαϊκής Υποδομής Ζωτικής Σημασίας (ECI) να χρησιμεύσουν ως κατευθυντήριες γραμμές για τις βελτιώσεις της προστασίας, στους εμπορικούς λιμένες;

5. Τα εργαλεία διαχείρισης της προστασίας μπορούν να χρησιμοποιηθούν αποτελεσματικά για την διαχείριση, την παρακολούθηση και τον έλεγχο των συστημάτων PICT. Τι είδους τεχνικά και λειτουργικά χαρακτηριστικά θα πρέπει να έχουν τα εργαλεία αυτά;

6. Ποια είναι τα ενδιαφερόμενα μέρη και ποιοι οι σχετικοί φορείς, στον τομέα της ναυτιλίας, που θα πρέπει να συμμετέχουν στην ευαισθητοποίηση, αυξάνοντας την προστασία του κυβερνοχώρου και του IT των συστημάτων PICT, καθώς και στο σχεδιασμό των ασφαλών συστημάτων PICT;

Στην εργασία αυτή, οι εμπορικοί λιμένες θεωρούνται υποδομές πληροφοριών ζωτικής σημασίας (CII), φιλοξενώντας έτσι κρίσιμα συστήματα ICT, που προσφέρουν κρίσιμες υπηρεσίες και επιβάλλουν πρόσθετες απαιτήσεις ασφαλείας (π.χ. εμπιστευτική ακεραιότητα, αυθεντικότητα και διαθεσιμότητα των δεδομένων και των χρηστών). Για το λόγο αυτό, συνιστούμε ώστε τα ευρωπαϊκά λιμάνια να ακολουθούν την προστασία ICT, τα πρότυπα και τις οδηγίες ασφαλείας CIIP, καθώς και κοινές μεθοδολογίες ασφάλειας και πρακτικές, αντι των εμπορικών προσεγγίσεων στις οποίες βασίζονται γι' αυτόν τον σκοπό. Μια ολιστική προσέγγιση της διαχείρισης της ασφάλειας της ΕΕ, στον τομέα των ICT, και η προστασία στον κυβερνοχώρο των συστημάτων PICT πρέπει να υιοθετηθούν, προκειμένου να οικοδομήσουμε ένα έμπιστο, διαλειτουργικό ναυτιλιακό περιβάλλον της ΕΕ, επιτρέποντας να προσφέρουμε τις διασυνοριακές, ασφαλείς και συνειδητές, για την ιδιωτική ζωή, υπηρεσίες ηλεκτρονικού λιμένος, σε όλους τους ναυτιλιακούς εταίρους.

Τα παραπάνω ερωτήματα έχουν ληφθεί υπόψη και εξετάζονται στα επόμενα κεφάλαια.

Η παρούσα εργασία αποτελείται από: το σώμα-πυρήνα και δύο παραρτήματα (περιγραφή των πιο γνωστών μεθοδολογιών διαχείρισης προστασίας ICT, ναυτιλιακά πρότυπα, πρωτοβουλίες και μεθοδολογίες αξιολόγησης του κινδύνου).

Κεφάλαιο 2: Λιμένες στην κοινωνία της πληροφορίας

Όπως ορίστηκε από το Ευρωπαϊκό Συμβούλιο (2008), μια **κρίσιμη υποδομή** (CI) είναι ένα *«επενδυτικό αγαθό, σύστημα ή μέρος, το οποίο είναι απαραίτητο για την διατήρηση των ζωτικών λειτουργιών της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των ανθρώπων, και η βλάβη ή η καταστροφή των οποίων θα έχει σημαντικές επιπτώσεις, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών »*.

Στη σημερινή κοινωνία, η ανάπτυξη προηγμένων πληροφοριακών συστημάτων και η διάδοση και ταχεία εξέλιξη των υποδομών ευρυζωνικών επικοινωνιών, προκάλεσαν την ευρεία υιοθέτηση της τεχνολογίας των επικοινωνιών (ICT), από όλες τις υποδομές ζωτικής σημασίας (CI). Η υποβάθμιση, βλάβη ή καταστροφή των υποδομών αυτών θα έχουν σοβαρό αντίκτυπο στην καθημερινή ζωή των πολιτών. Στη συνέχεια, οι διαδικασίες ανταλλαγής πληροφοριών που υποστηρίζονται από τις ICT, αποτελώντας υποδομές ζωτικής σημασίας, για τον εαυτό τους ή όντας κρίσιμης σημασίας, για τη λειτουργία των άλλων κρίσιμων υποδομών, ορίζονται ως *υποδομές πληροφοριών ζωτικής σημασίας* (CII).

Οι εμπορικοί λιμένες είναι οι φορείς CII στην ψηφιακή εποχή, δεδομένου ότι φιλοξενούν κρίσιμα συστήματα ICT, των οποίων η βλάβη ή η καταστροφή έχει σημαντική επίπτωση στην οικονομία, το εμπόριο και την εθνική ασφάλεια[1]. Η κανονική λειτουργία των εμπορικών λιμένων εξαρτάται, σε μεγάλο βαθμό, από την ορθή λειτουργία των συστημάτων τους ICT. Η μεγάλη ποσότητα των κρίσιμων και ευαίσθητων δεδομένων, των πληροφοριών και των υπηρεσιών που διαχειρίζονται σε καθημερινή βάση, ο μεγάλος αριθμός των φορέων που καλούνται να εξυπηρετηθούν, και οι αλληλεξαρτήσεις με άλλες υποδομές, απαιτούν αποτελεσματική διαχείριση της ασφάλειας.

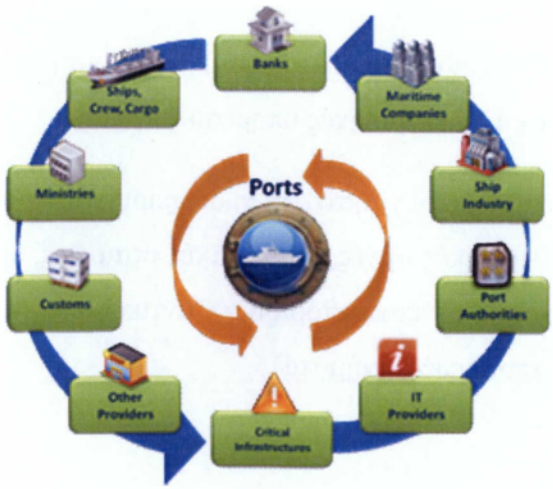
Οι εμπορικοί λιμένες εφαρμόζουν κρίσιμες ηλεκτρονικές υπηρεσίες και επιχειρηματικές διαδικασίες. Έτσι, απαιτούνται οι προσεγγίσεις κατάλληλης

διαχείρισης της ασφάλειας και της προστασίας, διατηρώντας την ασφαλή εκτέλεση των λιμένων σε περίπτωση βλάβης, επιθέσεων, ατυχημάτων ή κακόβουλων ενεργειών και, επίσης, για ελαχιστοποίηση του χρόνου αποκατάστασης των ζημιών. Μεγάλη προσοχή πρέπει να δοθεί στην ασφάλεια και την προστασία των υφισταμένων, την ανάπτυξη και την νέα γενιά κρίσιμων υπηρεσιών ηλεκτρονικού λιμένος.

Στις ακόλουθες παραγράφους, παρουσιάζουμε μια πολύ σύντομη εισαγωγή στο ναυτιλιακό οικοσύστημα, τα στοιχεία των συστημάτων PICT, καθώς και και τις υπηρεσίες ηλεκτρονικού λιμένος. Το υλικό αυτό είναι πολύ χρήσιμο για την κατανόηση της εκτίμηση της κρισιμότητας των υπηρεσιών ηλεκτρονικού λιμένος, η οποία αποτελεί αναπόσπαστο μέρος της διαχείρισης ασφάλειας των συστημάτων PICT.

2.1. Ναυτιλιακό Περιβάλλον-Ο ρόλος των εμπορικών λιμένων

Το ναυτιλιακό περιβάλλον είναι πολύπλοκο, όπως φαίνεται στο επόμενο σχήμα (Σχήμα 1), λόγω τη συμμετοχή πολλών φορέων - λιμένες, πλοία (μαζί με τους επιβάτες, το πλήρωμα και το φορτίο), λιμενικές αρχές, ναυτιλιακές και ασφαλιστικές εταιρείες, τελωνεία, βιομηχανία των πλοίων, τράπεζες, υπουργεία, άλλοι εμπορικοί πάροχοι, άλλες κρίσιμες υποδομές (π.χ. σιδηρόδρομοι, αεροδρόμια)- οι οποίοι αλληλεπιδρούν μεταξύ τους και υποστηρίζονται από πολύπλοκα και ετερογενή συστήματα ICT.



Σχήμα 1 Θαλασσίου Περιβάλλοντος

Κεντρικός ρόλος, στο ναυτιλιακό περιβάλλον, έχει αναληφθεί από τους εμπορικούς λιμένες, δεδομένου ότι είναι η μόνη οντότητα που αλληλεπιδρά άμεσα με όλους τους ναυτιλιακούς εταίρους, προσφέροντας υπηρεσίες *(λιμενικές υπηρεσίες)*, με διαφορετικό βαθμό κρισιμότητας.

2.2. Στοιχεία των PICT

Πολλές από τις υπηρεσίες που προσφέρονται και από τις διαδικασίες που υποστηρίζουν τη λειτουργία του εμπορικού λιμένα έχουν αυτοματοποιηθεί. Τα **Συστήματα Πληροφορικής και Τηλεπικοινωνιών Λιμένων (PICT)** είναι σύνθετα και αποτελούνται (όπως όλα τα συστήματα ICT) από τα ακόλουθα έξι (6) συνεχή σημεία αναφοράς:

1. **Φυσικές υποδομές** (π.χ. κτίρια, αποβάθρες, πύλες, μαρίνες, κέντρα δεδομένων, πλατφόρμες),

2. **Υποδομές ICT** (π.χ. δίκτυα, εξοπλισμός, τους δορυφόρους, εξυπηρετητές, σταθμοί αναμετάδοσης, παράπλευροι σταθμοί),

3. **Συστήματα και λογισμικό** (π.χ. δίκτυα επικοινωνιών, συστήματα μετάδοσης, δεδομένα ταυτοποίησης, θαλάσσια ναυσιπλοΐα, Προγραμματισμός Επιχειρηματικών Πόρων -ERPs-, έκδοση εισιτηρίων, GIS, συστήματα προσαρμοστικότητας λιμένων),

4. **Πληροφορίες και ηλεκτρονικά** δεδομένα (π.χ. θαλάσσια και παράκτια δεδομένα, εμπορικά δεδομένα),

5. **Υπηρεσίες** (π.χ. τιμολόγιο, πλοήγηση, διαχείριση αποσκευών / φορτίου / πλοίου, λογιστική, ηλεκτρονικές υπηρεσίες υγείας),

6. **Χρήστες:** α. εσωτερικοί χρήστες (π.χ. διαχειριστές, προσωπικό) β. εξωτερικοί χρήστες (π.χ. λιμενικές αρχές, ναυτιλιακές εταιρείες, τελωνεία, ασφαλιστικές εταιρείες, παροχείς IT και εμπορίου γ). αντικείμενα (π.χ. πλοία, φορτίο του πληρώματος, αποσκευές, οχήματα).

2.3. Υπηρεσίες ηλεκτρονικού λιμένος (E-Port)

Υπάρχουν διάφορες υπηρεσίες ηλεκτρονικού λιμένος (e-port), οι οποίες μπορούν να κατηγοριοποιηθούν, ανάλογα με τον κύριο στόχο τους και τις λειτουργείες τους, στις ακόλουθες πέντε (5) κατηγορίες:

- **Υπηρεσίες διαχείρισης πλοίων:** παρέχοντας ηλεκτρονικές πληροφορίες, για την κατάσταση σκαφών σε όλους τους πράκτορες· ηλεκτρονικές διοικητικές διαδικασίες· ηλεκτρονική επικοινωνία με το λιμάνι / ναυτιλιακές αρχές, αστυνομία, επιτροπή ελέγχου μετανάστευσης, κλπ· υπηρεσίες ελέγχου ταυτότητας σκάφους και παρακολούθησης (μέσω RFID, συστήματα GIS)· υπηρεσίες πλοήγησης,
- **Υπηρεσίες διαχείρισης φορτίου:** παροχή ηλεκτρονικής τεκμηρίωσης, σε όλους τους εμπλεκόμενους φορείς· ηλεκτρονικές πληροφορίες για την κατάσταση του φορτίου, ηλεκτρονική διαχείριση φορτίου, έλεγχος ταυτότητας φορτίου και υπηρεσίες παρακολούθησης (μέσω RFID, συστήματα GIS)· υπηρεσίες πλοήγησης,
- **Λογιστικές υπηρεσίες της ενδοχώρας:** ηλεκτρονική διαχείριση των λειτουργιών χερσαίων μεταφορών (π.χ. μεταφορές / αποδοχή / ηλεκτρονικές παραγγελίες παράδοσης)· ηλεκτρονικός εφοδιασμός, ηλεκτρονική τιμολόγηση, ηλεκτρονική πληρωμή· υπηρεσίες ηλεκτρονικής ανίχνευσης (π.χ. ηλεκτρονικές πληροφορίες σχετικά με τις μεταφορές σε ολόκληρη την λογιστική αλυσίδα)· ηλεκτρονική κράτηση,
- **Επικοινωνία στο επίπεδο λιμένος:** Διακαναλική ανακοίνωση (τηλεόραση, Διαδίκτυο, ασύρματο δίκτυο, VPN, δίκτυα *επικοινωνίας*), υπηρεσίες λιμένος για την επικοινωνία με όλες τις ναυτιλιακές εταιρείες (άλλοι λιμένες, πλοία, πλήρωμα κλπ.),
- **Ενσωμάτωση με άλλα συστήματα:** Υπηρεσίες ολοκλήρωσης με τα τελωνειακά συστήματα, για τα διάφορα ηλεκτρονικά διοικητικά τελωνειακά έγγραφα (π.χ. τελωνειακές διασαφήσεις, εισαγωγές / εξαγωγές) και τους ελέγχους (π.χ. φόροι, κυρώσεις)· ολοκλήρωση, με την αστυνομία λιμένος και τα συστήματα μετανάστευσης, της ηλεκτρονικής παρακολούθησης και του ελέγχου των πλοίων, των φορτίων, των αγαθών και των ανθρώπων· ενοποίηση των συστημάτων οργανισμών υγείας, για την παροχή υπηρεσιών

ηλεκτρονικής υγείας (ειδικά στο πλήρωμα)· ενοποίηση με άλλες μεταφορές CII (π.χ. σιδηρόδρομοι, αεροδρόμια), προσφέροντας συνεργατικές ηλεκτρονικές υπηρεσίες τουρισμού (κρατήσεις, προγραμματισμός, έκδοση εισιτηρίων).

Ωστόσο, δεν έχουν όλες οι παραπάνω υπηρεσίες τους ίδιους βαθμούς "ηλεκτρονικής εκλέπτυνσης", δηλαδή οι επιχειρηματικές τους διαδικασίες δεν έχουν τον ίδιο βαθμό εξάρτησης, από τα ηλεκτρονικά μέσα. Για την μέτρηση του επιπέδου της υπάρχουσας ωριμότητας εκλέπτυνσης κάθε ηλεκτρονικής υπηρεσίας, κάποιος μπορεί να υιοθετήσει το πλαίσιο τεσσάρων επιπέδων που χρησιμοποιούνται στον τομέα της ηλεκτρονικής διακυβέρνησης, δηλαδή τις πληροφορίες, την αλληλεπίδραση, την αμφίδρομη αλληλεπίδραση και τον πλήρη χειρισμό. Ειδικότερα, το πρώτο, διαγραμμικό επίπεδο εξειδίκευσης περιλαμβάνει τις υπηρεσίες που παρέχουν μόνο πληροφορίες σε απευθείας σύνδεση (καμία περαιτέρω αλληλεπίδραση επιτρέπεται). Στο δεύτερο επίπεδο, υπάρχει η δυνατότητα να κατεβάσετε ένα ηλεκτρονικό έγγραφο (καμία περαιτέρω αλληλεπίδραση επιτρέπεται). Υπηρεσίες του τρίτου επιπέδου (αμφίδρομη επικοινωνία), είναι εκείνες που προσφέρουν την δυνατότητα ηλεκτρονικής πρόσληψης, με επίσημη ηλεκτρονική μορφή, για να ξεκινήσει η διαδικασία για την απόκτηση αυτής της υπηρεσίας. Τέλος, στο τέταρτο επίπεδο, οι υπηρεσίες προσφέρουν τη δυνατότητα πλήρης εφαρμογής της λιμενικής υπηρεσίας σε ηλεκτρονική μορφή, συμπεριλαμβανομένης της απόφασής και της παράδοσης. Καμία άλλη επίσημη διαδικασία δεν είναι απαραίτητη για τον αιτούντα μέσω των "γραπτών αιτήσεων". Τα δύο τελευταία επίπεδα απαιτούν έλεγχο ταυτότητας του χρήστη και του διαχειριστή της υπηρεσίας ηλεκτρονικού λιμένος.

2.4. Εμπόδια για την ασφάλεια επίγνωση e-λιμενικών υπηρεσιών

Οι υπηρεσίες ηλεκτρονικού λιμένος θα πρέπει να εργάζονται σε ένα αξιόπιστο περιβάλλον. Παραδοσιακά, ο όρος «ασφαλείς υπηρεσίες» σήμαινε το απόρρητο των σχετικών δεδομένων που είναι αποθηκευμένα σε συστήματα ηλεκτρονικών υπολογιστών. Τώρα, υπάρχουν οι πρόσθετες διαστάσεις της ακεραιότητας και διαθεσιμότητας, που πρέπει να ληφθούν υπόψη. Στον τομέα της ηλεκτρονικής επιχείρησης, τα ηλεκτρονικά έγγραφα δεν πρέπει μόνο να είναι εμπιστευτικά μεταξύ του πωλητή και του αγοραστή. Θα πρέπει επίσης να είναι απρόσβλητα από τις

μεταβολές καθ 'οδόν. Το πιο σημαντικό, κανένα εμπλεκόμενο μέρος δεν θα πρέπει να είναι σε θέση να αρνηθεί ότι η συναλλαγή έχει πραγματοποιηθεί (φαινόμενο γνωστό ως μη άρνηση της προέλευσης και παραλαβής).

Κατά τα τελευταία χρόνια, οι Υποδομές Δημόσιου Κλειδιού (PKI) έχουν χαρακτηριστεί ως ένα κατάλληλο πλαίσιο για την παροχή των μέτρων ασφαλείας (όπως η εμπιστευτικότητα των δεδομένων, η ακεραιότητα, η διαθεσιμότητα και η μη άρνηση), σε διάφορους επιχειρηματικούς τομείς. Τα μέτρα αυτά προσφέρονται, μέσω κατάλληλων μηχανισμών ασφάλειας PKI (π.χ. κρυπτογράφηση δεδομένων, ψηφιακή υπογραφή, χρονοσήμανση), οι οποίοι μπορούν να εξασφαλίσουν ασφαλείς ηλεκτρονικές συναλλαγές.

Μία από τις τρέχουσες κύριες ανάγκες PKI είναι η διαλειτουργικότητα, η οποία καθιστά δυνατή την ασφαλή διασύνδεση και συνεργασία μεταξύ των διαφόρων δομών PKI, ενισχύοντας έτσι την σκοπιμότητα και την δυνατότητα εφαρμογής τους σε περιφερειακό, εθνικό, όσο και διεθνές επίπεδο. Αυτό είναι ακόμη πιο σημαντικό στον τομέα των θαλάσσιων μεταφορών, λόγω της αυξημένης ζήτησης για κινητικότητα των ναυτιλιακών εταίρων και της κρισιμότητας των λιμενικών δεδομένων, που καθιστούν την ασφαλή και διαλειτουργικη ανταλλαγή πληροφοριών ως ένα βασικό στοιχείο, για την παροχή λιμενικών υπηρεσιών υψηλού επιπέδου.

Η διαλειτουργικότητα PKI αντιμετωπίζεται συνήθως μέσω της υπηρεσίας διασταυρούμενης πιστοποίησης, η οποία μπορεί να περιγραφεί ως ο δρόμος για την δημιουργία αλυσίδων εμπιστοσύνης, μεταξύ των διαφόρων Αρχών Πιστοποίησης (ΑΠ). Ωστόσο, οι Αρχές Πιστοποίησης δεν έχουν ακόμη καθοριστεί για τον τομέα της ναυτιλίας, σε επίπεδο ΕΕ, και η διασταυρούμενη πιστοποίηση δεν παρέχεται ακόμη τεχνικά με αυτοματοποιημένο τρόπο, με αποτέλεσμα συχνά μια δύσκολη και χρονοβόρα διαδικασία, που βασίζεται στις έγγραφες αιτήσεις, μειώνοντας την ευελιξία και την ευχρηστία της ίδιας της μεθόδου.

Η έλλειψη αυτόματων διασταυρούμενων πιστοποιήσεων οφείλεται, σε μεγάλο βαθμό, στην ανεπαρκή τυποποίηση των Πολιτικών Πιστοποιητικού (CP), η οποία καθορίζει το προφίλ των πιστοποιητικών PKI και, συνεπώς, αυτά αποτελούν τα βασικά κριτήρια σύγκρισης, για την αμοιβαία αποδοχή των εθνικών ΑΠ. Πιο

συγκεκριμένα, αν και η δομή CP ορίζεται σε ορισμένα από τα υφιστάμενα πρότυπα, εξακολουθεί να υπάρχει ένα σημαντικό κενό στην τυποποίηση του περιεχομένου CP (π.χ. οι ρόλοι των εμπλεκόμενων ατόμων, οι απαιτήσεις πιστοποίησης και εγγραφής, κλπ.). Επιπλέον, δεν υπάρχει συστηματοποιημένος δρόμος για την ανάπτυξη και την σύγκριση του CP, καθιστώντας έτσι την συγκριτική ανάλυση τους ένα δύσκολο έργο.

Οι ανωτέρω περιορισμοί, σε συνδυασμό με την έλλειψη της απαραίτητης νομικής / κανονιστική εναρμόνισης PKI, δυσχεραίνει την αυτόματη σύγκριση CP, εμποδίζοντας, με τον τρόπο αυτό, την αυτοματοποίηση της συνολικής υπηρεσίας διασταυρούμενης πιστοποίησης και, ως εκ τούτου, καθιστώντας δύσκολη την ασφαλή ηλεκτρονική συνεργασία, ανταλλαγή πληροφοριών, ανταλλαγή γνώσεων και εμπειριών.

Αν και αυτό είναι ένα γενικό πρόβλημα των πιστοποιητικών PKI, που επηρεάζει όλους τους επιχειρηματικούς τομείς, υπάρχει επίσης ανάγκη για μια τομεακή ανάλυση (στην περίπτωση του ναυτιλιακού τομέα), ιδίως στο τμήμα τυποποίησης CP, όπου πρέπει να εξετασθούν οι αφιερωμένες απαιτήσεις των κοινοτήτων των βασικών χρηστών.

Ένα άλλο σημαντικό πρόβλημα είναι ότι οι τεχνολογίες που χρησιμοποιούνται για την αξιοποίηση των ηλεκτρονικών λιμενικών υπηρεσιών δεν αξιολογούνται, από άποψη ασφαλείας, και δεν εφαρμόζονται τα απαιτούμενα μέτρα ασφαλείας. Για παράδειγμα, οι τεχνολογίες Αναγνώρισης Συχνότητας Ραδιοκυμάτων (RFID) χρησιμοποιούνται συνήθως στα λογισμικά λιμένος, των εμπορευματοκιβωτίων και διαχείρισης του φορτίου. Ένας αριθμός από τις κορυφαίες λιμενικές εγκαταστάσεις της Ε.Ε. εξυπηρετούν ήδη, ή έχουν συναφθεί για να εξυπηρετούν, τις τεχνολογίες RFID. Ωστόσο, οι τεχνολογίες RFID αντιμετωπίζουν πολλές απειλές π.χ. οι υποκλοπές στις μηχανές ανάγνωσης RFID είναι μια σημαντική απειλή. Μπορεί να είναι μια πολύ αποτελεσματική μορφή της εταιρικής αντικατασκοπείας. Οι ίδιες οι μηχανές ανάγνωσης RFID μπορούν να μεταδίδουν δεδομένα RFID σε μεγάλες αποστάσεις - συχνά μέχρι και εκατοντάδες μέτρα μακριά. Αυτό σημαίνει ότι ένας ωτακουστής μπορεί να συγκεντρώσει τις σχετικές πληροφορίες και μπορεί να τις χρησιμοποιήσει ή να τις τροποποιήσει.

2.5. Ασφάλεια και προστασία: Δύο αλληλένδετες έννοιες

Είναι πολύ κοινό, στην βιβλιογραφία για την ναυτιλιακή ασφάλεια, ότι οι έννοιες της προστασίας και της ασφάλειας βρίσκονται σε σύγχυση. Για τον λόγο αυτό, παρέχουμε ορισμένες διευκρινίσεις για την έννοια και την σχέση μεταξύ αυτών των δύο εννοιών.

Λέμε ότι ένα σύστημα ICT (όπως τα συστήματα PICT) είναι **ασφαλές**, αν όλα τα στοιχεία των παραπάνω έξι αναφορών πληρούν όλες τις προϋποθέσεις της προστασίας, δηλαδή την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικότητα ή πρόσβαση ελέγχου και τη διαθεσιμότητα. Με **την ασφάλεια** (ή φυσική προστασία), εννοούμε την ικανοποίηση των δύο συνιστωσών της προστασίας και, συγκεκριμένα, τον έλεγχο πρόσβασης και την διαθεσιμότητα των επενδυτικών αγαθών, στην πρώτη και την έκτη αναφορά. Ως εκ τούτου, η ασφάλεια είναι ένα υποσύνολο της προστασίας ICT, όπως φαίνεται στο επόμενο σχήμα:

Σχήμα 2 Ασφάλεια και προστασία

Στην ναυτιλιακή βιβλιογραφία, υπάρχει μια παρεξήγηση σχετικά με αυτές τις δύο έννοιες, καθώς συμπίπτουν στις περισσότερες περιπτώσεις. Ειδικότερα, διάφορες υφιστάμενες προσπάθειες που ισχυρίζονται ότι σχετίζονται με την ασφάλεια των συστημάτων PICT, στην πραγματικότητα αφορούν μόνο την ασφάλεια των λιμένων.

2.6. Συμπεράσματα

Η υποβάθμιση, βλάβη ή καταστροφή των ηλεκτρονικών και κινητών λιμενικών υπηρεσιών έχουν σοβαρές επιπτώσεις στην αποτελεσματική λειτουργία και την εκμετάλλευση όχι μόνο των λιμένων, αλλά και των αλληλεπιδρώντων ναυτιλιακών εταίρων και τις λειτουργίες και επιχειρήσεις τους. Οι λιμένες είναι ζωτικής σημασίας υποδομές, φιλοξενώντας συστήματα PICT, τα οποία προσφέρουν διάφορες (ηλεκτρονικές ή κινητές) λιμενικές υπηρεσίες, η κρισιμότητα των οποίων εξαρτάται από το επιγραμμικό επίπεδο εξειδίκευσης τους, τις επιπτώσεις στις επιχειρήσεις τους και την αλληλεξάρτηση με άλλες υπηρεσίες ή συστήματα. Η έλλειψη ενός διασυνοριακά πιστοποιημένου PKI είναι μια μεγάλη πρόκληση και, ταυτόχρονα, εμπόδιο στο αξιόπιστο περιβάλλον που απαιτείται για την παροχή ασφαλών ηλεκτρονικών λιμενικών υπηρεσιών.

Η προστασία και ασφάλεια είναι δύο αλληλένδετες έννοιες. Ιδίως η προστασία είναι μια ευρύτερη έννοια που περιλαμβάνει την ασφάλεια. Στον τομέα των θαλάσσιων μεταφορών, αυτές οι δύο έννοιες χρησιμοποιούνται εναλλακτικά προκαλώντας παρεξηγήσεις, όπως θα δούμε στο επόμενο κεφάλαιο.

Κεφάλαιο 3: Συστήματα PICT για την διαχείριση της προστασία

Με την διαχείριση προστασίας (ICT), εννοούμε την αποτελεσματική εφαρμογή, την εγκατάσταση, την αξιολόγηση, την παρακολούθηση, την βελτίωση και τον έλεγχο της ασφάλειας του συστήματος ICT (όλα τα επενδυτικά αγαθά, στα έξι επίπεδα αναφοράς του συστήματος ICT). Η διαχείριση προστασίας ICT απαιτεί συνεχή και συστηματική διαδικασία εντοπισμού, καθώς και την ανάλυση, τον μετριασμό, την υποβολή εκθέσεων και την παρακολούθηση των τεχνικών, λειτουργικών και άλλων τύπων κινδύνων για την ασφάλεια (διαχείριση κινδύνου), και, παράλληλα, την εφαρμογή των κατάλληλων μέτρων ασφαλείας και ελέγχου. Αν και διάφορες προσπάθειες και διαδικασίες μπορούν να βρεθούν στην διαχείριση της προστασίας των λιμενικών συστημάτων, κανένα από αυτά δεν αφορά την διαχείριση προστασίας ICT από τα συστήματα PICT. Αντιμετωπίζουν μόνο την σωματική ασφάλεια και ασχολούνται με τη διαχείριση της ασφάλειας των λιμενικών συστημάτων. Ως μέσο για την υποστήριξη αυτης της δήλωσης, παρουσιάζουμε τα κενά των υφιστάμενων πρωτοβουλιών-μεθοδολογιών, στους ακόλουθους τομείς: την ασφάλεια στη θάλασσα, την πιο γνωστή εκτίμηση κινδύνου ICT και τις μεθοδολογίες διαχείρισης και την διαχείριση προστασίας CII.

3.1. Θαλάσσιες προσπάθειες ασφάλειας

Αν και υπάρχουν πολλές προσπάθειες ασφαλείας, οι προσπάθειες του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) [27] είναι οι πιο γνωστές. Ο IMO έχει εκδώσει μια σειρά οδηγιών που εμπίπτουν σε δύο κατηγορίες, τις SOLAS και MARPOL: Οι οδηγίες SOLAS για την ασφάλεια των πλοίων, των επιβατών και του φορτίου και οι οδηγίες MARPOL για την περιβαλλοντική (θάλασσα) προστασία.

Η οδηγία ISPS 2002 του IMO (Διεθνής Κώδικας Ασφαλείας Πλοίων και Λιμενικών Εγκαταστάσεων) είναι η πιο κατάλληλη αντιμετώπιση θεμάτων ασφαλείας, ωστόσο η ISPS καλύπτει μόνο: την ασφαλή πρόσβαση, τον έλεγχο, τον ασφαλή χειρισμό του φορτίου, την διαθεσιμότητα των τηλεπικοινωνιακών υποδομών, την υποβολή εκθέσεων συμβάντων, την δημιουργία ομάδας ασφαλείας Κινδύνου, την αξιολόγηση και την κατάρτιση. Η ISPS δεν εξετάζει ούτε τις απειλές στον κυβερνοχώρο ούτε τα μέτρα ασφαλείας για τα συστήματα PICT.

Σε ευρωπαϊκό επίπεδο, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια στην Θάλασσα (EMSA) [21] είναι ένας παροχέας υπηρεσιών στους τομείς της ασφάλειας της ναυσιπλοΐας, την φυσική ασφάλεια και την πρόληψη της ρύπανσης, ο οποίος στέλνει σχετικές πληροφορίες στην Επιτροπή, τα κράτη μέλη και άλλους σχετικούς φορείς της Ευρωπαϊκής Ένωσης. Το σύστημα SafeSeaNet, [56] που φιλοξενείται από την EMSA, συλλέγει θαλάσσιες πληροφορίες από τις σχετικές με την θάλασσα εθνικές αρχές (αφήνοντας την ασφαλή διακίνηση αυτών των πληροφοριών σε εθνικό επίπεδο).

Άλλοι ευρωπαϊκοί φορείς που σχετίζονται με την θάλασσα (π.χ. η Ευρωπαϊκή Γραμματεία Ασφάλειας της Αεροπορίας [20], ο Διευρωπαϊκός Εκτελεστικός Οργανισμός του Δικτύου Μεταφορών (TEN-T EA) [59]) δεν περιλαμβάνουν, στο υπόμνημά ασφάλειας τους, την προστασία του κυβερνοχώρου.

Ένας αριθμός προπαρασκευαστικής δράσης για έρευνα προστασίας (PASR) και προγράμματα Έρευνας για την Ασφάλεια FP7 έχουν δρομολογηθεί, κατά την τελευταία δεκαετία, για την αντιμετώπιση των θεμάτων που σχετίζονται με την ενίσχυση της ασφάλειας των λιμένων ή / και των συστημάτων τους PICT. Τα περισσότερα από αυτά τα έργα εμπίπτουν σε τρεις κύριες κατηγορίες, όπως ακολούθως:

- *Βελτίωση των συστημάτων θαλάσσιας επιτήρησης* (έργα αυτής της κατηγορίας είναι τα: AMASS, UNCOSS, SOBCAH, SEABILLA),
- *Η διαλειτουργικότητα των συστημάτων PICT* (έργα αυτής της κατηγορίας είναι τα: AMASS, UNCOSS, SOBCAH, SEABILLA, OPERAMAR, SECCONDD),

- *Προστασία των κρίσιμων θαλάσσιων υποδομών* (SECTRONIC, SUPPORT).

Στοχευμένες μεθοδολογίες για την εκτίμηση της επικινδυνότητας των λιμένων, όπως το MSRAM (Maritime Security Risk Analysis Model) [16] και η εκτεταμένη έκδοση του MSRAM-PLUS/FORETELL [3], εξετάζουν μόνο τη σωματική ασφάλεια και είναι συμβατές με τις ISPS. Ομοίως, τα διαθέσιμα συστήματα εκτίμησης ναυτιλιακού κινδύνου, όπως το MARISA [4], επικεντρώνονται στην ασφαλή πλοήγηση των πλοίων, κατά τη διάρκεια της παρουσίας τους στο λιμάνι. Το σύστημα αξιολόγησης των κινδύνων CMA [37] εντοπίζει ανώμαλη συμπεριφορά των πλοίων και προσδιορίζει σημαντικές απειλές. Διάφορες μελέτες εθνικής υπόθεσης, για τις στρατηγικές διαχείρισης κινδύνου και τα συστήματα που χρησιμοποιούνται στα λιμάνια της Εσθονίας [25], την Ιορδανία [32] και τη Ρωσία [57], [41], επικεντρώνονται επίσης στην ασφάλεια των λιμένων.

Όλες οι αξιολογήσιμες θαλάσσιες οδηγίες διαχείρισης της ασφάλειας, οι μεθοδολογίες και τα έργα εξετάζουν μόνο την ασφάλεια (φυσική ασφάλεια) και εν μέρει (αν όχι καθόλου) την ασφάλεια ICT.

Ειδικότερα:

- καλύπτουν μόνο δύο (από τα έξι) επίπεδα αναφοράς των PICT, δηλαδή το πρώτο (φυσικών υποδομών) και το έκτο (χρήστης), αφήνοντας έτσι τα ενδιάμεσα επίπεδα απροστάτευτα.
- ασχολούνται μόνο με τις φυσικές απειλές και δεν υπολογίζουν τον φυσικό σχετικό κίνδυνο· δεν εξετάζουν τις απειλές στον κυβερνοχώρο που αυξάνονται από τα ανεξάρτητα συστήματα PICT ή την αλληλεξάρτηση τους με τις άλλες ναυτιλιακές εταιρείες που μπορούν να προκαλέσουν πολλαπλές επιπτώσεις.
- δεν διερευνούν την ασφάλεια PICT ανεξάρτητα, αλλά σε σχέση με την ασφάλεια των πλοίων. Η εφαρμογή του κώδικα ISPS αφορά το εθνικό επίπεδο, δηλαδή δεν υπάρχει ένα πρότυπο που παρέχει τις ακριβείς διαδικασίες και τα μέτρα που πρέπει να αναληφθούν (π.χ. όπως το ISO27002 [30]), προκειμένου ένα λιμάνι να γίνει συμβατό με τον κώδικα ISPS.

- δεν επικεντρώνονται στον χρήστη· θεωρούν τον χρήστη ως παθητικά συμμετέχουσα οντότητα που πρέπει να ακολουθήσει τη μεθοδολογία, χωρίς αλληλεπίδραση ή συνεργασία.

Οι προσπάθειες της ισχύουσας ναυτιλιακής νομοθεσίας ή τυποποίησης δεν καλύπτουν επαρκώς την ασφάλεια ICT των εμπορικών λιμένων. Ειδικότερα, οι εμπορικοί λιμένες δεν αντιμετωπίζονται ως ανεξάρτητες κρίσιμες υποδομές φιλοξενίας των κρισίμων συστημάτων ICT που αλληλεπιδρούν με πολλούς φορείς και η ασφάλειά τους δεν αξιολογείται ή διαχειρίζεται σε έναν ολιστικό, αποτελεσματικό τρόπο. Το γεγονός ότι οι λιμένες αποτελούν υποδομές ζωτικής σημασίας, θέτει συγκεκριμένες απειλές (π.χ. απεργίες, τρομοκρατικές επιθέσεις, καιρικές συνθήκες), αφού οι ταυτοποιήσεις και οι επιπτώσεις (π.χ. στην εθνική οικονομία, την εθνική ασφάλεια, την διατάραξη της δημόσιας τάξης) οι οποίες αγνοούνται, δίνουν ανακριβείς αξιολογήσεις κινδύνου.

3.2. Μεθοδολογίες Διαχείρισης Ασφάλειας ICT

Σε αυτή την ενότητα, παρέχεται μία επισκόπηση των προτύπων διαχείρισης της ασφάλειας ICT και των μεθοδολογιών και εξετάζεται η καταλληλότητά τους για τα συστήματα PICT. Στην συνέχεια, εντοπίζονται τα κενά και τα εμπόδια και παρέχονται οι απαιτήσεις που πρέπει να πληρούνται από τις λύσεις προοπτικής.

Η Ακαδημία έχει προτείνει, τα ακόλουθα δώδεκα (12) κριτήρια αξιολόγησης που θα χρησιμοποιηθούν κατά την αξιολόγηση των μεθοδολογιών διαχείρισης κινδύνου ICT [17], [63]:

- **1. Πεδίο εφαρμογής** : η δυνατότητα εφαρμογής της μεθόδου. Οι ακόλουθοι τύποι έχουν εντοπιστεί:
    - Γενική μέθοδος - που καλύπτει μόνο εξειδικευμένες απαιτήσεις των ICT.
    - Στοχευμένη μέθοδος χρήσης - που καλύπτει συγκεκριμένα τομεακά χαρακτηριστικά, τις ιδιαιτερότητες, τις ανάγκες και τις απαιτήσεις.
- **2. Ομάδα στόχος** : το πιο κατάλληλο είδος των οργανώσεων στις οποίες απευθύνεται η μέθοδος.

- **3. RA / RM υποστήριξη**: οι φάσεις που υποστηρίζει η μέθοδος (ανάλυση κινδύνου ή / και διαχείριση των κινδύνων).
- **4. Κλίμακα αξιολόγησης**: η προσέγγιση συστημάτων (ποσοτική ή ποιοτική) που χρησιμοποιείται στις μεθόδους για την αξιολόγηση του επιπέδου κινδύνου.
- **5. Η αξιολόγηση του αντίκτυπου**: η προσέγγιση συστημάτων που υιοθετήθηκε στις μεθόδους για να καθορίσει το επίπεδο των επιπτώσεων. Κάθε μέθοδος χρησιμοποιεί τα συγκεκριμένα σενάρια, παράγοντες, τις παραμέτρους και τις κατευθυντήριες γραμμές, για τον καθορισμό των επιπτώσεων ενός συμβάντος.
- **6. Η εκτίμηση του κινδύνου**: η προσέγγιση συστημάτων που χρησιμοποιείται στις μεθόδους, για τον υπολογισμό του επιπέδου κινδύνου. Σύμφωνα με την έρευνα [63], έχουν εντοπιστεί οι ακόλουθοι τύποι προσεγγίσεων συστημάτων:
    - *Τύπος 1* : Κίνδυνος (απειλή, επενδυτικά αγαθά) = Πιθανότητα (απειλή) ⊗ ευπάθειας (απειλή, επενδυτικά αγαθά) ⊗ Επιπτώσεις (απειλή, επενδυτικά αγαθά)

Η έννοια του κινδύνου σχετίζεται με μια απειλή και ένα επενδυτικό αγαθό (ή ομάδα επενδυτικών αγαθών) και περιλαμβάνει την πιθανότητα της απειλής, το επίπεδο ευπάθειας του επενδυτικού αγαθού (ών) για την απειλή, και τον αντίκτυπο της απειλής για το επενδυτικό αγαθό (ά).

- *Τύπος 2* : Κίνδυνος (απειλή, επενδυτικό αγαθό, ανάγκες) = Επιπτώσεις (απειλή, ανάγκες) ⊗ ευπάθεια (απειλή, επενδυτικό αγαθό)

Η έννοια του κινδύνου σχετίζεται με μια απειλή, ένα επενδυτικό αγαθό και τις συγκεκριμένες ανάγκες ασφαλείας. Περιλαμβάνει την ευπάθεια του επενδυτικού αγαθού στοιχείου και τον αντίκτυπο της απειλής για τις ανάγκες ασφαλείας.

- *Τύπος 3* : Κίνδυνος (Απειλή, επενδυτικό αγαθό) = ΕΕΣ (απειλή, επενδυτικό αγαθό) = Πιθανότητα (απειλή, επενδυτικό αγαθό) ⊗ μέση απώλεια (απειλή, επενδυτικό αγαθό)

Η έννοια του κινδύνου (που ορίζεται ως Ετήσια προσδοκία Απώλειας (ALE)) σχετίζεται με μία απειλή και ένα επενδυτικό αγαθό, και περιλαμβάνει την πιθανότητα της απειλής που επηρεάζει το επενδυτικό αγαθό και την μέση απώλεια του προκύπτοντος περιστατικού.

- *Τύπος 4* : Κίνδυνος (Απειλή, κριτικό επενδυτικό αγαθό) = Επιπτώσεις (απειλή, κριτικό επενδυτικό αγαθό) ⊗ ευπάθεια (κριτικό επενδυτικό αγαθό)

Η έννοια του κινδύνου σχετίζεται με μια απειλή και ένα κρίσιμο επενδυτικό αγαθό, σε σχέση με την επίπτωση της απειλής για το κρίσιμο πλεονέκτημα και την ευπάθεια του περιουσιακού στοιχείου.

- *Τύπος 5* : Κίνδυνος (Συμβάν, επενδυτικό αγαθό) = Πιθανότητα (Συμβάν) ⊗ Συνέπειες (Συμβάν, επενδυτικό αγαθό)

Η έννοια του κινδύνου σχετίζεται με κάποιο συμβάν (δηλαδή, μια απειλή που εκμεταλλεύεται την ευπάθεια) και ένα επενδυτικό αγαθό, και περιλαμβάνει την πιθανότητα του περιστατικού και τις συνέπειες του ίδιου του συμβάντος.

- **7. Δυνατότητες συνεργασίας** : η ικανότητα των μεθόδων για την προώθηση της συνεργασίας των χρηστών, στην διαδικασία αξιολόγησης.
- **8. Υπολογιστικές δυνατότητες** η ικανότητα των μεθόδων για την ανάλυση και τον συνδυασμό διαφορετικών και κατανεμημένων εταιρικών γνώσεων.
- **9. Απαιτούμενες δεξιότητες**: το επίπεδο των δεξιοτήτων που απαιτούνται για την χρήση και την διατήρηση της μεθόδου.
- **10. Κόστος** : το σχήμα αδειοδότησης που διατίθεται για την μέθοδο.
- **11. Αυτοματοποιημένα εργαλεία**: η διαθεσιμότητα των εργαλείων που υποστηρίζουν τη μέθοδο.
- **12. Συμβατότητα με τα πρότυπα**: συμμόρφωση με τα εθνικά ή διεθνή πρότυπα.

Οι υπάρχουσες μεθοδολογίες (αναλύονται στο Παράρτημα) βασίζονται στα παραπάνω δώδεκα (12) κριτήρια· μια συνολική αξιολόγηση παρουσιάζεται στον επόμενο πίνακα:

Κριτήρια / Μέθοδοι	Γ1	Γ2	Γ3	Γ4	Γ5	Γ6	Γ7	Γ8	Γ9	Γ10	Γ11	Γ12
OCTAVE [50]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες, ΜΜΕ	RA / RM	Ποιοτικός	Με βάση τα περιουσιακά στοιχεία ζωτικής σημασίας	Τύπος 4	Μέσον	Χαμηλός	Πρότυπο	Δωρεάν	Ναι / Εμπορικός	-
CRAMM [28]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες	RA / RM	Ποιοτικός	Με βάση τα ανοιχτά σενάρια βλάβης	Τύπος 1	Χαμηλός	Χαμηλός	ITC ειδικοί	Εμπορικός	Ναι / Εμπορικός	ISO / IEC 27002:2005
Ebios [23]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες, ΜΜΕ	RA / RM	Ποιοτικός	Με βάση τις ανάγκες ασφάλειας	Τύπος 2	Μέσον	Χαμηλός	Πρότυπο	Δωρεάν	Ναι / Δωρεάν	ISO / IEC 27001:2005, ISO / IEC 27002:2005, ISO / IEC 27005:2008
IT-Grundschutz [7], [8], [9]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες, ΜΜΕ	RA / RM	Ποιοτικός	Με βάση τα ανοιχτά σενάρια βλάβης	Τύπος 5	Χαμηλός	Χαμηλός	Πρότυπο	Δωρεάν	Ναι / Εμπορικός	ISO / IEC 27001:2005, ISO / IEC 27002:2005
Magerit [13], [14], [15]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες, ΜΜΕ	RA / RM	Ποσοτική / Ποιοτική	Με βάση τα ανοιχτά σενάρια βλάβης	Τύπος 5	Χαμηλός	Χαμηλός	ITC ειδικοί	Δωρεάν	Ναι / Εμπορικός	ISO / IEC 27001:2005, ISO / IEC 27002:2005 ISO / IEC 27005:2008
MEHARI [11]	Γενικού σκοπού	Κυβέρνηση, φορείς Μεσαίες και μεγάλες επιχειρήσεις	RA / RM	Ποιοτικός	Βασίζεται σε σταθερά σενάρια βλάβης	Τύπος 1	Χαμηλός	Χαμηλός	ITC ειδικοί	Εμπορικός	Ναι / Εμπορική πολιτική / Ελεύθερη	ISO / IEC 27001:2005 ISO / IEC 27005:2008
ISAMM [26]	Γενικού σκοπού	Κυβέρνηση, φορείς, Οι μεγάλες εταιρείες, ΜΜΕ	RA / RM	Ποιοτικός	Με βάση την νομισματική απώλεια	Τύπος 3	Χαμηλός	Χαμηλός	Πρότυπο	N / A	Ναι / Εμπορική πολιτική / Ελεύθερη	ISO / IEC 27002:200

Πίνακας 1 Αξιολόγηση των κυριότερων μεθοδολογιών για τη διαχείριση της προστασίας ICT

Όλες οι μεθοδολογίες και οι μέθοδοι που παρουσιάζονται περιγράφουν συγκεκριμένα βήματα υλοποίησης, για την αξιολόγηση του επιπέδου ασφαλείας των οργανισμών. Εκτός από τα πρότυπα ISO 27001 [29] και ISO 27002 [30], τα οποία παρέχουν γενικές απαιτήσεις της αξιολόγησης του κινδύνου και δεν περιλαμβάνουν πτυχές χειρισμού του κινδύνου ειδικά, όλες οι άλλες προσεγγίσεις παρέχουν σαφώς καθορισμένες ενέργειες και τα μέτρα για την εκτέλεση της ανάλυσης κινδύνου και των διαδικασιών διαχείρισης κινδύνων. Επίσης, οι περισσότερες από τις μεθόδους προορίζονται να χρησιμοποιηθούν με ποιοτικές μετρήσεις, και αυτό επιβεβαιώνει το γεγονός ότι οι περισσότερες εκτιμήσεις κινδύνου σήμερα διεξάγονται με έναν ποιοτικό τρόπο, κυρίως λόγω της έλλειψης αξιόπιστων ποσοτικών δεδομένων ή χρονικών περιορισμών.

Έχουμε εντοπίσει τις ακόλουθες παγίδες των παραπάνω περιγραφόμενων μεθοδολογιών:

- Μόνο ένα μέρος από αυτά υποστηρίζεται από τα λογισμικά (σε ορισμένες περιπτώσεις δωρεάν) εργαλεία (βλέπε κριτήριο C11 στον Πίνακα 1). Τα γενικά χαρακτηριστικά αυτών των εργαλείων είναι:
    - δεν είναι εύκολα στη χρήση, χωρίς υψηλή τεχνογνωσία προστασίας ,
    - είναι μονολιθικά και αυτόνομα, αποτυγχάνοντας έτσι να αντιμετωπίσουν προηγμένες απαιτήσεις των σύγχρονων πληροφοριακών συστημάτων,
    - η χρήση προηγμένων και διαδραστικών γραφικών διεπαφών χρήστη, που βασίζεται στο Διαδίκτυο, και η πτυχή της συνεργασίας είναι δύο σημαντικές απαιτήσεις που τα υφιστάμενα εργαλεία και οι εφαρμογές δεν ανταποκρίνονται. Για τον λόγο αυτό, οι λύσεις αυτές δεν διευκολύνουν την διανομή και ανταλλαγή πληροφοριών, εμπειριών και εμπειρογνωμοσύνης, στο πλαίσιο μιας επιχείρησης, και δεν ενθαρρύνουν τους χρήστες να εργαστούν από κοινού για την εφαρμογή των φάσεων της ανάλυσης και διαχείρισης των κινδύνων, με έναν αποτελεσματικό και ομαλό τρόπο.

Όσον αφορά την αξιολόγηση του επιπέδου επιπτώσεων [63], το ISO 27005 [31] και ISO 27002 [30] επιβάλλει ότι ο αντίκτυπος ενός συμβάντος προστασίας αξιολογείται

από την άποψη της επιχειρησιακής ζημίας που προκλήθηκε στην οργάνωση. Στην MEHARI, οι αναλυτές συμμετέχουν στην διαδικασία μέτρησης του επιπέδου των επιπτώσεων και ανάλυσης κινδύνου, με βάση ένα «σταθερό» σενάριο των επιπτώσεων. Από την άλλη πλευρά, οι CRAMM, IT-Grundshutz, NIST SP 800-30 [39] και Magerit δίνουν την ευκαιρία στους αναλυτές να καθορίσουν διαφορετικά σενάρια επιπτώσεων (π.χ., από καταστροφικές έως περιθωριακές), απεικονίζοντας τις αρνητικές επιπτώσεις ενός γεγονότος (π.χ. απειλή, προσβολή), σχετικά με την οργάνωση. Σε αυτό το πλαίσιο, οι προσεγγίσεις αυτές υιοθετούν την έννοια των σεναρίων ζημιών. Οι επιπτώσεις των μέτρων OCTAVE βασίζονταν στο πόσο "σκληρά" επηρεάζει μια εκδήλωση της ασφάλειας ένα κρίσιμο περιουσιακό στοιχείο. Στην EBIOS, το επίπεδο των επιπτώσεων ενός συμβάντος μετριέται λαμβάνοντας υπόψη την απαιτούμενη ασφάλεια, την οποία η ειδική εκδήλωση παραβιάζει. Ομοίως, στην ISAMM εκτιμάται ο αντίκτυπος από την άποψη των οικονομικών απωλειών που η οργάνωση έχει υποστεί, ως αποτέλεσμα ενός γεγονότος.

- Αποτυγχάνουν να συλλάβουν την πολυπλοκότητα της διασύνδεσης των υποδομών, των διατομεακών επιπτώσεων, τις εξαρτήσεις από άλλα συστήματα ή υποδομές και τις πολλαπλές επιπτώσεις σε έναν τομέα ή σε όλους τους τομείς. Ως εκ τούτου, οι διάφορες τροποποιήσεις απαιτούνται, προκειμένου να εφαρμοστεί η διαχείριση της ασφάλειας των συστημάτων PICT, δεδομένου ότι τα συστήματα αυτά αλληλεπιδρούν με πολλούς ναυτιλιακούς εξωτερικούς φορείς (ανάλυση αλληλεξαρτήσεων).

Όσον αφορά την αξιολόγηση του επιπέδου κινδύνου, μπορούν να συναχθούν τα ακόλουθα συμπεράσματα. Στις CRAMM, MEHARI και NIST SP 800-30, ο κίνδυνος περιλαμβάνει την πιθανότητα και τις επιπτώσεις της απειλής να επηρεάσουν μια ομάδα επενδυτικών αγαθών και το επίπεδο ευαισθησίας αυτής της ομάδας. Στις IT-Grundshutz και Magerit, ο κίνδυνος περιλαμβάνει την πιθανότητα να συμβεί ένα ατύχημα (δηλαδή, μια απειλή που εκμεταλλεύεται κάποια τρωτά σημεία), καθώς και τις θετικές ή αρνητικές επιπτώσεις αυτού του περιστατικού. Από την άλλη πλευρά, οι EBIOS, OCTAVE και ISAMM αφορούν μία ειδική προσέγγιση στον υπολογισμό του επιπέδου κινδύνου. Ειδικότερα, οι EBIOS και OCTAVE υιοθετούν μια ποιοτική μέθοδο για την αξιολόγηση του κινδύνου, ενώ η ISAMM συνδέεται με τις ποσοτικές έννοιες των πιθανοτήτων και την μέση νομισματική απώλεια. Όσον αφορά την

οικογένεια ISO, το ISO 27005 παρέχει μόνο κατευθυντήριες γραμμές για το πώς να δημιουργηθεί το πλαίσιο διαχείρισης κινδύνου ISO 27002, ενώ και το ISO 27001 θέτει γενικές απαιτήσεις αξιολόγησης του κινδύνου και δεν περιλαμβάνει πτυχές χειρισμού του κινδύνου ειδικά.

- Όλες οι μέθοδοι βασίζονται σε συνεντεύξεις και εργαστήρια, για την συγκέντρωση και την συσσώρευση των στοιχείων της αξιολόγησης ασφάλειας. Ωστόσο, οι περισσότερες από αυτές παρουσιάζουν περιορισμένες δυνατότητες συνεργασίας, δεδομένου ότι δεν προωθούν την εκτεταμένη και αποδοτική συνεργασία μεταξύ των εμπλεκόμενων φορέων, την αποτελεσματική συζήτηση και την ανταλλαγή πληροφοριών, ιδεών και σκέψεων, καθώς και την ενεργό συμμετοχή των εταιρικών αντιπροσώπων. Αυτό είναι ένα σημαντικό μειονέκτημα, αν θέλουμε να τις εφαρμόσουμε στα συστήματα PICT, δεδομένου ότι υπάρχουν πολλοί χρήστες και οι απαιτούμενες διαπροσωπικές συνεντεύξεις απαιτούν χρόνο, προσπάθεια και πόρους. Μόνο οι OCTAVE και Ebios παρέχουν βασικές δυνατότητες συνεργασίας, γιατί περιέχουν ειδικά χαρακτηριστικά που επιτρέπουν στους χρήστες να συμμετέχουν ενεργά, σε πολλά μέρη της διαδικασίας αξιολόγησης.
- Ένα άλλο σημαντικό μειονέκτημα των προσεγγίσεων ανάλυσης κινδύνου είναι η έλλειψη αποτελεσματικών και προηγμένων υπολογιστικών τεχνικών. Συνήθως, βασίζονται σε πρωτόγονες μεθόδους για την αξιολόγηση, τον προσδιορισμό και την άμβλυνση των εταιρικών κινδύνων και χρησιμοποιούν αναποτελεσματικές διαδικασίες και τεχνικές, για να αναλύσουν και να συνδυάσουν τις ποικίλες γνώσεις που βρίσκεται στις οργανώσεις. Η υιοθέτηση των πιο προηγμένων προσεγγίσεων που ενισχύουν τις εγγενείς δυνατότητες των λύσεων ανάλυσης κινδύνου θα αυξήσει την ακρίβεια των συμπερασμάτων τους.

Οι μεθοδολογίες προσπαθούν να καλύψουν τις υποχρεώσεις που επιβάλλονται από την ομάδα προτύπων ISO (ISO / IEC 27001:2005, ISO / IEC 27002:2005, ISO / IEC 27005:2008). Ωστόσο, μόνο οι Ebios και Magerit επιτυγχάνουν πλήρη συμμόρφωση με τους κανόνες και τις διαδικασίες τους. Οι CRAMM, ISAMM και IT-Grundschutz ακολουθούν τον κώδικα εφαρμογής ενός ISMS, όπως περιγράφεται από το πρότυπο ISO / IEC 27002:2005, ενώ οι NIST 800-30, IT-Grundschutz και

MEHARI πληρούν τις απαιτήσεις που ορίζονται από το πρότυπο ISO / IEC 27001:2005.

- Υιοθετούν και χρησιμοποιούν μια πληθώρα απογοητευτικών ερωτηματολογίων και συνεντεύξεων, για την αξιολόγηση των απειλών και των τρωτών σημείων.
- Είναι πολύ γενικές, παραλείποντας να παράσχουν στοχευμένες τεχνικές λύσεις που απευθύνονται ειδικά σε προβλήματα και απειλές τομεακού επιπέδου (π.χ. ναυτιλία). Οι αλληλοεξαρτώμενες απειλές αυξάνονται από τις συνδεδεμένες επιχειρήσεις, τις απειλές για συγκεκριμένους τομείς (π.χ. καιρικές συνθήκες, απεργίες) και την τομεακή νομοθεσία (π.χ. ISPS στο θαλάσσιο περιβάλλον).

3.2.1. Η αξιολόγηση του αντίκτυπου

- Έχουμε παρουσιάσει τις γενικές υπηρεσίες ηλεκτρονικού λιμένος, σε προηγούμενες ενότητες. Η ανάγκη για τη διαχείριση της ασφάλειας προκύπτει από την ανάγκη να προσφερθούν ασφαλείς και αξιόπιστες ηλεκτρονικές υπηρεσίες. Το σημείο εκκίνησης της κάθε μεθοδολογίας εκτίμησης του κινδύνου προκλήθηκε από την εκτίμηση της κρισιμότητας των βασικών υπηρεσιών της (η οικονομική ευημερία του λιμένα εξαρτάται από την επιτυχή υλοποίηση των λιμενικών υπηρεσιών). Σε αυτήν την ενότητα, παρουσιάζουμε ένα παράδειγμα εκτίμησης της κρισιμότητας των υπηρεσιών ηλεκτρονικού λιμένος.

3.2.1.1 Αξιολόγηση επιχειρηματικής κρισιμότητας των υπηρεσιών ηλεκτρονικού λιμένος

Μια υπηρεσία ηλεκτρονικού / κινητού λιμένος είναι *σημαντική επιχειρηματικά*, εάν η αποικοδόμηση, βλάβη ή η καταστροφή της έχει σοβαρές επιπτώσεις, στην αποτελεσματική λειτουργία και την εκμετάλλευση του λιμένα ή / και την αλληλεπίδραση των ναυτιλιακών εταιρειών, καθώς και στην οικονομία και τις κυβερνήσεις στο σύνολό τους.

Πηγαίνοντας ένα βήμα πέρα, η μελέτη αυτή προτείνει μια γενική μεθοδολογία για την εκτίμηση της επιχειρησιακής κρισιμότητας των ηλεκτρονικών λιμενικών υπηρεσιών. Αυτές οι εκτιμήσεις είναι σημαντικές για την αξιολόγηση των επιπτώσεων, τις οποίες η παραβίαση της ασφάλειας των κρίσιμων ηλεκτρονικών λιμενικών υπηρεσιών θα προκαλέσει, με επίκεντρο τον τρόπο που επηρεάζει όχι μόνο τους ίδιους, αλλά και τις ναυτιλιακές εταιρείες. Το προτεινόμενο πλαίσιο αποτελείται από τα ακόλουθα βήματα:

- Καθορίστε το επίπεδο της επιγραμμικής εκλέπτυνσης που προσφέρεται από την υπηρεσία με βάση το εγκριθέν πλαίσιο τεσσάρων σταδίων (που περιγράφεται παραπάνω).
- Καθορίστε το εύρος των υπηρεσιών που παρέχονται σε τοπικό, εθνικό, περιφερειακό ευρωπαϊκό ή διεθνές επίπεδο.
- Καθορίστε τις εξαρτήσεις της με άλλους φορείς ή υπηρεσίες (π.χ. χρησιμοποιώντας Μοντελοποίηση Επιχειρησιακών Διαδικασιών ή Θεωρία Γραφημάτων).
- Καθορίστε τους αποδέκτες των υπηρεσιών.
- Καθορίστε το επίπεδο των επιχειρησιακών επιπτώσεων της υπηρεσίας, για όλους τους δικαιούχους και όλα τα εξαρτώμενα πρόσωπα.

Υιοθετώντας αυτό το απλό πλαίσιο, μπορεί κανείς να ταξινομήσει τις προσφερόμενες υπηρεσίες του, από την άποψη της κρισιμότητας των επιχειρήσεων.

3.2.1.2 Αξιολόγηση της κρισιμότητας ασφάλειας των ηλεκτρονικών υπηρεσιών λιμένος

Οι εμπορικοί λιμένες φιλοξενούν, αποθηκεύουν και ανταλλάσουν τα δεδομένα πληροφοριών (4ο στρώμα PICT) χρησιμοποιώντας διάφορες επιχειρηματικές διαδικασίες (ηλεκτρονικές, έγγραφες ή και τις δύο), προκειμένου να προσφέρουν ηλεκτρονικές και κινητές (e / m) λιμενικές υπηρεσίες (5ο στρώμα PICT) στους ναυτιλιακούς εταίρους, με κύριο στόχο την διευκόλυνση των καθημερινών δραστηριοτήτων και τις αλληλεπιδράσεις με αυτές, ενισχύοντας τις επιχειρήσεις και

τις εμπορικές τους δραστηριότητες και αλληλεπιδρώντας πιο αποτελεσματικά με όλες τις ναυτιλιακές εταιρείες.

Μια e / m-υπηρεσία λιμένος χαρακτηρίζεται ως *κρίσιμη για την ασφάλεια* αν είναι σημαντική επιχειρηματικά και η υποβάθμιση, βλάβη ή η καταστροφή της έχει σοβαρό αντίκτυπο στην ασφαλή λειτουργία του συστήματος PICT ή / και άλλων διασυνδέσεων των συστημάτων ICT και μπορεί επίσης να επηρεάσει την προστασία της ηλεκτρονικής επιχείρισης ή την εθνική ασφάλεια. Ανάλογα με το επίπεδο εξειδίκευσης της επιγραμμικής e / m-υπηρεσίας λιμένος και της επιχειρησιακής κρισιμότητας του, μπορούμε να εκχωρήσουμε τα διάφορα επίπεδα κρισιμότητας:

Επίπεδο κρισιμότητας 0: το πρώτο επίπεδο των επιγραμμικά εξελιγμένων ηλεκτρονικών λιμενικών υπηρεσιών, με χαμηλό επιχειρηματικό αντίκτυπο στην διακοπή των εν λόγω υπηρεσιών, έχει αντίκτυπο ούτε στην ασφάλεια ούτε την ιδιωτική ζωή ή την επιχείρηση, ενώ δεν υπάρχουν κρίσιμες εξαρτήσεις σε άλλες υπηρεσίες.

Επίπεδο κρισιμότητας 1: το δεύτερο επίπεδο των επιγραμμικά εξελιγμένων υπηρεσιών ηλεκτρονικού λιμένος, με χαμηλό έως μέτριο επιχειρηματικό αντίκτυπο, στοχεύει στην διευκόλυνση των χρηστών από το ναυτιλιακό περιβάλλον (όχι μόνο σε εθνικό αλλά και σε ευρωπαϊκό ή διεθνές επίπεδο), με τις πράξεις τους. Η διακοπή των υπηρεσιών αυτών δεν έχει καμία επίπτωση στην ασφάλεια ή την ιδιωτική ζωή, ενώ δεν υπάρχουν κρίσιμες εξαρτήσεις σε άλλες υπηρεσίες.

Επίπεδο κρισιμότητας 2: το δεύτερο και το τρίτο επίπεδο των επιγραμμικά εξελιγμένων υπηρεσιών του ηλεκτρονικού λιμένος, με χαμηλό έως μέτριο επιχειρηματικό αντίκτυπο, προσανατολίζονται στην υποστήριξη των χρηστών από το ναυτιλιακό περιβάλλον (όχι μόνο σε εθνικό αλλά και σε ευρωπαϊκό ή διεθνές επίπεδο), με τις πράξεις τους. Η διακοπή των υπηρεσιών αυτών έχει μια απλή επίπτωση στην ασφάλεια ή την ιδιωτική ζωή, ενώ κρίσιμες εξαρτήσεις με άλλες υπηρεσίες είναι δυνατές.

Επίπεδο κρισιμότητας 3: το δεύτερο και το τέταρτο επίπεδο των επιγραμμικά εξελιγμένων υπηρεσιών του ηλεκτρονικού λιμένος, με μέτριο επιχειρηματικό αντίκτυπο, παρέχονται σε ναυτιλιακές εταιρείες μέσω της αυτοματοποίησης των

παραδοσιακών επιχειρηματικών διαδικασιών, καθιστώντας τους ως το κύριο κανάλι συναλλαγών με το Δημόσιο (όχι μόνο σε εθνικό αλλά και σε ευρωπαϊκό ή διεθνές επίπεδο), για μια συγκεκριμένη υπηρεσία του οποίου η διάσπαση θα έχει σημαντική επίπτωση είτε την ασφάλεια ή την ιδιωτική ζωή ή ακόμα στις κρίσιμες εξαρτήσεις από άλλες υπηρεσίες.

Επίπεδο κρισιμότητας 4: το τρίτο και το τέταρτο επίπεδο των επιγραμμικά εξελιγμένων υπηρεσιών του ηλεκτρονικού λιμένος παρέχονται σε ναυτιλιακές εταιρείες, με μέτριο προς υψηλό επιχειρηματικό αντίκτυπο, μέσω της αυτοματοποίησης των παραδοσιακών ναυτιλιακών διεργασιών, καθιστώντας τους ως το κύριο κανάλι συναλλαγής (όχι μόνο σε εθνικό αλλά και σε ένα ευρωπαϊκό και διεθνές επίπεδο) για μια συγκεκριμένη υπηρεσία, η βλάβη της οποίας θα έχει σημαντική επίπτωση στην ασφάλεια ή / και τα ζητήματα προστασίας της ιδιωτικής ζωής ή / και στις κρίσιμες εξαρτήσεις από άλλες υπηρεσίες και ναυτιλιακές εταιρείες.

Επίπεδο κρισιμότητας 5: το τρίτο και το τέταρτο επίπεδο των επιγραμμικά εξελιγμένων υπηρεσιών του ηλεκτρονικού λιμένος παρέχονται σε ναυτιλιακές εταιρείες με υψηλό επιχειρηματικό αντίκτυπο, μέσω της αυτοματοποίησης των παραδοσιακών ναυτιλιακών, επιχειρησιακών και κυβερνητικών διεργασιών, καθιστώντας τις ως το κύριο κανάλι συναλλαγής (όχι μόνο σε εθνικό αλλά και σε ευρωπαϊκό ή διεθνές επίπεδο) για μια συγκεκριμένη υπηρεσία, η διάσπαση της οποίας θα έχει σημαντική επίπτωση στην ασφάλεια ή / και τα ζητήματα προστασίας της ιδιωτικής ζωής ή / και σε κρίσιμες εξαρτήσεις από άλλες ναυτιλιακές εταιρείες και, ειδικά, άλλες κρίσιμες υποδομές.

3.3 Διαχείριση Ασφαλείας CII

Δεδομένου ότι οι λιμένες αποτελούν υποδομές πληροφοριών ζωτικής σημασίας (CII) που φιλοξενούν κρίσιμα συστήματα PICT, τα διάφορα πρότυπα και οι μεθοδολογίες για την προστασία των κρίσιμων υποδομών πληροφοριών (CIIP) θα πρέπει επίσης να λαμβάνονται υπόψη στις μελλοντικές προσπάθειες για την δημιουργία στοχευμένων, αποτελεσματικών μεθοδολογιών διαχείρισης της ασφάλειας ICT, για συστήματα PICT.

Διάφορες μεθοδολογίες υπάρχουν, δίνοντας έμφαση στην CIIP. Οι περισσότερες από αυτές περιέχουν τις διαδικασίες, τους ορισμούς και τις επεξηγήσεις των τεχνικών που χρησιμοποιούνται για τη συλλογή και ανάλυση των πληροφοριών, στο πλαίσιο της CIIP. Οι μεθοδολογίες έχουν αξιολογηθεί [62] σύμφωνα με τα ακόλουθα κριτήρια:

- ***Διαθεσιμότητα***: η λειτουργία των υποστηριζόμενων εφαρμογών (σύμφωνα με την έρευνα (R) ή / και την ανάπτυξη (D)), είναι ήδη διαθέσιμη για χρήση είτε από το ευρύ κοινό, με εμπορικούς σκοπούς (C) ή από ολιγάριθμη ή περιορισμένη ομάδα, συνήθως στρατιωτική (L);
- ***επιτηδευμένο CI***: Οι τομείς κρίσιμης υποδομής (CI), που καλύπτονται με βάση το NIPP (2009) και την οδηγία 114/08 (CEU, 2008), περιλαμβάνουν: ηλεκτρική ενέργεια (1)· φυσικό αέριο (2)· το πετρέλαιο και τους αγωγούς (3)· πόσιμο νερό (4)· λύματα και υγρά απόβλητα (5)· βιομηχανικό έλεγχο (6)· τηλεπικοινωνίες (7)· δίκτυα υπολογιστών και συστήματα πληροφοριών (8)· σιδηροδρόμους (9)· αυτοκινητοδρόμους και οδούς (10)· ανθρώπινες δραστηριότητες, συμπεριλαμβανομένων των υπηρεσιών και εκκένωση έκτακτης ανάγκης (11)· τραπεζικό και χρηματοπιστωτικό τομέα (12). Επίσης, τα χαρακτηριστικά των πολιτικών και των κανονισμών (13),
- ***στάδιο***: η λειτουργικότητα που παρέχεται σε καθένα από τα στάδια των προγραμμάτων διαχείρισης του κινδύνου: αναγνώριση των περιουσιακών στοιχείων (α)· αξιολόγηση του κινδύνου (β)· ιεράρχηση των δράσεων (γ)· προγράμματα εφαρμογής (δ) και μέτρηση της αποτελεσματικότητας (ε).

Καθώς οι PICT ανήκουν στον τομέα των μεταφορών CII, μπορούμε να συμπεράνουμε ότι οι μεθοδολογίες CIIP που μπορεί να είναι κατάλληλες για να εφαρμοστούν (μετά από κατάλληλες τροποποιήσεις) στα PICT, είναι αυτές που επηρεάζουν: τις τηλεπικοινωνίες CIIP · τα δίκτυα υπολογιστών και συστήματα πληροφοριών · τους σιδηροδρόμους και τους αυτοκινητοδρόμους και δρόμους.

Οι κύριες μεθοδολογίες CIIP που μπορούν να εφαρμοστεί σε κρίσιμες υποδομές των λιμένων (καθώς και σε άλλους τομείς) αξιολογούνται στον ακόλουθο πίνακα:

CI μεθοδολογίες IP	Διαθεσιμότητα	Τομέας Γ	Στάδιο
ATHENA	L	1,2,3,4,5,6, **7,8,9,10** , 11,12,13	β
CI3	L	1,2,4,5,6, **7**	γ
CIP / DSS	L	1,2,3,4,5,6, **7,9,10** , 11,12,13	a, c, d, e
CIPMA	L	1,2,3, **7,8** , 12,13	δ, ε
DUTCH NRA	L	1,3,4, **10** , 11,13	α, β, γ
EAR / PILAR	C	**8** , 11,13	α, β, γ, δ
EMCAS	C	1, **7** , 12	α, β, γ
FAIT	L	1,2,5, **9**	α, β
FINSIM	R	7 , 12	α, β
FMEA / FMECA	C	6, **7** , 11,12	α, β, γ
FORT-FUTURE	L	1,2,3,4,5,6, **7,9,10** , 11,12,13	α, β, γ, ε
FTA	C	6, **7** , 11,12	α, β, γ
GIS Inter-operatibility	R	9, **10**	γ, ε
GoRAF	R	1,4,6, **8** , 11	β, γ, δ
HAZOP	C	1,2,3, **7** , 11,13	α, β, γ
IIM	R	1,4, **7,8,10** , 13	a, c, d
INTEPOINT VU	C	1, **7,9,10** , 11	γ
LUND	R	1, **9,10**	α, β
MARGERIT V2	C	**8** , 11,12,13	α, b, d
MIA	R	**7,8** , 13	α, β
MIN	R	**10** , 11	ένα
MUNICIPAL	R	1, **7,8**	a, c
N-ABLE	L	1, **9** , 12	a, c, d, e
NEMO	L	1,2,4, **9** , 13	γ, δ, ε
NSRAM	R	1, **7**	γ, δ, ε
Risk Maps	R	1,2,3,4,5,6, **7,9,10** , 11,12,13	A
TRAGIS	L	**9,10**	A
UIS	L	4,5, **7,10** , 11	α, β, γ, δ
VINCI	R	**8**	δ

Πίνακας 2 Αξιολόγηση των κατάλληλων μεθόδων CIIP

Μια σύντομη περιγραφή των παραπάνω μεθοδολογιών CIIP παρουσιάζεται στον παρακάτω πίνακα:

Μεθοδολογίες CIIP	Φύση	Περιγραφή
ATHENA	Εργαλείο λογισμικού	Παρέχει ένα μοντέλο για την ανάλυση ευαισθησίας των αλληλοεξαρτώμενων δικτύων υποδομής
Υποδομές ζωτικής σημασίας Αλληλεξαρτήσεις ολοκληρωτή (CI3)	Εργαλείο λογισμικού	Εκτιμήσεις του χρόνου αποκατάστασης και του κόστους των υπηρεσιών
Σύστημα υποστήριξης αποφάσεων προστασία υποδομών ζωτικής σημασίας (CIP / DSS)	Εργαλείο λογισμικού	Παρέχει υποστήριξη λήψης αποφάσεων για την CIIP, την σύγκριση της αποτελεσματικότητας των στρατηγικών για την μείωση της πιθανότητας ενός κινδύνου
Μοντελοποίηση προστασίας των κρίσιμων υποδομών και ανάλυση (CIPMA)	Εργαλείο λογισμικού	Αξιολογεί τις επιπτώσεις στη λειτουργία διακοπής των υπηρεσιών CII εντός και μεταξύ των τομέων
μοντέλο προσομοίωσης της οικονομίας των ΗΠΑ, βασισμένο σε παράγοντα (COMM-ASPEN)	Εργαλείο λογισμικού	Παρέχει προσομοιώσεις των αποτελεσμάτων των δύο αποφάσεων για την αγορά και τις διακοπές των υποδομών τηλεπικοινωνιών στην οικονομία, με βάση μία προσέγγιση παράγοντα
Περιστατικά ασφαλείας σε υπολογιστές της ομάδας απόκρισης (CERT / CSIRT)	Μεθοδολογία εργασίας	Σχεδιασμένο για την παραλαβή, την αναθεώρηση, την παρακολούθηση, τον συντονισμό και την ανταπόκριση, σε διάφορα περιστατικά ασφάλειας των υπολογιστών
DUTCH NRA	Μεθοδολογία εργασίας	Παρέχει μια προσέγγιση λήψης αποφάσεων πολλαπλών κριτηρίων για την αξιολόγηση του κινδύνου, σχετικά με τα πολιτικά και κοινωνικά ζητήματα
Procedimiento informatico-logico 'para el analisis de riesgos (EAR-PILAR)	Εργαλείο λογισμικού	Υποστηρίζει μια ολοκληρωμένη μέθοδο ανάλυσης κινδύνου
Προσαρμοστικό περίπλοκο σύστημα αγοράς ηλεκτρικής ενέργειας (EMCAS)	Εργαλείο λογισμικού	Παρέχει μια σε βάθος διερεύνηση των επιχειρησιακών και οικονομικών επιπτώσεων στο ηλεκτρικό σύστημα, όπως αυτή επηρεάζεται από διάφορα εξωγενή γεγονότα, με βάση μια προσέγγιση παράγοντα προσομοίωσης
Εργαλείο γρήγορης ανάλυσης υποδομής (FAIT)	Εργαλείο λογισμικού	Παρέχει ένα πλαίσιο για τη διενέργεια αξιολόγησης των οικονομικών επιπτώσεων σε πολλούς τομείς
Υποδομές του χρηματοπιστωτικού συστήματος (FINSIM)	Εργαλείο λογισμικού	Ισχύει για τα σενάρια της κρίσης που πλήττει το τραπεζικό σύστημα πληρωμών, την χρήση του πλαστικού χρήματος στην αγορά των ομοσπονδιακών κεφαλαίων και τις αλληλεπιδράσεις μεταξύ αυτών των οντοτήτων
Τρόποι αστοχίας και ανάλυση αποτελεσμάτων (FMEA-FMECA)	Μεθοδολογία εργασίας	Παρέχει μια διαδικαστική προσέγγιση για τον εντοπισμό και την ανάλυση πιθανών αστοχιών στον σχεδιασμό, την ανάπτυξη και την συντήρηση του συστήματος, με βάση την σοβαρότητα ή το αποτέλεσμα των αποτυχιών του συστήματος
FORT-FUTURE	Εργαλείο λογισμικού	Παρέχει ένα πλαίσιο που επιτρέπει στους ιθύνοντες να δοκιμάσουν σχεδόν πιθανές λύσεις που ενεργοποιούν πολλαπλές δυναμικές προσομοιώσεις
Ανάλυση δένδρου σφάλματος (FTA)	Μεθοδολογία εργασίας	Παρέχει μια μέθοδο για την ανάλυση της αποτυχίας, τον εντοπισμό των αιτιών που οδηγούν στην εκδήλωση του κινδύνου μέσα σε ένα σύστημα
Διαλειτουργικότητα (GIS)	Μεθοδολογία εργασίας	Χρήση Γεωγραφικών Συστημάτων Πληροφοριών, στον συντονισμό έκτακτης ανάγκης και την υποστήριξη για τη λήψη αποφάσεων
GORAF	Εργαλείο λογισμικού	Παρέχει ένα πλαίσιο για τον προσδιορισμό και την ανάλυση των πιο κρίσιμων πόρων μέσα σε μια υποδομή
Επικίνδυνες λειτουργίες-χειρισμοί (HAZOP)	Μεθοδολογία εργασίας	Υποστηρίζουν μια σειρά από τεχνικές για την αναγνώριση των δυνητικά επικίνδυνων συνθηκών και τους κινδύνους που

		βασίζονται σε υποθέσεις
Μοντέλο εισόδου-εξόδου διαλειτουργικότητας (IIM)	Εργαλείο λογισμικού	Παρέχει ένα ολοκληρωμένο πλαίσιο που θα βασίζεται σε αναλυτικά μοντέλα για τον εντοπισμό και την αντιμετώπιση κινδύνων που προέρχονται από την ενδο-και δια-σύνδεση των οικονομικών τομέων
INTEPOINT VU	Εργαλείο λογισμικού	Υιοθετεί ένα μοντέλο υποστήριξης αποφάσεων για την ανάλυση του σχεδιασμού απαντήσεων σε εκούσια και ακούσια γεγονότα
LUND	Μεθοδολογία εργασίας	Παρέχει μια μέθοδο για την αναπαράσταση ενός συστήματος οδικής ή σιδηροδρομικής υποδομής διασυνδεδεμένων μεταφορών
Metodologia de Analisis y Gestion de Riesgos delossistemas de Informacion (MARGERIT)	Μεθοδολογία εργασίας	Παρέχει μια προσέγγιση που δίνει έμφαση στην προστασία των υποδομών ICT
Μεθοδολογία για την αξιολόγηση των αλληλεξαρτήσεων (MIA)	Μεθοδολογία εργασίας	Αποσκοπεί στον εντοπισμό και την αξιολόγηση των αλληλεξαρτήσεων μεταξύ των κρίσιμων στοιχείων ICT
Multi-layer Infrastructure (MIN)	Εργαλείο λογισμικού	Παρέχει ένα δυναμικό παιγνιοθεωρητικό μοντέλο για την ανάλυση πολυστρωματικών δικτύων υποδομών
Πολυ-δίκτυο αλληλοεξαρτώμενων κρίσιμων προγραμμάτων υποδομής για την ανάλυση των χειραγωγών (MUNICIPAL)	Εργαλείο λογισμικού	Παρέχει ένα πλαίσιο για τον εντοπισμό, την ανάλυση και την αντιμετώπιση γεγονότων που επηρεάζουν την αλληλεξάρτηση των αστικών υποδομών
Εθνικό εργαστήριο για την οικονομία βασισμένο σε πράκτορες (N-ABLE)	Εργαλείο λογισμικού	Αναγνωρίζει και αναλύει οικονομικούς παράγοντες, ανατροφοδοτήσεις, ή αρνητικές επιπτώσεις των υποδομών των οδικών μεταφορών και της ηλεκτρικής ενέργειας
Μοντέλο χειρισμού, με βάση το δίκτυο -κεντρικά αποτελέσματα (NEMO)	Εργαλείο λογισμικού	Παρέχει ένα περιβάλλον για την υποστήριξη της λήψης αποφάσεων στον τομέα του σχεδιασμού ενός συστήματος υποδομής
Μοντέλο εκτίμησης κινδύνου προστασίας των δικτύων (NSRAM)	Εργαλείο λογισμικού	Αναλύσεις διασυνδεδεμένων δικτύων πολλαπλών υποδομών, προκειμένου να καθοριστεί η συμπεριφορά του συστήματος σε διάφορα είδη αρνητικών γεγονότων
Χάρτες κινδύνου	Μεθοδολογία εργασίας	Υποστηρίζει μια μέθοδο για τον εντοπισμό και την καταγραφή των κινδύνων, κατά συστηματικό και αποτελεσματικό τρόπο
Σύστημα ανάλυσης δρομολόγησης μεταφορών γεωγραφικών πληροφοριών (TRAGIS)	Εργαλείο λογισμικού	Παρέχει μια μέθοδο για τη βελτιστοποίηση των οδών μεταφοράς
Αστική ακολουθία υποδομής (UIS)	Εργαλείο λογισμικού	Παρέχει μια προσέγγιση που βασίζεται στην προσομοίωση αντιπροσωπεύουν αστικών υποδομών και πληθυσμών
Εικονική κοινότητα αλληλεπιδρώντων δικτύων (VINCI)	Μεθοδολογία εργασίας	Παρέχει εικονική αναπαράσταση της αρχιτεκτονικής του δικτύου των κρίσιμων υποδομών

Πίνακας 3 Σύντομη Περιγραφή Μεθοδολογιών CIIP

Αυτές οι μεθοδολογίες CIIP είναι διεθνικές και χρησιμοποιούν διαφορετικά κριτήρια αξιολόγησης των επιπτώσεων (π.χ. οικονομία, δημόσια υγεία και ασφάλεια, ψυχολογική / κοινωνική / δημόσια εμπιστοσύνη, πολυπλοκότητα, περιβάλλον, επιχειρήσεις, εθνική / εδαφική ασφάλεια). Αυτές οι μεθοδολογίες μπορούν να χρησιμοποιούνται στους λιμένες με κατάλληλες τροποποιήσεις.

Οι μεθοδολογίες CIIP που παρουσιάζονται σε αυτό το κεφάλαιο αφορούν κυρίως απειλές για την ασφάλεια, οι περισσότερες από τις οποίες υλοποιούνται σε εργαλεία λογισμικού. Οι υπόλοιπες είναι γενικές μεθοδολογίες.

Τα περισσότερα από τα πρότυπα CIIP και τις μεθοδολογίες είναι από τον τομέα της ενέργειας και, πιο συγκεκριμένα, από το Υπουργείο Ενέργειας των ΗΠΑ [61] και την Αξιόπιστη Ένωση Βόρειας Αμερικής (NERC) [3] . Από τα ογδόντα τρία (83) πρότυπα της μια ομάδα ειδικών προτύπων (CIP-002-3 και CIP-003-3), αφορά την προστασία των υποδομών ζωτικής σημασίας, αλλά μόνο για τα ηλεκτρικά συστήματα ενέργειας σε ένα πολύ αφηρημένο τρόπο. Ωστόσο, δεδομένου ότι είναι πολύ γενικά, μπορούν να παρέχουν μια εικόνα για τους λιμένες. Υπάρχουν διάφορες εθνικές μεθοδολογίες εκτίμησης επικινδυνότητας των κρίσιμων υποδομών, που χρησιμοποιούν διάφορους τρόπους για την εκτίμηση της κρισιμότητας της υποδομής, ακόμη και σε εθνικό επίπεδο (π.χ. στην Ολλανδία [36] [38]). Δεν υπάρχει ούτε ένας τυποποιημένος τρόπος για την εξέταση της κρισιμότητας μιας υποδομής ή / και την αντιμετώπιση των απειλών στον κυβερνοχώρο.

Κεφάλαιο 4: Προτάσεις για τη διαχείριση της ασφάλειας των συστημάτων PICT

Οι καλά γνωστές μεθοδολογίες διαχείρισης της ασφάλειας που παρουσιάστηκαν παραπάνω (π.χ. OCTAVE, CRAMM, Magerit, MEHARI και COBIT) δεν μπορούν να αντιμετωπίσουν (ως έχουν) τις νέες προκλήσεις, δεδομένου ότι: α) είναι πολύ γενικές και β) οι τρέχουσες ICT χαρακτηρίζονται από την αυξανόμενη πολυπλοκότητα, την διανομή, την παρέμβαση και την εξάρτηση με άλλες ICT και από την πληθώρα των ηλεκτρονικών υπηρεσιών φιλοξενίας. Αυτές τις μέρες, η ICT ενός οργανισμού (ιδίως των οργανώσεων αυτών, που φιλοξενούν τα CI) χρησιμοποιείται από μεγάλο αριθμό χρηστών (εσωτερικούς - εξωτερικούς διαχειριστές, χρήστες ή παρόχους), και αντιμετωπίζουν έναν αυξανόμενο αριθμό των διαφορετικών τύπων των χωρικών και χρονικών αποτελεσμάτων της διασποράς των επιθέσεων. Οι υφιστάμενες μεθοδολογίες και τα εργαλεία πρέπει να ενισχυθούν, προκειμένου να αντιμετωπίσουν τις προκλήσεις αυτές, μέσω της παροχής της συνεργασίας, του κόστους και του χρόνου υλοποίησης, αποκτώντας την γνώση των συμμετεχόντων όλων των ICT. Επιπλέον, θα πρέπει να αντιμετωπιστούν τα χαρακτηριστικά του τομέα επάνω στον οποίο εφαρμόζονται.

Αυτό είναι ένα γενικό πρόβλημα στην διαχείριση της προστασίας των νέων οργανισμών που φιλοξενούν διανεμημένα, πολύπλοκα και πολυδιάστατα συστήματα ICT, τα οποία αλληλεπιδρούν με άλλα πολύπλοκα κατανεμημένα συστήματα ICT.

4.1. Προϋποθέσεις για μια στοχευμένη μεθοδολογία διαχείρισης της ασφάλειας και το αντίστοιχο εργαλείο χειρισμού

Μια προτεινόμενη λύση για την καλύτερη αντιμετώπιση της προστασίας PICT είναι ο συνδυασμός των ISPS με τα πρότυπα διαχείρισης της προστασίας, στις ICT και CIIP. Ωστόσο, τα γνωστά πρότυπα διαχείρισης προστασίας που περιγράφονται ανωτέρω, θα χρειαστούν περαιτέρω τροποποιήσεις για να προσαρμοστούν με την ασφάλεια λιμένα ICT, έτσι ώστε να μπορούν να αντιμετωπίσουν τις ειδικές τομεακές απειλές, δηλαδή τις αλληλοεξαρτώμενες απειλές που προκύπτουν αυξανόμενες από όλους τους φορείς στο ναυτιλιακό περιβάλλον, συγκεκριμένες απειλές (π.χ. καιρικές συνθήκες, απεργίες) και την ναυτιλιακή νομοθεσία (π.χ. ISPS).

Μια στοχευμένη μεθοδολογία διαχείρισης προστασίας για τα συστήματα PICT θα πρέπει να αντιμετωπίσει τις ακόλουθες γενικές προϋποθέσεις:

- *Συμβατή με* τα πρότυπα: το πρότυπο ISO27001, τα πρότυπα CIIP και ISPS,
- *Συνεργασία*: Διασφάλιση συνεργασίας μεταξύ όλων των χρηστών ICT του λιμένα,
- *Αλληλοεξαρτήσεις*: Η ανάλυση αλληλεξάρτησης από και προς άλλα πιστωτικά ιδρύματα κρίνεται απαραίτητη,
- *Ευρεία ανάλυση*: Ανάλυση διασύνδεσης και αλληλεξάρτησης των απειλών και αξιολόγηση των άμεσων και έμμεσων κινδύνων,

- *Χρόνος και οικονομικοί πόροι:* να αποφευχθεί η πληθώρα των ερωτηματολογίων και να ματαιωθούν οι συνεντεύξεις με όλους τους εταίρους προκειμένου να εντοπιστεί η αρχιτεκτονική των ICT, η σημασία της προστασίας των επιμέρους επενδυτικών αγαθών ICT, οι αλληλεξαρτήσεις τους και οι αντίστοιχες απειλές τους,

- *Ευκολία εφαρμογής*: ο εμπειρογνώμονας δεν θα πρέπει να χρειάζεται υψηλό επίπεδο κατάρτισης για να εφαρμόσει τη μέθοδο,
- *Ανοιχτή:* αποφύγετε την προστασία μέσω της αδιαφάνειας,
- *Κάλυψη και των* έξι στρωμάτων PICT,
- *Κεντρικός χρήστης,*
- *Υποστήριξη από ένα αυτοματοποιημένο εργαλείο*: εφαρμογή της μεθοδολογίας με ένα συνεργατικό εργαλείο, φιλικό προς τον χρήστη ανοικτού κώδικα.

Οποιαδήποτε στοχευμένη μεθοδολογία θα πρέπει να υποστηρίζεται από ένα εργαλείο. Αυτό το εργαλείο θα χρησιμοποιηθεί από την ομάδα προστασίας του λιμένα, ώστε να διαχειριστεί η προστασία του. Ένα τέτοιο εργαλείο πρέπει να αντιμετωπίσει τις ακόλουθες γενικές προϋποθέσεις:

- *Υποστήριξη για την κωδικοποίηση της ασφάλειας των πληροφοριών διαχείρισης της γνώσης των κινδύνων*: Οι συμμετέχοντες θα πρέπει να είναι σε θέση να βρουν σχετικές γνώσεις διαχείρισης κινδύνων. Μια στρατηγική κωδικοποίηση ίσως λειτουργεί καλύτερα για ορισμένα είδη της γνώσης που δεν αναμένεται να αλλάζουν συχνά. Οι συμμετέχοντες μπορούν, στην συνέχεια, να ανακτήσουν εύκολα τις μεθόδους και τις βέλτιστες πρακτικές που έχουν αποδειχθεί στο παρελθόν, και την επαναχρησιμοποίηση τους αναλόγως.
- *Στήριξη για την διαχείριση ασφάλειας πληροφοριών εξατομίκευσης*: Επειδή η διαχείριση της προστασίας είναι η λήψη αποφάσεων συναίνεσης, η γνώση δεν είναι πάντα άμεσα «σταθερά» αρκετή για να κωδικοποιηθεί, διότι έως ότου επιτευχθεί συναίνεση, οι αποφάσεις θα μπορούσαν να αλλάξουν. Για τέτοια γνώση, μια στρατηγική εξατομίκευσης θα μπορούσε να αποδειχθεί χρήσιμη, επιτρέποντας στους συμμετέχοντες να βρουν ο'τιδήποτε. Επιπλέον, οι τεχνικές εξατομίκευσης θα πρέπει επίσης να είναι πολύτιμες για την υποστήριξη των συζητήσεων και των διαπραγματεύσεων μεταξύ των συμβαλλομένων μερών.
- *Υποστήριξη για την συνεργασία*: Επειδή η διαχείριση της προστασίας είναι η συναίνεση στη λήψη αποφάσεων, ένα εργαλείο ανταλλαγής γνώσεων πρέπει να υποστηρίζει άμεσα την συνεργασία μεταξύ των διαφόρων χρηστών. Αυτή η ιδιότητα επιτρέπει την ενεργό συμμετοχή όλων των σημαντικών φορέων, στην διαδικασία λήψης αποφάσεων.

- *Ρόλος-συγκεκριμένες απόψεις περιεχομένου*: Δεδομένου ότι η διαχείριση της προστασίας περιλαμβάνει τρεις λειτουργίες (εξάσκηση, άσκηση κριτικής και αναθεώρηση) στις οποίες εμπλέκονται συνήθως οι ρόλοι διαφορετικών συμμετεχόντων, το εργαλείο πρέπει να υποστηρίζει εξειδικευμένες απόψεις σχετικά με το διαθέσιμο περιεχόμενο, όπως τα ανοικτά ζητήματα ή την έγκριση αποφάσεων.
- *Περιγραφική προσέγγιση*: Δεδομένου ότι η διαδικασία διαχείρισης της προστασίας είναι εξαιρετικά δημιουργική, το εργαλείο ανταλλαγής γνώσεων δεν πρέπει να έχει δεσμευτικό χαρακτήρα. Μια πιο περιγραφική προσέγγιση προς τη διαχείριση της γνώσης θα διευκολύνει, με τον καλύτερο τρόπο, την δημιουργικότητα των συμμετεχόντων.
- *Προσανατολισμένη Υπηρεσία*: Όλα τα βήματα που εμπλέκονται στην μεθοδολογία διαχείρισης της προστασίας θα πρέπει να παρέχονται ως συνεργατικές υπηρεσίες.

Οι ανωτέρω απαιτήσεις έχουν ληφθεί υπόψη στο εθνικό -Ελληνικό- έργο *S-Port* [48], το οποίο μπορεί να χρησιμεύσει ως μια εθνική μελέτη περίπτωσης. Μια σύντομη περιγραφή των στόχων και των διδαγμάτων που αντλήθηκαν από το εν λόγω έργο παρουσιάζονται στις επόμενες ενότητες:

4.2. S-Port: Ένα ελληνικό έργο εθνικής υπόθεσης

Το εθνικό πρόγραμμα S-Port [58] θεωρεί τους λιμένες ως CII και θέτει δύο (2) κύριους στόχους:

- Την ανάπτυξη μιας στοχευμένης συνεργατικής μεθοδολογίας διαχείρισης κινδύνων για τα PICT-συστήματα που βασίζεται σε πρότυπα διαχείρισης της ασφάλειας ICT και τον κώδικα ISPS που αφορά όλους τους χρήστες PICT.

- Την ανάπτυξη ενός συνεργατικού εργαλείου διαχείρισης για την ασφάλεια των PICT-συστημάτων, που βασίζεται σε πρότυπα διαχείρισης της ασφάλειας ICT και τοη κώδικα ISPS για την συμμετοχή όλων των χρηστών PICT.

Ο πρώτος στόχος απευθύνεται στην S-Port εφαρμόζοντας την συνεργατική μεθοδολογία αξιολόγησης κινδύνου STORM-RM [42], [43], που βασίζεται στο

πρότυπο ISO27001 [29], AS / NZS 4360 [2]. Στο STORM-RM, εφαρμόζεται μία συνεργατική τεχνική λήψης αποφάσεων βασισμένη σε πολλαπλά κριτήρια, επιτρέποντας σε όλους τους χρήστες (εσωτερικούς και εξωτερικούς) να αξιολογήσουν τις επιπτώσεις, ανάλογα με την εμπειρία και τον ρόλο τους στην αλληλεπίδρασή τους με το υπό εκτίμηση σύστημα IT. Το STORM-RM έχει παραμετροποιηθεί για τα συστήματα PICT [43], εξετάζοντας τα επιπλέον PICT και τις απειλές στον κυβερνοχώρο και θέτοντας κριτήρια για την αξιολόγηση των επιπτώσεων που αυξάνονται από το γεγονός ότι τα λιμάνια είναι CII.

Ο δεύτερος στόχος των S-Port απευθύνεται στην ανάπτυξη ενός συνεργατικού περιβάλλοντος [45] (μια πρόσφατη τάση στον τομέα των διαδικτυακών υπηρεσιών που εφαρμόζονται σε διάφορους τομείς, π.χ. το ηλεκτρονικό εμπόριο [43], [33], [44] τον ηλεκτρονικό λιμένα [48] και την ηλεκτρονική μετανάστευση [53], [54], [22]) με την χρήση καινοτόμων τεχνολογιών Web 2.0.

Στο συνεργατικό περιβάλλον S-Port, η στοχευμένη μεθοδολογία διαχείρισης κινδύνων προσφέρεται, ως συνεργατική υπηρεσία S-Port, στους χρήστες PICT. Πρόσθετες S-Port υπηρεσίες συνεργατικής διαχείρισης της ασφάλειας προσφέρονται μέσω του περιβάλλοντος S-Port, συμπεριλαμβανομένων της χαρτογραφίας: γραφική αναπαράσταση των υποδομών PICT και εντοπισμός όλων των επενδυτικών αγαθών των συστημάτων PICT · Αναφορά: γενιά της ασφάλειας των εγγράφων, π.χ. πολιτικές ασφάλειας, σχέδια επιχειρησιακής συνέχειας, σχέδια αποκατάστασης καταστροφών (όπως καλλιέργεια, έγγραφα)· συνεργατικές υπηρεσίες Web2.0: ιστοσελίδες συζήτησης, ιστοσελίδες κοινωνικής δικτύωσης και συζήτησης / γνωριμιών, δημοσκοπήσεις, ερωτηματολόγια, για την οικοδόμηση κοινωνικών αλληλεπιδράσεων στην επίλυση και συζήτηση θεμάτων ασφάλειας.

Τα διδάγματα από αυτό το εθνικό έργο μπορούν να συνοψιστούν ως εξής:

- Οι συμμετέχοντες λιμένες (παρόλο που ήταν όλοι ελληνικοί) χρησιμοποιούσαν διαφορετικά συστήματα PICT από διάφορους παρόχους, και διαφορετική αρχιτεκτονική·
- Είχαν μια διαφορετική κουλτούρα ασφάλειας (χρησιμοποιούσαν διαφορετικές πρακτικές ασφαλείας)·

- Οι πολιτικές ασφάλειας δεν ανανεώθηκαν κατάλληλα (μετά από μία αλλαγή στο σύστημα PICT)·
- Οι υπηρεσίες ηλεκτρονικού λιμένος βρίσκονταν στα επίπεδα κρισιμότητας 1-2 και δεν ήταν διαλειτουργικές.
- Η S-Port ανάλυση των απειλών των επενδυτικών αγαθών από έναν από τους εμπλεκόμενους λιμένες αποκαλύπτει τις απειλές που μπορεί ένας λιμένας να αντιμετωπίσει και τους λόγους που προκάλεσαν αυτές τις απειλές.

4.3. Συμπεράσματα

Η διαχείριση των κινδύνων για την προστασία πληροφοριών είναι μια σημαντική ανησυχία των οργανώσεων σε όλο τον κόσμο και, ιδιαίτερα, για τις CII. Αν και υπάρχουν πολλές διαθέσιμες μεθοδολογίες διαχείρισης της προστασίας, κανένας από αυτούς τους στόχους δεν πληρεί τις ανάγκες των σημερινών πολύπλοκων συστημάτων ICT (που διανέμονται και διασυνδέονται με άλλα συστήματα ICT και χειρίζονται πληθώρα δεδομένων και υπηρεσιών).

Σε αυτό το κεφάλαιο, προτείνονται γενικές απαιτήσεις για την ανάπτυξη νέων ή την βελτίωση των υφιστάμενων μεθόδων διαχείρισης κινδύνων, για την προστασία πληροφοριών, προκειμένου να αντεπεξέλθουν στις σημερινές ανάγκες. Παρέχονται επίσης επιπλέον γενικές απαιτήσεις για ένα συνεργατικό σύστημα, καθοδηγώντας τους διαχειριστές να διαχειρίζονται οι ίδιοι την προστασία τους.

Οι βελτιωμένες μεθοδολογίες θα πρέπει να είναι σε θέση να παραμετροποιηθούν, σύμφωνα με τις ανάγκες των κλάδων. Ως καλή πρακτική, που υλοποιεί αυτές τις απαιτήσεις, είναι το εθνικό σχέδιο *S-Port* και παρουσιάζεται εδώ, ελπίζοντας ότι το παράδειγμα αυτό θα ανοίξει το δρόμο για περαιτέρω εξελίξεις, στον τομέα της συνεργατικής διαχείρισης της προστασίας, που μπορεί να εφαρμοστεί στον τομέα της ναυτιλίας. Το S-Port εφάρμοσε την συνεργατική μεθοδολογία διαχείρισης προστασίας, το STORM-RM (παραμετροποιημένο για τα συστήματα λιμένος ICT), προκειμένου να εντοπιστεί και να αντιμετωπιστεί το διαφορετικό είδος των απειλών που καταπολεμούν τα συστήματα PICT. Η παρουσιαζόμενη μεθοδολογία βασίζεται στη μέθοδο λήψης αποφάσεων της ομάδας, AHP [55], δεδομένου ότι θεωρεί την

διαχείριση κινδύνων ως πολυκριτηριακή απόφαση λήψης, πρόβλημα που αφορά όλους τους συμμετέχοντες φορείς PICT, με διαφορετικές και αντικρουόμενες απαιτήσεις και ανάγκες αξιοποιώντας την πείρα, τις γνώσεις και την εμπειρία τους.

Κεφάλαιο 5: Ναυτιλιακά νέφη

Οι ναυτιλιακές δραστηριότητες επλήγησαν σοβαρά από την πιο πρόσφατη οικονομική κρίση, αλλά την ίδια στιγμή θα είναι στο επίκεντρο της περιφερειακής και της ευρωπαϊκής οικονομικής ανάκαμψης. Οι διασυνοριακές, αποτελεσματικές, αξιόπιστες υπηρεσίες ηλεκτρονικού λιμένος θα επιταχύνουν την παρουσία τους στην ψηφιακή ναυτιλιακή αγορά, βελτιώνοντας την οικονομία του κλάδου και την οικονομίας της ΕΕ, στο σύνολό της. Η κύρια οικονομική κινητήρια δύναμη για τους λιμένες προκύπτει από τις υπηρεσίες ηλεκτρονικού λιμένος. Η εξέλιξη τους σε διασυνοριακές, αποτελεσματικές, ασφαλείς υπηρεσίες ηλεκτρονικού λιμένος θα επιταχύνει την παρουσία τους στην πολλά υποσχόμενη ψηφιακή ναυτιλιακή αγορά, θεωρώντας ότι εναρμονίζονται οι ψηφιακές πρακτικές προστασίας που διασφαλίζουν την ανταλλαγή πληροφοριών και την δημιουργία γνώσης. Ωστόσο, οι λιμένες δεν διαθέτουν τους πόρους για επένδυση, προκειμένου να ενισχυθούν οι ηλεκτρονικές τους υπηρεσίες και να γίνουν ανταγωνιστικές.

Η υιοθέτηση της τεχνολογίας *Cloud Computing* μπορεί να φέρει μια νέα επανάσταση στον ναυτιλιακό τομέα, επιτρέποντας ένα ολιστικό συνεργατικό περιβάλλον. Το περιβάλλον αυτό προσφέρει διασυνοριακές, αξιόπιστες ηλεκτρονικές υπηρεσίες, σε όλους τους εμπορικούς λιμένες και τους χρήστες τους, με οικονομικά αποδοτικό τρόπο, καθώς φιλοξενείται είτε από μια κεντρική αξιόπιστη αρχή της ΕΕ (π.χ. Ευρωπαϊκή Κοινότητα για τις Ναυτιλιακές Υποθέσεις, EMSA, IMO) που ενεργεί ως πάροχος νεφών στα πλαίσια της Ευρωπαϊκής Ένωσης, ή από μια εθνική αρχή (π.χ. Υπουργείο Ναυτιλίας), που ενεργεί ως εθνικός πάροχος νεφών.

Τα κύρια πλεονεκτήματα της υιοθέτησης της τεχνολογίας *Cloud Computing* στην παροχή λιμενικών υπηρεσιών νέφους, περιλαμβάνουν:

1. Μείωση της ανάπτυξης και των λειτουργικών εξόδων,
2. *Επεκτασιμότητα*: οι υπηρεσίες μπορούν να χρησιμοποιηθούν από πολλούς χρήστες,
3. Μείωση του χρόνου εκτέλεσης και του χρόνου απόκρισης,
4. Ποιότητα των υπηρεσιών,
5. Θέματα προστασίας, απορρήτου και διαλειτουργικότητας θα επιλυθούν σε κεντρικό επίπεδο, καθώς θα πρέπει να γίνεται από τον πάροχο της τεχνολογίας νεφών,
6. Εύκολη πρόσβαση, μέσω ενός προγράμματος περιήγησης, ή σύνδεση μέσω διαφόρων συσκευών (κινητά τερματικά, υπολογιστές, κλπ) από οπουδήποτε, ανά πάσα στιγμή,
7. *Εύκολο στη χρήση*: Οι χρήστες είναι εξοικειωμένοι με την χρήση και μπορούν να περιηγηθούν εύκολα, μέσα από τα προγράμματα περιήγησης στο Διαδίκτυο. Δεν απαιτούνται εξειδικευμένες γνώσεις, για τη χρήση των υπηρεσιών ή των αιτήσεων,
8. Οικονομία κλίμακας.

5.1. Εφαρμογές Νεφών

Υπάρχουν διάφοροι τύποι των νεφών που μπορούν να εφαρμοστούν στον τομέα της ναυτιλίας: Ένα *ιδιωτικό νέφος* είναι περιορισμένο εντός των ορίων μιας συγκεκριμένης επιχείρησης ή ενός περιβάλλοντος. Ένα ναυτιλιακό ιδιωτικό νέφος μπορεί να εφαρμοστεί σε τοπικό επίπεδο, προσφέροντας υπηρεσίες ηλεκτρονικού λιμένος σε έναν εγχώριο λιμένα. Ένα ιδιωτικό νέφος που χρησιμοποιείται από άλλη επιχείρηση με παρόμοια ενδιαφέροντα, ομάδες-στόχους και πολιτικές (π.χ. ασφάλεια, προστασία της ιδιωτικής ζωής και πιστοποιητικό) ονομάζεται *κοινότητα νέφους*. Μια κοινότητα νέφους των ναυτιλιακών μεταφορών μπορεί να εφαρμοστεί σε εθνικό, περιφερειακό ή ευρωπαϊκό επίπεδο προσφέροντας διασυνοριακές ηλεκτρονικές λιμενικές υπηρεσίες σε έναν εθνικό, περιφερειακό ή ευρωπαϊκό λιμένα (ονομάζεται ναυτιλιακό εθνικό / περιφερειακό / ευρωπαϊκό νέφος αντίστοιχα). Όταν ένα νέφος παρέχει υπηρεσίες στο ευρύ κοινό χωρίς περιορισμούς, παρόμοια με το παραπάνω, τότε έχουμε το *δημόσιο νέφος*. Ένα ευρωπαϊκό ναυτιλιακό νέφος θα μπορούσε να εφαρμοστεί προκειμένου να προσφέρει επιγραμμικές ηλεκτρονικές υπηρεσίες, επιπέδου πολυπλοκότητας 1 και 2, ή υπηρεσίες με τα επίπεδα κρισιμότητας 0 και 1 π.χ. υπηρεσίες πληροφόρησης: προγραμματισμός, πλοηγήσεις, πληροφορίες για κρουαζιέρες σε όλους τους εγχώριους και ευρωπαϊκούς λιμένες, καθώς και στους χρήστες τους. Τέλος, ένα *υβριδικό νέφος* είναι ένας συνδυασμός των προηγούμενων τύπων. Ένα ναυτιλιακό υβριδικό νέφος μπορεί να εφαρμοστεί για να προσφέρει υπηρεσίες προς το ευρύ κοινό, αλλά και να παρέχει ηλεκτρονικές υπηρεσίες, σε όλα τα επίπεδα της κρισιμότητας, στους διάφορους λιμένες (είτε σε εθνικό, περιφερειακό ή ευρωπαϊκό δίκτυο).

Η υλοποίηση μιας υποδομής νέφους μπορεί να είναι οικονομικά αποδοτική, δεδομένου ότι υπάρχουν πολλές λύσεις ανοιχτού κώδικα, όπως οι OpenStack [52], Eucalyptus [10], OpenNebula [51], Nimbus [40], Ubuntu [60], EyeOS [24], Collectd [12], BitNami Cloud Hosting [5], οι οποίες μπορεί να αξιοποιηθούν από τον πάροχο των ναυτιλιακών νεφών, προκειμένου να οικοδομηθεί μια οικονομικά αποδοτική υποδομή νέφους.

5.2. Οι υπηρεσίες θαλάσσιων νεφών

Η ασφάλεια και η διαχείριση της ιδιωτικής ζωής, η παρακολούθηση και ο έλεγχος θα μπορούσαν να παρέχονται σε όλους τους ευρωπαϊκούς εμπορικούς λιμένες από μια υπηρεσία ναυτιλιακού νέφους, την *προστασία ως υπηρεσία* που προσφέρεται από μια αξιόπιστη ναυτιλιακή οργάνωση (π.χ. την EMSA). Αυτό θα επιτρέψει την παροχή της προστασίας και της ιδιωτικότητας, με βάση ενιαία πρότυπα και μεθοδολογίες, που επιτρέπουν την πιστοποίηση και την παροχή αξιόπιστων, διασυνοριακών ναυτιλιακών υπηρεσιών. Για παράδειγμα, το S-Port θα μπορούσε να προσφέρεται ως υπηρεσία νέφους διαχείρισης της προστασίας, για τα συστημάτα PICT τα οποία προσφέρονται από τον πάροχο των ναυτιλιακών νεφών.

Η Διαχείριση της Ταυτότητας ως υπηρεσία μπορεί επίσης να παρέχεται ως υπηρεσία νέφους, η οποία εγκρίθηκε από την αρμόδια κεντρική αρχή που επιτρέπει την εξακρίβωση της γνησιότητας των ναυτιλιακών εταίρων και την έκδοση της εντολής της άδειας και των μαρκών. Σε αυτήν την *κεντρική* επιλογή, μια ναυτιλιακή αρχή ενεργεί ως πάροχος νέφους, αναλαμβάνει τη διαχείριση των διαφορετικών ονομάτων, της ταυτότητας όλων των συμμετεχόντων φορέων και την έκδοση των μαρκών της άδειας, χρησιμοποιώντας το κεντρικό σύστημα διαχείρισης της ταυτότητας.

Μια άλλη επιλογή είναι η εναλλακτική λύση *Federated*, όπου οι τοπικοί, εθνικοί και περιφερειακοί πάροχοι ναυτιλιακού νέφους συμφωνούν να εμπιστεύονται, ο ένας στον άλλο, την εξακρίβωση της γνησιότητας και τις πληροφορίες εξουσιοδότησης που περνούν, και να θεσπίσουν κανόνες και πολιτικές για να βεβαιωθούν ότι μπορεί να αντιμετωπιστεί αυτή η εμπιστοσύνη. Αυτή η συνεργασία εμπιστοσύνης είναι γνωστή ως Ομοσπονδία. Εντός της Ομοσπονδίας, οι σχετικές με τους χρήστες πληροφορίες είναι διαθέσιμες μόνο στον πάροχο των ναυτιλιακών νεφών, με τον οποίο ο χρήστης συνδέεται, καθώς υπάρχουν κεντρικά σημεία της διαχείρισης ταυτότητας. Είναι η άδεια να έχουν πρόσβαση σε πόρους, που μοιράζεται παρά τα προσωπικά στοιχεία του χρήστη. Αυτή η ικανότητα μπορεί επίσης να αξιοποιηθεί σε ναυτιλιακά νέφη ομοσπονδιών.

Υπάρχουν πολλές τεχνολογικές λύσεις, για την εφαρμογή της κεντρικής και της ομόσπονδης διαχείρισης ταυτότητας, οι οποίες μπορούν να χρησιμοποιηθούν από

πιθανούς παρόχους ναυτιλιακού νέφους. Οι τεχνολογίες αυτές ορίζουν ένα σύνολο πρωτοκόλλων για την ασφαλή ανταλλαγή των πληροφοριών ταυτότητας, τα οποία μπορούν να χρησιμοποιηθούν μεταξύ των παρόχων νεφών. Μεταξύ των κοινών προτύπων στα οποία μπορούν να βασίζονται είναι: το SAML [49] και το Liberty Alliance [34], το WS-Federation [35] και το WS-Trust [6].

Τέλος, *όλες οι ηλεκτρονικές υπηρεσίες λιμένος*, μπορούν να προσφέρονται από (εθνικούς, περιφερειακούς, ευρωπαϊκούς) παροχείς ναυτιλιακών νεφών, σε όλους τους λιμένες της Ευρωπαϊκής Ένωσης, προκειμένου να επιτευχθεί η διαλειτουργικότητα και μία ολοκληρωμένη ναυτιλιακή πολιτική.

5.3. Συμπεράσματα

Οι εμπορικοί λιμένες υποδέχονται, αποθηκεύουν ή ανταλλάσουν πληροφορίες και δεδομένα, με σκοπό την παροχή των ναυτιλιακών εταίρων με ηλεκτρονικές και κινητές, λιμενικές και ναυτιλιακές υπηρεσίες. Είναι προφανές, ότι ένας μεγάλος αριθμός προβλημάτων που παρουσιάζονται στους λιμένες, συνδέονται είτε με την έλλειψη των πληροφοριών, ή με την απουσία αυτοματοποίησης και ολοκλήρωσης των ενιαίων ναυτιλιακών επιχειρήσεων των παρεχόμενων υπηρεσιών. Το πιο σημαντικό, τα λιμάνια δεν διαθέτουν τους πόρους (λόγω της οικονομικής κρίσης) για την κατασκευή καινοτόμων, διασυνοριακών, αξιόπιστων υπηρεσιών ηλεκτρονικού λιμένος, οι οποίοι θα τα καταστήσουν πιο ανταγωνιστικά στις συγκριτικές αγορές ναυτιλιακών μεταφορών και θα συμβάλουν προς την κατεύθυνση μιας οικονομικής ανάκαμψης, στην Ευρωπαϊκή Ένωση.

Η υιοθέτηση της τεχνολογίας *Cloud Computing* μπορεί να φέρει μια νέα επανάσταση, στον τομέα των ναυτιλιακών μεταφορών, επιτρέποντας ένα ολιστικό συνεργατικό περιβάλλον. Έτσι, προσφέρονται διασυνοριακές αξιόπιστες ηλεκτρονικές υπηρεσίες, σε όλους τους εμπορικούς λιμένες και τους χρήστες τους, με οικονομικά αποδοτικό τρόπο.

Η παροχή αξιόπιστων πληροφοριών άμεσης επεξεργασίας της αίτησης και βελτιωμένων ναυτιλιακών υπηρεσιών μέσω ναυτιλιακού νέφους, αξιοποιώντας την γνωστή τεχνολογία Cloud Computing, θα μπορούσε να είναι το επόμενο βήμα για την

επίλυση των θεμάτων αυτών. Διάφοροι τύποι των νεφών (π.χ. ιδιωτικά, κοινότητας, δημόσια και υβριδικά) μπορούν να εφαρμοστούν, προκειμένου να προσφέρουν υπηρεσίες ναυτιλιακών νεφών, σε σχέση με μία ποικιλία από ανταγωνιστικές, καινοτόμες, διασυνοριακές υπηρεσίες ναυτιλιακών νεφών (π.χ. ασφάλεια ως υπηρεσία, διαχείριση ταυτότητας όπως μια υπηρεσία, υπηρεσίες ηλεκτρονικού λιμένος), σε εθνικό, περιφερειακό και ευρωπαϊκό επίπεδο.

Οι ναυτιλιακές υπηρεσίες νεφών θα λύσουν το πρόβλημα της διαλειτουργικότητας των διασυνοριακών υπηρεσιών, ενισχύοντας τον ευρωπαϊκό τομέα ναυτιλιακής αγοράς προς μια ολιστική προσέγγιση, συμβάλλοντας στην υλοποίηση μιας ευρωπαϊκής ολοκληρωμένης ναυτιλιακής πολιτικής.

Κεφάλαιο 6: Συνολικά συμπεράσματα και συστάσεις

Οι λιμένες είναι σημαντικοί φορείς παροχής υπηρεσιών, ωστόσο δεν υιοθετούν τις «Καλές πρακτικές προστασίας ICT και ιδιωτικής ζωής», δηλαδή δεν ασχολούνται αποτελεσματικά με την ασφάλεια ICT (π.χ. επιθέσεις, μεταμφιεσμένες ταυτότητες, παρακολούθηση της κυκλοφορίας δικτύου) ή απειλές προστασίας της ιδιωτικής ζωής (π.χ. κλοπή / τροποποίηση των προσωπικών δεδομένων)· δεν εφαρμόζουν τα μέτρα προστασίας με τις τεχνολογίες που χρησιμοποιούν (π.χ. RFID), θέτοντας έτσι σε κίνδυνο (π.χ. απώλεια φήμης, απώλεια της νομικής συμμόρφωσης, διακοπή της λειτουργίας των επιχειρήσεων) όχι μόνο τους ιδίους, αλλά ολόκληρη την αλυσίδα των ναυτιλιακών αξιών. Η ICT συμπεριφορά τους για την προστασία γίνεται ένα σημαντικό πρόβλημα, που μπορεί να έχει επιχειρησιακές επιπτώσεις στους υπόλοιπος εταίρους του ναυτιλιακού περιβάλλοντος. Μπορούν να χαρακτηριστούν ως αδύναμοι κρίκοι, στην ασφάλεια των πληροφοριών.

6.1. Κατάταξη συμπερασμάτων

1. Η προστασία και η ασφάλεια είναι δύο έννοιες αλληλένδετες· στον τομέα των θαλάσσιων μεταφορών, αυτές οι δύο έννοιες χρησιμοποιούνται εναλλακτικά, προκαλώντας παρεξηγήσεις. Τα υφιστάμενα πρότυπα προστασίας των θαλάσσιων μεταφορών, οι μεθοδολογίες και τα εργαλεία επικεντρώνονται μόνο στην φυσική προστασία των λιμένων (*ασφάλεια*), ιδίως όσον αφορά τον έλεγχο πρόσβασης των υποδομών των λιμένων, σε σχέση με την ασφάλεια των πλοίων. Με άλλα λόγια, ασχολούνται μόνο με το πρώτο στρώμα (υποδομή) και την τελευταία στρώση (χρήστες) του συστήματος PICT. Μόνο τα δύο συστατικά του ελέγχου της προστασίας, δηλαδή η πρόσβαση και η διαθεσιμότητα, αγνοούν όλα τα άλλα στρώματα και συστατικά, καθιστώντας τα λιμάνια αδύναμους κρίκους προστασίας. Επιπλέον, οι λιμένες δεν θεωρούνται υποδομές κρίσιμης σημασίας και η προστασία PICT τους δεν είναι οργανωμένη, διαχειρίσιμη, κατοχυρωμένη, πιστοποιημένη ή δεν ελέγχεται ως τέτοια.

3. Οι προσπάθειες της ισχύουσας ναυτιλιακής νομοθεσίας ή προτυποποίησης δεν καλύπτουν επαρκώς την ασφάλεια ICT των εμπορικών λιμένων. Ειδικότερα, οι εμπορικοί λιμένες δεν αντιμετωπίζονται ως ανεξάρτητες κρίσιμες υποδομές φιλοξενίας των κρισίμων συστημάτων ICT, αλληλεπιδρώντας με πολλούς φορείς, και η προστασία τους δεν αξιολογείται ή διαχειρίζεται με έναν ολιστικό, αποτελεσματικό τρόπο. Το γεγονός, ότι οι λιμένες αποτελούν υποδομές ζωτικής σημασίας, κυοφορεί συγκεκριμένες απειλές (π.χ. από απεργίες, τρομοκρατικές επιθέσεις, καιρικές συνθήκες). Καθώς οι ταυτοποιήσεις και οι επιπτώσεις (π.χ. στην εθνική οικονομία, την εθνική ασφάλεια, η διατάραξη της δημόσιας τάξης) αγνοούνται, οι αξιολογήσεις κινδύνου είναι ανακριβείς. Οι προσπάθειες της ναυτιλιακής προτυποποίησης επικεντρώνονται μόνο στην σωματική ασφάλεια των λιμένων, αφήνοντας απροστάτευτα τα συστήματα PICT από απειλές στον κυβερνοχώρο και, κατά συνέπεια, οι ηλεκτρονικές υπηρεσίες λιμένος και τα δεδομένα που προσφέρονται από τα συστήματα PICT είναι σε κίνδυνο. Οι συνεργατικές δράσεις και συνέργειες μεταξύ των διαφόρων φορέων (π.χ. IMO, EMSA, η

ΓΔ MARE, DG MOVE, DG INFSO) πρέπει να στηριχθούν, για να αντιμετωπιστεί κατάλληλα η διαχείριση προστασίας των συστημάτων PICT.

4. Οι θαλάσσιες δραστηριότητες επλήγησαν σοβαρά από την πιο πρόσφατη οικονομική κρίση, αλλά την ίδια στιγμή θα είναι στο επίκεντρο της περιφερειακής και ευρωπαϊκής οικονομικής ανάκαμψης. Οι διασυνοριακές, αποτελεσματικές, περιφερειακές υπηρεσίες ηλεκτρονικού λιμένος θα επιταχύνουν την παρουσία τους στην πολλά υποσχόμενη ψηφιακή ναυτιλιακή αγορά, υπό την προϋπόθεση ότι έχουν εναρμονιστεί οι ψηφιακές πρακτικές προστασίας, διασφαλίζοντας την ανταλλαγή πληροφοριών και την δημιουργία γνώσης. Έτσι, η αξιόπιστη, διασυνοριακή τροφοδότηση των υπηρεσιών ηλεκτρονικού λιμένος πρέπει να εξασφαλίζεται, για την προώθηση των τοπικών, εθνικών, περιφερειακών και ευρωπαϊκών οικονομιών και την ανάπτυξη των εμπορικών τους δραστηριοτήτων, στην ψηφιακή εποχή. Οι ευρωπαϊκές οικονομίες στηρίζονται ακόμη περισσότερο στις ναυτιλιακές επιχειρηματικές τους δραστηριότητες. Απαραίτητη προϋπόθεση για την κατασκευή των διασυνοριακών ηλεκτρονικών-λιμενικών υπηρεσιών είναι η δημιουργία της πολλαπλά διαβαθμισμένης Αρχής Πιστοποίησης της Ευρωπαϊκής Ένωσης, προσφέροντας διασυνοριακές υπηρεσίες προστασίας (π.χ. αναγνωρισμένα ψηφιακά πιστοποιητικά, ψηφιακά πιστοποιητικά), στους ναυτιλιακούς εταίρους.

5. Οι τεχνολογίες που χρησιμοποιούνται στη αξιοποίηση των υπηρεσιών ηλεκτρονικού λιμένος πρέπει να προστατεύονται. Για παράδειγμα, η Αναγνώριση Συχνότητας Ραδιοκυμάτων (RFID), που χρησιμοποιείται συνήθως στα λογιστικά ενός λιμένος, στην διαχείριση των εμπορευματοκιβωτίων και του φορτίου αντιμετωπίζει διάφορες απειλές. Συνιστάται η πιστοποίηση (π.χ. κοινά κριτήρια) των συστημάτων και των τεχνολογιών.

6. Η δημιουργία του νέου προτύπου ναυτιλιακής προστασίας δεν συνιστάται (η διαδικασία τυποποίησης είναι χρονοβόρα) και δεν είναι απαραίτητη, δεδομένου ότι τα υπάρχοντα πρότυπα ISPS, ICT και CIIP είναι επαρκή. Η ολιστική προσέγγιση για την διαχείριση της ασφάλειας των συστημάτων PICT που η μελέτη αυτή προτείνει, είναι η δημιουργία στοχευμένων μεθοδολογιών

διαχείρισης της προστασίας, για τα συστήματα PICT, συμβατών με τα πρότυπα ναυτικής ασφάλειας (π.χ. κώδικας ISPS) και τα πρότυπα διαχείρισης της ασφάλειας ICT και CIIP.

7. Μια γενική σύσταση αφορά την ενίσχυση των υφισταμένων μεθοδολογιών για τη διαχείριση προστασίας ICT, υποδεικνύοντας ότι οι απαιτήσεις και τα χαρακτηριστικά των σημερινών επιχειρήσεων (π.χ. κατανεμημένο, πολύπλοκο, εξαιρετικά διαδραστικό ICT) πρέπει να αναπτυχθούν από τα υπάρχοντα συστήματα (π.χ. OCTAVE, CRAMM, EBIOS, Magerit). Η κατάσταση αυτή δεν καθιστά δυνατή την συνεργασία και δεν εξετάζει όλα τα κριτήρια (τεχνολογικά, επιχειρηματικά, νομικά, οικονομικά), που επηρεάζουν την αξιολόγηση των απομονωμένων και αλληλοεξαρτώμενων απειλών ICT και των τρωτών σημείων των σημερινών επιχειρήσεων, οδηγώντας σε ελλιπή, αναποτελεσματική και μη αντικειμενική διαχείριση των κινδύνων. Επιπλέον, αυτές οι παραδοσιακές μεθοδολογίες RM απαιτούν πληθώρα συνεχών συνεντεύξεων με όλους τους συμμετέχοντες, προκειμένου να εντοπιστεί η αρχιτεκτονική των ICT, η σημασία της ασφάλειας των επιμέρους επενδυτικών αγαθών ICT, οι αλληλεξαρτήσεις τους και οι αντίστοιχες απειλές τους· κάνοντας αυτές τις μεθοδολογίες ακατάλληλες (δαπανηρές, ανεπαρκείς, λόγω του χρόνου και των πόρων που καταναλώνουν), για τις τρέχουσες μεγάλες κατανεμημένες επιχειρήσεις (π.χ. λιμένες). Οι μεθοδολογίες αυτές είναι πολύ γενικές και γίνονται κουραστικές, όταν εφαρμόζονται σε συγκεκριμένους τομείς (π.χ. στην θάλασσα). Αυτό είναι ένα γενικό πρόβλημα που ισχύει και για τους λιμένες.

8. Μια στοχευμένη μεθοδολογία διαχείρισης της ασφάλειας για τα συστήματα PICT θα πρέπει να αντιμετωπίσει τις ακόλουθες γενικές προϋποθέσεις:

- *Συμμόρφωση με τα πρότυπα*: το πρότυπο ISO27001, AS / NZS 4360, τα πρότυπα CIIP και οι ISPS,

- *Συνεργασία*: Διασφάλιση συνεργασίας μεταξύ όλων των χρηστών ICT του λιμένα,
- *Ευρεία ανάλυση*: Ανάλυση διασύνδεσης και αλληλεξάρτησης των απειλών και αξιολόγηση των άμεσων και έμμεσων κινδύνων,

- *Χρόνος και οικονομικοί πόροι*: να αποφευχθεί η πληθώρα των ερωτηματολογίων και απογοητευτικών συνεντεύξεων· δεν θα πρέπει να λαμβάνονται υπόψη οι απειλές που δεν ισχύουν για τα λιμάνια του περιβάλλοντος,

- *Ευκολία στην εφαρμογή*: να εφαρμοστεί η μεθοδολογία σε ένα φιλικό προς το χρήστη εργαλείο συνεργασίας ανοιχτής πηγής.

Οι βελτιωμένες μεθοδολογίες θα πρέπει να είναι πολύ συγκεκριμένες (σταδιακή προσέγγιση) και η εφαρμογή τους δεν θα πρέπει να αφεθεί σε εθνικό επίπεδο. Ορισμένα καινοτόμα, συνεργατικά εργαλεία διαχείρισης προστασίας θα πρέπει να αναπτυχθούν, προκειμένου να εφαρμοστούν αυτές οι μεθοδολογίες και να προσφερθούν ως συνεργατικές υπηρεσίες. Τα νέα συνεργατικά εργαλεία πρωτοποριακής διαχείρισης της προστασίας πρέπει να αναπτυχθούν για τη στήριξη της ασφάλειας των πληροφοριών διαχείρισης κινδύνων, της κωδικοποίησης της γνώσης, της διαχείρισης προστασίας των πληροφοριών εξατομίκευσης, της συνεργασίας, των ζητημάτων εξειδικευμένου περιεχομένου, της περιγραφικής προσέγγισης, με προσανατολισμό στις υπηρεσίες. Στο πλαίσιο αυτό, το έργο S-Port παρουσιάστηκε ως μια εθνική προσπάθεια για την ανάπτυξη του εν λόγω εργαλείου διαχείρισης προστασίας. Το S-Port μπορεί να χρησιμοποιηθεί από την ομάδα προστασίας των λιμένων, προκειμένου να καθοριστούν από κοινού οι επιπτώσεις, οι απειλές και τρωτά σημεία, να υπολογιστούν οι κίνδυνοι προστασίας και να βρεθούν τα κατάλληλα αντίμετρα.

9. Η διαλειτουργικότητα είναι ένα άλλο σημαντικό μειονέκτημα, σε όλα τα επίπεδα (αρχιτεκτονικά PICT, τεχνολογίες, διαδικασίες και δεδομένα), κατά την υλοποίηση των διασυνοριακών ηλεκτρονικών υπηρεσιών. Απαιτείται η συνεργασία μεταξύ όλων των σχετικών φορέων (π.χ. Ηνωμένα Έθνη, IMO, IALA, SMDG, ITIGG, PROTECT), προκειμένου να τυποποιηθεί η ανταλλαγή των πληροφοριών για τα θαλάσσια ρεύματα, τις διαδικασίες και τα μηνύματα. Συνιστάται ο ανασχεδιασμός των διαδικασιών, ώστε να επιτευχθεί η εναρμονισμένη των διασυνοριακών υπηρεσιών λιμένος.

10. Η υιοθέτηση της τεχνολογίας *Cloud Computing* μπορεί να φέρει μια νέα επανάσταση, στον τομέα των θαλάσσιων μεταφορών, επιτρέποντας ένα ολιστική συνεργατικό περιβάλλον που προσφέρει διασυνοριακές, αξιόπιστες ηλεκτρονικές υπηρεσίες, σε όλους τους εμπορικούς λιμένες και τους χρήστες τους, με οικονομικά αποδοτικό τρόπο. Η τεχνολογία αυτή φιλοξενείται είτε σε ευρωπαϊκό (μια ευρωπαϊκή αξιόπιστη κεντρική αρχή) ή σε εθνικό επίπεδο (εθνικό Υπουργείο Ναυτιλίας).

11. Η οικονομική κρίση έχει επιφέρει την ιδιωτικοποίηση των ευρωπαϊκών λιμένων και οι ξένοι επενδυτές διαχειρίζονται τα συστήματα PICT, με βάση τις δικές τους πρακτικές προστασίας. Αυτό αποτελεί μια άλλη απειλή για τις επιχειρήσεις κατασκοπείας, με αρνητικές επιπτώσεις στην οικονομία. Η Ευρωπαϊκή Ένωση πρέπει να επιβάλλει, να ελέγχει, και να παρακολουθεί τις πρακτικές προστασίας των λιμένων της Ευρωπαϊκής Ένωσης.

12. Η Ευρωπαϊκή Ένωση επιθυμεί να διατυπώσει μια Ολοκληρωμένη Ναυτιλιακή Πολιτική (IMP), προκειμένου να καταστεί δυνατή η ανάπτυξη της ναυτιλιακής οικονομίας και η ευημερία των παράκτιων περιοχών και να εξασφαλιστούν η ανταγωνιστικότητα, η ασφάλεια και η προστασία του τομέα. Η υλοποίηση της IMP απαιτεί την δημιουργία των θεσμικών οργάνων, των κρατών-μελών και των αποτελεσματικών δομών των γειτονικών παράκτιων περιοχών, για τους σκοπούς της διασυνοριακής συνεργασίας, στις προτεραιότητες της ναυτιλιακής προστασίας. Είναι αναγκαίες οι εθνικές και περιφερειακές συνεργατικές προσπάθειες, προκειμένου να εμπλακούν περισσότερο στη διαδικασία της IMP, αντιμετωπίζοντας τις ανάγκες τους για προστασία, και τα προβλήματα που προέρχονται από την εθνική και περιφερειακή ιδιοσυγκρασία και την κουλτούρα. Οι προσπάθειες αυτές επιτρέπουν την εναρμόνιση των τοπικών, περιφερειακών και εθνικών πολιτικών που θα συμβάλουν σε ολιστικές λύσεις για τα προβλήματα ασφάλειας και θα παράσχουν, στοιχεία από αυτή την εμπειρία, σε διάφορες ναυτιλιακές πολιτικές, διαμορφώνοντας ομάδες (π.χ. ECSA, ICS-ISF) και συμβάλλοντας στην αποδεκτή, εφαρμόσιμη IMP, αυξάνοντας την προβολή της ευρωπαϊκής ναυτιλίας.

13. Ένας από τους στόχους των IMP «είναι να ενισχύσει τα επαγγελματικά προσόντα και τις μελέτες, στον τομέα της θάλασσας, για να προσφέρει καλύτερες προοπτικές επαγγελματικής σταδιοδρομίας, στον τομέα. Μπορούμε να πάμε ένα βήμα παραπέρα και να προτείνουμε την ενίσχυση των ναυτιλιακών σπουδών, συμπεριλαμβανομένης των μαθημάτων ασφάλειας και της προστασίας της ιδιωτικής ζωής, προκειμένου να οικοδομηθεί ένας αξιόπιστος και ανταγωνιστικός ναυτιλιακός τομέας.

Κεφάλαιο 7: ΠΑΡΑΡΤΗΜΑ Α: διαχείριση προστασίας ICT

Οποιαδήποτε *διαδικασία διαχείρισης προστασίας* ICT αποτελείται από τα ακόλουθα γενικά στάδια [2]:

- Πλαίσιο Ίδρυσης: προτίθεται να ορίσει όριο διαχείρισης κινδύνου, στο σύστημα ICT,
- Ανάλυση Απειλής: Προσδιορίζει τις απειλές, για όλα τα επενδυτικά αγαθά, στο σύστημα ICT (υπό εξέταση) και τα επίπεδα ευπάθειά τους για αυτές τις απειλές,
- Ανάλυση Κινδύνων (Αναγνώριση κινδύνου & Εκτίμηση φάσεων): σκοπεύει να αξιολογήσει το επίπεδο κινδύνου,

- Αξιολόγηση Κινδύνων (Ανάλυση κινδύνου και Αξιολόγηση φάσεων): χρησιμοποιείται για την λήψη αποφάσεων και την συνειδητοποίηση των στόχων της οργάνωσης,
- Αντιμετώπιση Κινδύνου (Αντιμετώπιση Κινδύνου & φάσεις Αποδοχής Κινδύνου): στόχος είναι να μειώσει, να διατηρήσει, να αποτρέψει ή να μεταφέρει τους κινδύνους,
- Εκθέσεις ασφαλείας: Δημιουργεί, εφαρμόζει και ενημερώνει συνεχώς την πολιτική ασφάλειας, τις διαδικασίες και τις περιφερειακές πολιτικές (π.χ. σχέδιο επιχειρησιακής συνέχισης, σχέδιο ανάκαμψης από κινδύνους).

Τα κοινά πρότυπα που χρησιμοποιούνται για τη διαχείριση προστασίας ICT, περιλαμβάνουν μια δέσμη προτύπων για τις προηγούμενες φάσεις, δηλαδή:

Το ISO / IEC 27001:2005 είναι ένα εμπορικό πρότυπο που καθορίζει τις αρχές για την δημιουργία, την υλοποίηση, την παρακολούθηση και αξιολόγηση, διατήρηση και βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Το ISMS είναι ένα συνολικό πλαίσιο διαχείρισης και ελέγχου για την διαχείριση των κινδύνων και την προστασία των πληροφοριών ενός οργανισμού. Το ISO / IEC 27001 δεν καθορίζει ειδικούς ελέγχους προστασίας των πληροφοριών, αλλά σταματά στο διοικητικό και λειτουργικό επίπεδο. Συνήθως, μια ομάδα αναλυτών με την τεχνογνωσία και την υψηλή εμπειρία ICT επαληθεύει την συμμόρφωση του οργανισμού με τις καθορισμένες απαιτήσεις. Ωστόσο, αν και η διαδικασία συμμόρφωσης απαιτεί την εμπλοκή πολλών χρηστών, οι συνεργατικές ικανότητες του προτύπου είναι περιορισμένες, λόγω της εγγενούς πολυπλοκότητας του.

Το πρότυπο καλύπτει, ως επί το πλείστον, τις οργανώσεις μεγάλης κλίμακας (π.χ. κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις), ενώ θεωρείται πολύ βαρύ για τις πολύ μικρές, μικρές και μεσαίου μεγέθους επιχειρήσεις.

Θα πρέπει να σημειωθεί ότι το πρότυπο ISO / IEC 27001, δεν είναι στην ουσία πραγματικές μέθοδοι για RM, αλλά μάλλον πρότυπα συμμόρφωσης, αναφέροντας μια λίστα ελέγχου για τις ορθές πρακτικές ασφάλειας και τις προϋποθέσεις, κάτω από τις οποίες μια υπάρχουσα μέθοδος θα πρέπει να είναι συμβατή με τα πρότυπα. Συγκεκριμένα, παρέχει γενικές απαιτήσεις ανάλυσης και

διαχείρισης κινδύνων που πρέπει να γίνουν μέσω μιας αναγνωρισμένης μεθόδου, χωρίς να παρέχει μια συγκεκριμένη μέθοδο.

Επί του παρόντος, υπάρχει μια ποικιλία από δωρεάν (π.χ. η Ebios αναπτύχθηκε από το Κεντρικό Τμήμα Πληροφοριακών Συστημάτων Προστασίας (Γαλλία)) και εμπορικό λογισμικό (π.χ. CRAMM που αναπτύχθηκε από το Insight Consulting), που επαληθεύουν την συμμόρφωση του οργανισμού με το πρότυπο ISO / IEC 27001.

Το ISO / IEC 27005:2008 είναι ένα εμπορικό πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC), η οποία καθορίζει τις βασικές αρχές, τις πτυχές και τις δραστηριότητες μίας καλά καθορισμένης διαδικασίας διαχείρισης των κινδύνων. Έτσι, μπορεί να θεωρηθεί ως ένα ελάχιστο πλαίσιο που περιγράφει τις απαιτήσεις για την διαδικασία αξιολόγησης του κινδύνου, παρά ως μια ολοκληρωμένη μέθοδος διαχείρισης των κινδύνων. Το πρότυπο υποστηρίζει τις γενικές έννοιες που ορίζονται στο ISO / IEC 27001:2005, καθώς και τις κύριες διαδικασίες και τους κανόνες που περιγράφονται στο πρότυπο ISO / IEC 27002:2005. Μπορεί να εφαρμοστεί σε όλα τα είδη των οργανισμών (π.χ. κυβερνητικές υπηρεσίες, μεγάλες επιχειρήσεις, επιχειρήσεις μικρού και μεσαίου μεγέθους) που προτίθενται να διαχειρίζονται τους κινδύνους, οι οποίοι θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια ICT του οργανισμού.

Το ISO 27005 προτείνει την χρήση τόσο ποσοτικής όσο και ποιοτικής μεθόδου, για τον υπολογισμό του επιπέδου κινδύνου. Ωστόσο, δεν υποστηρίζει καμία συγκεκριμένη τεχνική προς επίτευξη του σκοπού αυτού ή οποιαδήποτε υπολογιστική μέθοδο, για να αναλύσει και να συνδυάσει τις πληροφορίες αξιολόγησης. Επίσης, η γενική φύση του προτύπου δεν περιλαμβάνει τις πτυχές που προωθούν την συνεργασία μεταξύ των χρηστών.

Σε αυτό το πλαίσιο, οι πιο ολοκληρωμένες μέθοδοι διαχείρισης κινδύνου, όπως οι Ebios, Magerit και MEHARI, συμμορφώνονται με τους κανόνες και τις υποχρεώσεις που ορίζονται από το συγκεκριμένο πρότυπο.

Το ISO / IEC 27002:2005 περιλαμβάνει τις βασικές αρχές του ISO / IEC 17799:2005 και ISO / IEC 17799:2005 / Cor.1: 2007. Πρόκειται για ένα εμπορικό

πρότυπο, που παρέχει τις προδιαγραφές με οδηγίες για την εγκατάσταση, εφαρμογή, συντήρηση και βελτίωση του «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών» (ISMS) σε έναν οργανισμό. Ως εκ τούτου, το πρότυπο ISO / IEC 27002 θεωρείται ως ο οδηγός που επιτρέπει εσωτερικές και εξωτερικές αναλύσεις, συνήθως με την τεχνογνωσία και την υψηλή εμπειρία ICT, προκειμένου να αξιολογηθεί το επίπεδο ασφάλειας ενός οργανισμού και να καθοριστούν οι πτυχές που θα βελτιώσουν την διαχείριση της ασφάλειας των πληροφοριών σε αυτό.

Ωστόσο, το πρότυπο ISO / IEC 27002 δεν χρησιμοποιεί μια μέθοδο για την ανάλυση και διαχείριση των κινδύνων, αλλά περιλαμβάνει έναν κατάλογο των δέκα βασικών τομέων ελέγχου (οργάνωση της ασφάλειας των πληροφοριών, διαχείριση επενδυτικών αγαθών, ασφάλεια των ανθρωπίνων πόρων, φυσική και περιβαλλοντική ασφάλεια, Επικοινωνίες και διαχείριση, έλεγχος πρόσβασης, απόκτηση, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων, διαχείριση της ασφάλειας των πληροφοριών, διαχείριση της επιχειρησιακής συνέχειας, συμμόρφωση) που αποτελούνται από 36 στόχους ελέγχου και 127 ελέγχους που καθορίζουν τις προϋποθέσεις, βάσει των οποίων ένας οργανισμός θα πρέπει να είναι συμβατός με τα πρότυπα. Παρ 'όλα αυτά, ούτε μια μέθοδος δεν αφορά την αξιολόγηση ούτε την διαχείριση των κινδύνων, που περιλαμβάνει τις πτυχές του χειρισμό των κινδύνων, όπως τον προσδιορισμό των κινδύνων και την δημιουργία ενός αρχικού σχεδίου αντιμετώπισης του κινδύνου.

Το πρότυπο είναι σε θέση να καλύψει όλα τα είδη των οργανισμών (π.χ. κυβερνητικές υπηρεσίες) και όλα τα μεγέθη, από μικρές έως μεσαίες και μεγάλες επιχειρήσεις μονάδες. Υπάρχουν διάφορες εφαρμογές που εφαρμόζουν το πρότυπο ISO / IEC 27002:2005. Τα πιο αντιπροσωπευτικά παραδείγματα είναι το δωρεάν αυτόνομο εργαλείο Ebios, που αναπτύχθηκε από το Κεντρικό Τμήμα Πληροφοριακών Συστημάτων Ασφαλείας (Γαλλία) και το εμπορικό αυτόνομο λογισμικό *RiskWatch*.

NIST 800 - 30 Οδηγός Διαχείρισης Κινδύνων για Συστήματα ICT: Ο NIST 800 - 30 είναι ένας δωρεάν οδηγός, που καθορίζει όλες τις πτυχές ενός αποτελεσματικού και αποδοτικού προγράμματος διαχείρισης κινδύνων. Ενσαρκώνει τις κατευθυντήριες γραμμές και τη διαδικασία η οποία απαιτείται για την αξιολόγηση και τον μετριασμό

των κινδύνων που προσδιορίζονται στο πλαίσιο των συστημάτων πληροφορικής. Ο NIST 800 - 30 έχει ως στόχο να βοηθήσει τις οργανώσεις, ως επί το πλείστον μεγάλης κλίμακας (όπως κυβερνητικές υπηρεσίες και μεγάλες εταιρείες), για την καλύτερη διαχείριση των κινδύνων που σχετίζονται με το IT.

Η προτεινόμενη προσέγγιση διαχείρισης κινδύνου περιλαμβάνει τρεις κύριες διαδικασίες:

Α. Η αξιολόγηση του κινδύνου , περιλαμβάνει τον εντοπισμό και την αξιολόγηση των τρωτών σημείων, απειλών και κινδύνων, και την σύσταση των κατάλληλων αντιμέτρων. Η διαδικασία αξιολόγησης των κινδύνων ενσωματώνει εννέα κύρια βήματα: Βήμα 1 - Χαρακτηρισμός Συστήματος, Βήμα 2 - Αναγνώριση απειλής, Βήμα 3 - Αναγνώριση ευπάθειας, Βήμα 4 - Ανάλυση Ελέγχου, Βήμα 5 - Καθορισμός Κινδύνου, Βήμα 6 - Ανάλυση των επιπτώσεων, Βήμα 7 - Προσδιορισμός των κινδύνων, Βήμα 8 - Συστάσεις ελέγχου, Βήμα 9 - Αποτελέσματα Τεκμηρίωσης.

Σύμφωνα με το NIST 800-30, ο κίνδυνος είναι η πιθανότητα μιας συγκεκριμένης απειλής, ασκώντας στην πηγή μία ιδιαίτερη δυνητική ευπάθεια, και των επιπτώσεων των εν λόγω ανεπιθύμητων ενεργειών, σχετικά με την οργάνωση. Ο τελικός προσδιορισμός του κινδύνου αποστολής (Χαμηλός - Μεσαίος - Υψηλός) βασίζεται σε έναν πρωτόγονο υπολογισμό και προέρχεται από τον πολλαπλασιασμό των αξιολογήσεων που έχουν ανατεθεί για την απειλή κινδύνου (Υψηλή, Μεσαία και Χαμηλή) και τις επιπτώσεις των απειλών (Υψηλές, Μεσαίες και Χαμηλές).

Β. Μετριασμός του κινδύνου , περιλαμβάνει την αξιολόγηση και την εφαρμογή των ελέγχων που ορίζονται στο πλαίσιο της διαδικασίας αξιολόγησης των κινδύνων,

Γ. Η Αξιολόγηση και η εκτίμηση παρέχουν τις κατευθυντήριες γραμμές της κατευθυνόμενης και συνεχούς διαδικασίας αξιολόγησης και εκτίμησης των κινδύνων.

Θα πρέπει να σημειωθεί, ότι η χρήση της πρωτόγονης μεθόδου για τον υπολογισμό του επιπέδου κινδύνου, σε συνδυασμό με την έλλειψη μίας

αποτελεσματικής υπολογιστικής τεχνικής, για την ανάλυση και τον συσχετισμό των γνώσεων που βρίσκονται σε ένα εταιρικό περιβάλλον, μειώνει τις δυνατότητες του NIST 800-30 για μια πιο ολοκληρωμένη προσέγγιση. Επιπλέον, παρά το γεγονός ότι η μέθοδος έχει υιοθετήσει και χρησιμοποιεί εκτεταμένες τεχνικές και λειτουργικά ερωτηματολόγια, που απαιτούν τη συμμετοχή μιας ποικιλίας των χρηστών, η έννοια της συνεργασίας, στον προσδιορισμό των συνολικών αποτελεσμάτων και την διαμόρφωση του τελικού σχεδίου θεραπείας, είναι περιορισμένη. Η ανάλυση κινδύνου και η διαδικασία διαχείρισης, που ορίζεται στο NIST 800 - 30, συνήθως εκτελείται από ειδική ομάδα εμπειρογνωμόνων ICT.

Η μέθοδος αυτή είναι σύμφωνη με το ISO / IEC 27001:2005, αξιοποιώντας όλες τις προϋποθέσεις για την καθιέρωση και την εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Σήμερα, το NIST 800-30 δεν υποστηρίζεται από κανένα ελεύθερο λογισμικό ή από εμπορικές εφαρμογές.

Λειτουργικά Κρίσιμη απειλή, επενδυτικά αγαθά, καθώς και Αξιολόγηση ευπάθειας (OCTAVE) :

Η OCTAVE είναι μια δωρεάν μέθοδος χρέωσης σε αξιολογήσεις ασφάλειας, που ενσωματώνει μία ολοκληρωμένη, οδηγούμενη από το περιβάλλον, και αυτο-κατευθυνόμενη διαδικασία εκτίμησης των κινδύνων. Η μέθοδος υιοθετεί μια προσέγγιση τριών φάσεων για να καταναλώνει, να κατανοήσει και να καταστήσει το επίπεδο ασφάλειας οργάνωσης και τεχνολογίας, δημιουργώντας το προφίλ της επιχείρησης. Οι φάσεις αυτές είναι: η διαμόρφωση του προφίλ απειλής, ο προσδιορισμός των τρωτών σημείων των υποδομών, καθώς και η ανάπτυξη της στρατηγικής, για την ασφάλεια και τα σχέδια.

Για την επίτευξη των στόχων της, η μέθοδος αυτή στηρίζεται σε εργαστήρια και εκτενή ερωτηματολόγια. Μέσω αυτών των διαύλων επικοινωνίας, η OCTAVE ενθαρρύνει την ανοικτή συζήτηση και συνεργασία μεταξύ των συμμετεχόντων και διευκολύνει την ανταλλαγή και την συσσώρευση πληροφοριών και γνώσεων, σχετικά με την ασφάλεια. Στην μέθοδο αυτή, οι εταιρικοί χρήστες έχουν τη δυνατότητα να συμμετέχουν ενεργά σε πολλά μέρη της διαδικασίας αξιολόγησης.

Για την διαδικασία ανάλυσης κινδύνου, η OCTAVE χρησιμοποιεί μια πρωτόγονη προσέγγιση που βασίζεται σε μια ποιοτική κλίμακα (υψηλή, μέση, χαμηλή). Ωστόσο, η μέθοδος δεν ενσωματώνει μια προηγμένη τεχνική για την ανάλυση και τον συνδυασμό των γνώσεων που βρίσκονται στο εταιρικό περιβάλλον. Έτσι, η πληροφορία βασίζεται σε μία ανεπαρκή μέθοδο, για τον προσδιορισμό των συνολικών αποτελεσμάτων.

Τέλος, η μέθοδος OCTAVE υποστηρίζεται από ένα εμπορικά αυτόνομο λογισμικό, το αυτοματοποιημένο εργαλείο *Octave*, που υλοποιείται από την Προηγμένη Τεχνολογία του Ινστιτούτου (ATI). Το εργαλείο είναι σε θέση να βοηθήσει τον χρήστη κατά τη φάση της συλλογής των δεδομένων, να οργανώσει τις πληροφορίες που συλλέγονται, και τελικά να παράγει τις εκθέσεις μελέτης.

Αξιολόγηση Κινδύνων CCTA και Μεθοδολογία Διαχείρισης (CRAMM)

Η CRAMM είναι μια μέθοδος που αναπτύχθηκε, για να βοηθήσει κυρίως τους οργανισμούς μεγάλου μεγέθους (όπως κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις) μέσω μιας προσέγγισης τριών φάσεων, της αναγνώρισης και αποτίμησης των στοιχείων του ενεργητικού, καθώς και την ανάλυση και διαχείριση των κινδύνων. Έτσι, προβαίνει σε αξιολόγηση των κινδύνων των πληροφοριακών συστημάτων και δικτύων, για να προσδιορίσει τις απαιτήσεις προστασίας και τις πιθανές λύσεις, και να ανιχνεύσει τις απαιτήσεις έκτακτης ανάγκης και τις πιθανές λύσεις. Η μέθοδος μπορεί να εφαρμοστεί σε διάφορα είδη των συστημάτων και των δικτύων πληροφοριών και μπορεί να καλύψει όλα τα στάδια του κύκλου ζωής του συστήματος πληροφοριών (π.χ. σχεδιασμός, ανάπτυξη και εφαρμογή, καθώς και λειτουργία εφαρμογής).

Σε αυτήν την μέθοδο, ένας αναλυτής ή μια ομάδα αναλυτών αναλαμβάνουν την ευθύνη να αξιολογήσουν την ασφάλεια και το επίπεδο κινδύνου του οργανισμού αναλύοντας και συνδυάζοντας τις ποικίλες γνώσεις που βρίσκονται κατανεμημένες στο εταιρικό περιβάλλον. Η υπολογιστική μέθοδος και η τεχνική που έχει υιοθετηθεί από την CRAMM, για τον συσχετισμό και τον προσδιορισμό των αποτελεσμάτων, είναι αρκετά πρωτόγονη και βασίζεται σε μια ποιοτική προσέγγιση. Επιπλέον, η

συμμετοχή των χρηστών των οργανώσεων στην πραγματική εκτίμηση μπορεί να θεωρηθεί χαμηλή, έτσι οι δυνατότητες συνεργασίας της μεθόδου χαρακτηρίζονται ως περιορισμένες. Προκειμένου οι αναλυτές να χρησιμοποιήσουν και να εκτελέσουν όλες τις φάσεις της μεθόδου (αναγνώριση και αποτίμηση των επενδυτικών αγαθών, ανάλυση και διαχείριση κινδύνου), πρέπει να έχουν ένα υψηλό επίπεδο δεξιοτήτων και την ανάλογη εμπειρία στην συλλογή και ανάλυση πληροφοριών για τον εντοπισμό των απειλών και των τρωτών σημείων. Άρα, συμπεράνουμε ότι οι κίνδυνοι καθορίζουν τα πλέον κατάλληλα αντίμετρα που ταιριάζουν στις ανάγκες των οργανισμών.

Ως μέθοδος, η CRAMM είναι αρκετά λεπτομερής και είναι σε θέση να καλύψει ένα ευρύ φάσμα χαρακτηριστικών στο Σύστημα Διαχείρισης, σε επιχειρησιακό και τεχνικό επίπεδο. Επίσης, η CRAMM συμμορφώνεται με τους κανόνες και την υποχρέωση που επιβάλλεται από το πρότυπο ISO / IEC 17799. Η CRAMM υποστηρίζεται από ένα εμπορικά αυτόνομο εργαλείο, που αναπτύχθηκε από το *Insight Consulting*, με σκοπό την παροχή ενός τρόπου για την εφαρμογή της προτεινόμενης μεθόδου.

Ebios

Η Ebios είναι μια προσέγγιση διαχείρισης του κινδύνου, που δημιουργήθηκε βάσει της γαλλικής Γενικής Γραμματείας Εθνικής Άμυνας, και έχει ως στόχο να παρέχει μια ολοκληρωμένη και συστηματική μεθοδολογία, για την αξιολόγηση και την αντιμετώπιση των κινδύνων, στον τομέα των συστημάτων πληροφοριών. Η προτεινόμενη προσέγγιση περιλαμβάνει μια διαδικασία πέντε φάσεων, που ασχολούνται με την ανάλυση της εξάρτησης από το σύστημα πληροφοριών (Φάση 1), τον προσδιορισμό των αναγκών ασφαλείας και την ανάλυση των απειλών (φάσεις 2 και 3), και, τέλος, την σε βάθος και ακριβή διάγνωση των κινδύνων (φάσεις 4 και 5).

Η μεθοδολογία EBIOS είναι εύκολη στην κατανόηση και την ανάπτυξη μέσω μίας απλής και διαισθητικής προσέγγισης. Έτσι, μπορεί να εφαρμοστεί από ένα σύνολο οργανισμών, που ποικίλλουν από κυβερνητικές υπηρεσίες και μεγάλες εταιρείες, μέχρι μικρές και μεσαίου μεγέθους επιχειρήσεις που καλύπτουν μόνο

ζητήματα Επιχειρησιακής Διοίκησης και χαρακτηριστικά. Η μεθοδολογία διαθέτει ικανότητες συνεργασίας, δεδομένου ότι συγκεντρώνει και συνδυάζει την εταιρική γνώση σε ένα ομαλό και αποτελεσματικό τρόπο, με βάση μια ποιοτική προσέγγιση. Ωστόσο, η έλλειψη ενός προηγμένου υπολογιστικού σχήματος, για την συσχέτιση και τον προσδιορισμό των αποτελεσμάτων, μπορεί να θεωρηθεί ένα κύριο μειονέκτημα.

Η EBIOS είναι σε θέση να καλύψει όλες τις απαιτήσεις, τα βήματα και τις διαδικασίες που ορίζονται από μια ποικιλία από πρότυπα πληροφορικής, όπως τα ISO / IEC 27001:2005, ISO / IEC 27002:2005 και ISO / IEC 27005:2008. Η μέθοδος αυτή υποστηρίζεται από ένα εργαλείο ανοικτού κώδικα, που έχει αναπτυχθεί από το Κεντρικό Τμήμα Πληροφοριακών Συστημάτων Ασφαλείας (Γαλλία), και είναι μια αυτόνομη εφαρμογή, που βασίζεται σε τεχνολογίες Java και xml. Το εργαλείο ενσωματώνει όλα τα βήματα της ανάλυσης και διαχείρισης των κινδύνων , τα οποία καθορίζονται από τις πέντε φάσεις EBIOS, βοηθώντας τους χρήστες με χαμηλή πείρα και εξειδίκευση πληροφορικής, στην αξιολόγηση και τον μετριασμό των εταιρικών κινδύνων.

IT-Grundschutz

Η IT-Grundschutz έχει αναπτυχθεί από την Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών της Γερμανίας και παρέχει μια μέθοδο για την δημιουργία μιας ολοκληρωμένης και αποτελεσματικής διαχείρισης προστασίας IT. Η προτεινόμενη διαδικασία ασφάλειας IT ενσωματώνει σαφώς καθορισμένα βήματα για την ανάλυση των εφαρμοζόμενων μέτρων προστασίας, τον εντοπισμό και την αξιολόγηση των απειλών, καθώς και την ιεράρχηση και υλοποίηση των κατάλληλων ελέγχων μείωσης του κινδύνου.

Η IT-Grundschutz έχει σχεδιαστεί για να ισχύει σε οργανισμούς με σύνθετη υποκείμενη υποδομή, όπως κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις, καθώς και επιχειρήσεις μικρού και μεσαίου μεγέθους με βασικά συστήματα. Η μέθοδος μπορεί να αναπτυχθεί από τους χρήστες, με βάση το πρότυπο IT, που σχετίζεται με

την τεχνογνωσία και την εμπειρία, αναλαμβάνοντας την ευθύνη για την εκτέλεση της διαδικασίας αξιολόγησης. Ωστόσο, οι συνεργατικές ικανότητες της μεθόδου μπορεί να θεωρηθούν χαμηλές, δεδομένου ότι οι εταιρικοί χρήστες συμμετέχουν μόνο σε συγκεκριμένα βήματα της εκτίμησης των κινδύνων.

Η IT-Grundschutz ενσωματώνει μια προσέγγιση ποιοτικής ανάλυσης του κινδύνου, που συνδέεται με μια πρωτόγονη υπολογιστική τεχνική, για την ανάλυση και συσχέτιση των πληροφοριών αξιολόγησης. Η μέθοδος είναι συμβατή με το πρότυπο αντιμετώπισης των καθορισμένων απαιτήσεων ISO / IEC 27001:2005, και είναι κατάλληλο για την εφαρμογή της διαδικασίας που περιγράφεται από το ISMS ISO / IEC 27002:2005. Στο πλαίσιο αυτό, η IT-Grundschutz στοχεύει στην παροχή βοήθειας, σε όλους τους χρήστες με διαχειριστικές, επιχειρησιακές και τεχνικές ευθύνες, στις προσπάθειές τους, για την διαχείριση της προστασίας των πληροφοριών και των πληροφοριακών πόρων, και την μείωση των κινδύνων με τους οποίους συνδέονται.

Η μέθοδος υποστηρίζεται από το εμπορικό λογισμικό *GStool*, που αναπτύχθηκε από την Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών (BSI). Η GSTOOL είναι μια αυτόνομη εφαρμογή, που υποστηρίζεται από την βάση δεδομένων.

Magerit

Η *Magerit* είναι μια ανοικτή μεθοδολογία για την ανάλυση και διαχείριση κινδύνων, που αναπτύχθηκε από το Ανώτατο Συμβούλιο της Ισπανίας για την Ηλεκτρονική Διακυβέρνηση. Είναι η απάντηση στην αυξανόμενη εξάρτηση των δημόσιων και ιδιωτικών οργανισμών από τις τεχνολογίες πληροφοριών, για την εκπλήρωση της αποστολής τους και την επίτευξη των επιχειρηματικών στόχων τους. Η προσέγγιση αυτή καλύπτει όλες τις αρχές μιας ολοκληρωμένης ανάλυσης κινδύνου. Η διαδικασία διαχείρισης περιέχει βήματα, όπως τα επενδυτικά αγαθά και την αναγνώριση απειλών, τον προσδιορισμό των επιπτώσεων, καθώς και τον προσδιορισμό και τον μετριασμό των κινδύνων.

Στην Magerit, η αξιολόγηση του κινδύνου μπορεί να είναι ποσοτική (χρησιμοποιώντας μια πρωτόγονη λειτουργία) ή ποιοτική (σε κλίμακα, βάσει των

επιπέδων (πολύ χαμηλό, χαμηλό, μέσο, υψηλό πολύ υψηλό)). Για τον υπολογισμό του κινδύνου, λαμβάνονται υπόψη δύο παράμετροι των επιπτώσεων σε ένα επενδυτικό αγαθό, που προκύπτουν από την απειλή και την συχνότητα των απειλών. Πρέπει επίσης να σημειωθεί ότι η υπολογιστική τεχνική που εφαρμόζεται στην *Magerit* δεν είναι επαρκής, δεδομένου ότι η ανάλυση και συσχέτιση των πληροφοριών αξιολόγησης βασίζεται σε πρωτόγονες λειτουργίες.

Διάφοροι οργανισμοί που διαθέτουν περίπλοκες υποδομές πληροφορικής (κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις), καθώς και βασικά συστήματα (επιχειρήσεις μικρού και μεσαίου μεγέθους) είναι σε θέση να εφαρμόσουν αυτήν την μέθοδο για να εντοπίσουν και να μετριάσουν τους κινδύνους ασφαλείας τους. Η Magerit μπορεί να χρησιμοποιείται και να συντηρείται μόνο από χρήστες με την τεχνογνωσία και την εμπειρία των ICT. Αυτοί οι χρήστες αναλαμβάνουν την ευθύνη για την εκτέλεση της διαδικασίας ανάλυσης κινδύνου, μέσω ημερίδων και συνεντεύξεων με ειδικούς εκπροσώπους της οργάνωσης, οι οποίοι συμμετέχουν μόνο σε συγκεκριμένες φάσεις της διαδικασίας αξιολόγησης. Στο πλαίσιο αυτό, η μέθοδος δεν υποστηρίζει επαρκείς ικανότητες και χαρακτηριστικά συνεργασίας.

Η *Magerit* συμμορφώνεται με μια σειρά από πρότυπα πληροφορικής. Συγκεκριμένα, απευθύνεται σε όλους τους κανόνες και τις υποχρεώσεις που επιβάλλονται από τα πρότυπα ανάλυσης και διαχείρισης κινδύνων ISO / IEC 27005:2008, καλύπτει όλες τις απαιτήσεις που ορίζονται από το πρότυπο ISO / IEC 27001:2005 και συμμορφώνεται με τον κώδικα εφαρμογής ενός ISMS, όπως καθορίζεται από το ISO / IEC 27002:2005.

Ένα εμπορικό λογισμικό που υλοποιεί και επεκτείνει η μεθοδολογία της Magerit είναι η EYA / PILAR. Αυτή είναι μια αυτόνομη εφαρμογή (με βάση τις τεχνολογίες Java και XML), που αναπτύχθηκε από την ALHJ Mañas και έχει σχεδιαστεί για να υποστηρίξει και να εκτελέσει την καθορισμένη διαδικασία διαχείρισης των κινδύνων.

MEHARI

Η MEHARI είναι μια δωρεάν ποιοτική ανάλυση κινδύνου (που περιλαμβάνει δραστηριότητες όπως η εγκατάσταση πλαισίου, οι πάσσαλοι ανάλυσης και ταξινόμησης επενδυτικών αγαθών, ο εντοπισμός του κινδύνου, η ανάλυση κινδύνου, η αξιολόγηση του κινδύνου) και η διαχείριση μεθόδου (η οποία περιλαμβάνει δραστηριότητες όπως η αξιολόγηση των κινδύνων, η αντιμετώπιση, η αποδοχή και η επικοινωνία), που αναπτύχθηκε από την CLUSIF. Η MEHARI παρέχει μια ολοκληρωμένη μεθοδολογία, με κατάλληλες βάσεις γνώσης (π.χ. εγχειρίδια και οδηγούς που περιγράφουν τις διαφορετικές ενότητες (πάσσαλοι, κίνδυνοι, ευπάθειες)), οι οποίες έχουν σχεδιαστεί για να βοηθήσουν τους ανθρώπους που εμπλέκονται στη διαχείριση της προστασίας (CISO, διαχειριστές κινδύνου, ελεγκτές, CIO), στην εκτέλεση εργασιών και τις δράσεις τους. Συγκεκριμένα, απευθύνεται σε χρήστες με διοικητικές λειτουργίες, καθώς και πιο τεχνικές αρμοδιότητες. Η μεθοδολογία είναι κατάλληλη για την εφαρμογή της διαδικασίας που περιγράφεται από το πρότυπο ISMS ISO / IEC 27001:2005.

Η MEHARI είναι η πλέον κατάλληλη για μεσαίας έως μεγάλης κλίμακας οργανώσεις, όπως κυβερνητικές υπηρεσίες και μεσαίου και μεγάλου μεγέθους επιχειρήσεις. Οι εταιρικοί χρήστες θα μπορούν να συμμετέχουν μόνο σε συγκεκριμένες φάσεις της μεθοδολογίας, σχετικά με την ταυτοποίηση των στοιχείων του ενεργητικού και των τρωτών σημείων. Σε αυτό το πλαίσιο, οι δυνατότητες συνεργασίας των μεθόδων μπορεί να θεωρηθούν περιορισμένες, δεδομένου ότι οι χρήστες δεν εμπλέκονται άμεσα στον υπολογισμό του κινδύνου και την διαμόρφωση του σχεδίου αντιμετώπισης του κινδύνου. Επιπλέον, η μέθοδος χρησιμοποιεί μία πρωτόγονη υπολογιστική μέθοδο, για να αναλύσει και συνδυάσει την ποικιλία των πληροφοριών, προκειμένου να συναγάγει τα τελικά αποτελέσματα.

Η MEHARI υποστηρίζεται από δύο ανεξάρτητα εργαλεία. Το πρώτο είναι το εμπορικό λογισμικό που διαχειρίζεται η εταιρεία Risicare και το δεύτερο είναι μια δωρεάν εφαρμογή, η MEHARI 2010 - ένα βασικό εργαλείο, που αναπτύχθηκε από την CLUSIF.

Πληροφορίες Αξιολόγησης Ασφάλειας & Μέθοδος Παρακολούθησης (ISAMM)

Η ISAMM είναι ένα ποσοτικό είδος της μεθοδολογίας διαχείρισης του κινδύνου, που μπορεί να εφαρμοστεί από διάφορες οργανώσεις, όπως κυβερνητικοί οργανισμοί, μεγάλες εταιρίες και μικρές ή μεσαίες επιχειρήσεις. Η αξιολόγηση του κινδύνου ISAMM περιέχει τρία κύρια μέρη: οριοθέτηση, συμμόρφωση και απειλές, και υπολογισμός και υποβολή εκθέσεων.

Η ISAMM είναι συμβατή με το πρότυπο ISO / IEC 27002 και παρέχει μέγιστη υποστήριξη του προτύπου 27001 ISMS ISO / IEC. Επίσης, υποστηρίζεται από ένα δωρεάν εργαλείο, το συμβουλευτικό εργαλείο ISAMM, και μια εμπορική εφαρμογή που ονομάζεται εργαλείο πελάτη ISAMM.

Κεφάλαιο 8: ΠΑΡΑΡΤΗΜΑ Β: Ασφάλεια στη θάλασσα

Η Ευρωπαϊκή Επιτροπή (ΕΕ) εργάζεται σε μια Ολοκληρωμένη Ναυτιλιακή

Πολιτική (IMP), με βάση τις στρατηγικές της Λισσαβόνας και του Göteborg. Η IMP (ιδρύθηκε από την ΕΕ) έχει ως αποστολή την ανάλυση των εθνικών ναυτιλιακών πολιτικών και τον συντονισμό τους, προκειμένου να επιτευχθεί ένα εναρμονισμένο, ευρέως αποδεκτό IMP. Ασχολείται, με τη βοήθεια των διαφόρων οργανισμών της ΕΕ, με τις ναυτιλιακές υποχρεώσεις, περιλαμβάνει διαβουλεύσεις με την κοινωνία των πολιτών και με όλα τα ενδιαφερόμενα μέρη. Ο στόχος της IMP είναι να μεγιστοποιηθούν τα οφέλη από τους ωκεανούς και τις θάλασσες, επιτρέποντας την ανάπτυξη της ναυτιλιακής οικονομίας και την άνθηση των παράκτιων περιοχών, την διασφάλιση της ανταγωνιστικότητας και της ασφάλειας του τομέα.

Οι ειδικοί στόχοι της IMP μπορούν να συνοψιστούν ως εξής:

- δημιουργία μίας στρατηγικής, για την άμβλυνση των επιπτώσεων της κλιματικής αλλαγής στις παράκτιες περιοχές,
- ενίσχυση των επαγγελματικών προσόντων και μελετών, στον τομέα των ναυτιλιακών μεταφορών, ώστε να προσφερθούν καλύτερες προοπτικές επαγγελματικής σταδιοδρομίας στον τομέα,
- δημιουργία ενός ευρωπαϊκού χώρου ναυτιλιακών μεταφορών χωρίς διοικητικούς ή τελωνειακούς φραγμούς, καθώς και μια ολοκληρωμένη στρατηγική ναυτιλιακών μεταφορών για το 2008-18, για τη βελτίωση της ανταγωνιστικότητας των ναυτιλιακών μεταφορών στην Ευρώπη,
- έκδοση κατευθυντηρίων γραμμών, για την εφαρμογή της περιβαλλοντικής νομοθεσίας που αφορά τους λιμένες και προτείνει μια νέα πολιτική για αυτούς, λαμβάνοντας υπόψη τους πολλαπλούς τους ρόλους,
- ενθάρρυνση της δημιουργίας πολλαπλών τομεακών δικτύων και προώθηση της τεχνολογικής καινοτομίας, στον τομέα της ναυπηγικής βιομηχανίας και της ενέργειας, χωρίς να επιβαρύνεται το περιβάλλον,
- υποστήριξη των διεθνών προσπαθειών, για την μείωση της θαλάσσιας ρύπανσης,
- εξασφάλιση μίας καλύτερης ποιότητας ζωής, στις παράκτιες και τις ιδιαιτέρως απόκεντρες περιφέρειες, καθώς συμβιβάζεται με την οικονομική ανάπτυξη και την περιβαλλοντική βιωσιμότητα, βάση της ενθάρρυνσης του παράκτιου τουρισμού,
- αύξηση της προβολής της «Θαλάσσιας Ευρώπης».

8.1. Οργανισμοί Τυποποίησης και οδηγίες

Διεθνής Ναυτιλιακός Οργανισμός (IMO): ο IMO ιδρύθηκε το 1959, και από τότε, λειτουργεί ως μία εξειδικευμένη υπηρεσία των Ηνωμένων Εθνών η οποία ασχολείται αποκλειστικά με τις ναυτιλιακές υποθέσεις. Παρέχει ένα σταθερό περιβάλλον, όπου οι κυβερνήσεις είναι σε θέση να συνεργάζονται και να εργάζονται από κοινού, στον τομέα των κανονισμών και των πρακτικών που αφορούν σε όλα τα είδη των ναυτιλιακών μεταφορών, και ασχολούνται με το διεθνές εμπόριο, διευκολύνοντας την υιοθέτηση των συνθηκών και προτύπων. Στόχος του είναι να ενισχύσει και να

βελτιώσει την προστασία, την ασφάλεια και την αποτελεσματικότητα στον τομέα της ναυτιλίας και του διεθνούς εμπορίου.

Από το 1959, ο IMO έχει υιοθετήσει περίπου 50 διεθνείς συμβάσεις και πρωτόκολλα και έχει κυκλοφορήσει πάνω από 800 κωδικούς, συστάσεις και κατευθυντήριες γραμμές, σχετικά με τις εν λόγω διεθνείς πράξεις. Οι περισσότερες από αυτές τις συμβάσεις και τα πρωτόκολλα εμπίπτουν στις παρακάτω κατηγορίες:

- *Διεθνής Σύμβαση για την Ασφάλεια της Ανθρώπινης Ζωής στη Θάλασσα (SOLAS) [6]* : Ο στόχος της είναι να καθορίσει τα πρότυπα για την κατασκευή των πλοίων, τον εξοπλισμό και τη λειτουργία, συμβατά με την ασφάλειά τους. Η σύμβαση SOLAS δίνει έμφαση στις ακόλουθες πτυχές:
- Γενικές διατάξεις, που περιλαμβάνουν ρυθμίσεις σχετικά με την έρευνα των διαφόρων τύπων πλοίων,
- Κατασκευές - Υποδιαίρεση και ευστάθεια, μηχανολογικές και ηλεκτρολογικές εγκαταστάσεις που παρουσιάζουν απαιτήσεις για στεγανότητα και διατάξεις υδροσυλλεκτών άντλησης για τα επιβατηγά πλοία, καθώς και απαιτήσεις ευστάθειας, για επιβάτες και φορτηγά πλοία,
- Πυροπροστασία, ανίχνευση πυρκαϊάς και απαιτήσεις εξαφάνισης για τα επιβατηγά πλοία, φορτηγά πλοία και δεξαμενόπλοια,
- Απαιτήσεις σχετικά με τα σωστικά μέσα και ρυθμίσεις για τις σωσίβιες λέμβους και τα σωσίβια, σύμφωνα με τον τύπο του πλοίου,
- Απαιτήσεις σε ραδιοεπικοινωνίες, σχετικά με την εφαρμογή ενός παγκόσμιου ναυτιλιακού συστήματος κινδύνου και προστασίας (GMDSS),
- Απαιτήσεις για την εφαρμογή ορισμένων υπηρεσιών προστασίας της ναυσιπλοΐας (προστασία της ναυσιπλοΐας),
- Απαιτήσεις για καταχώρηση και ασφάλιση του φορτίου ή των μονάδων φορτίου (Μεταφορά Εμπορευμάτων),
- Απαιτήσεις για την μεταφορά επικίνδυνων εμπορευμάτων, π.χ. ακτινοβολημένων πυρηνικών καυσίμων, υγροποιημένου φυσικού αερίου και χημικών υγρών (μεταφορά επικίνδυνων εμπορευμάτων),
- Απαιτήσεις για πυρηνοκίνητα πλοία,

- Διαχείριση της ασφαλούς λειτουργίας των πλοίων (Διεθνής Κώδικας Διαχείρισης της Ασφάλειας (ISM Code)),
- Μέτρα ασφαλείας για ταχύπλοα σκάφη (Διεθνής Κώδικας Ασφάλειας Ταχύπλοων Σκαφών (HSC)),
- Απαιτήσεις σχετικά με την έγκριση των αναγνωρισμένων οργανισμών, βελτιωμένες έρευνες, καθεστώς αναγνώρισης αριθμού πλοίου, έλεγχος του κράτους του λιμένα, στις επιχειρησιακές απαιτήσεις,
- Υποχρεώσεις που σχετίζονται με την ασφάλεια στη θάλασσα, (Διεθνής Κωδικός Παροχής Προστασίας Πλοίων και Λιμένων (ISPS Κώδικας)),
- Μέτρα ασφαλείας για πλοία μεταφοράς χύμα φορτίου,
- *Διεθνής Σύμβαση για την Πρόληψη της Ρύπανσης από Πλοία (MARPOL)*: Η διεθνής σύμβαση καλύπτει πτυχές που σχετίζονται με την πρόληψη της ρύπανσης του θαλάσσιου περιβάλλοντος από τα πλοία, λόγω επιχειρησιακών ή τυχαίων αιτίων.

Θα πρέπει να σημειωθεί ότι η μόνη οδηγία του IMO που είναι πιο κοντά στην αντιμετώπιση των ζητημάτων προστασίας ICT των λιμένων είναι η οδηγία ISPS 2002 του IMO (Διεθνής Κώδικας Ασφαλείας Πλοίων και Λιμενικών Εγκαταστάσεων), την οποία όλοι οι εμπορικοί λιμένες θα πρέπει να τηρούν. Ωστόσο, η ISPS αφορά κυρίως απαιτήσεις ασφάλειας, όπως μπορούμε να δούμε στην επόμενη ενότητα.

Διεθνής Κώδικας Ασφαλείας Πλοίων και Λιμενικών Εγκαταστάσεων (Κώδικας ISPS)

Ο Κώδικας ISPS διατυπώθηκε από τον IMO, ως απάντηση στις υποτιθέμενες απειλές σε πλοία και λιμάνια, στον απόηχο των τρομοκρατικών επιθέσεων του 2001, εναντίον των Ηνωμένων Πολιτειών. Η ISPS προσέγγιση για την προστασία των πλοίων και των λιμενικών εγκαταστάσεων βασίζεται σε μια διαδικασία διαχείρισης κινδύνων, η οποία εντοπίζει και αξιολογεί τους κινδύνους και, τέλος, καθορίζει ποιά είναι τα καταλληλότερα μέτρα προστασίας, σε κάθε συγκεκριμένη περίπτωση.

Ο κώδικας ISPS (ως τροποποίηση των περί Προστασίας της Ανθρώπινης Ζωής στη Θάλασσα (SOLAS)), ορίζει συγκεκριμένες απαιτήσεις και κανόνες ασφάλειας, που πρέπει να αντιμετωπιστούν από τα πλοία και τα λιμάνια. Ειδικότερα,

οι εγκαταστάσεις των λιμένων πρέπει να εκπληρώσουν διάφορες υποχρεώσεις, όπως οι εξής: (α) δημιουργία της κατάλληλης διαχείρισης προστασίας, καθορίζοντας ειδικά καθήκοντα και αρμοδιότητες σε όλο το προσωπικό της λιμενικής εγκατάστασης, (β) υιοθέτηση των αντισταθμιστικών μέτρων που καλύπτουν όλους τους τρόπους πρόσβασης στη λιμενική εγκατάσταση, (γ) προσδιορισμός των ζωνών περιορισμένης πρόσβασης, εντός της λιμενικής εγκατάστασης, για την προστασία των επιβατών, του πλοίου και του προσωπικού των λιμενικών εγκαταστάσεων, των πλοίων που χρησιμοποιούν και εξυπηρετούν τη λιμενική εγκατάσταση και κρίσιμων περιοχών προστασίας, (δ) έγκριση των μέτρων που αφορούν τη μεταφορά φορτίου, για την πρόληψη της αλλοίωσης, (ε) θέσπιση μέτρων προστασίας, για να εξασφαλιστεί ο έλεγχος των ασυνόδευτων αποσκευών (δηλαδή οποιασδήποτε αποσκευής), (στ) παρακολούθηση της λιμενικής εγκατάστασης (συμπεριλαμβανομένων των περιοχών περιορισμένης πρόσβασης και των πλοίων και βρίσκονται κοντά σε αυτές), σε ξηρά και θάλασσα, ανά πάσα στιγμή, (ζ) δημιουργία του διαδικαστικού πλαισίου, για την διασύνδεση με το πλοίο.

Από την άλλη πλευρά, οι ναυτιλιακές εταιρίες έχουν να αντιμετωπίσουν, τουλάχιστον τα ακόλουθα: (α) τον καθορισμό της διακυβέρνησης της προστασίας των πλοίων. Ο κανονισμός ορίζει ειδικά καθήκοντα και αρμοδιότητες σε όλο το προσωπικό του πλοίου, (β) την υιοθέτηση των μέτρων που εμποδίζουν την χρήση των όπλων, επικίνδυνων ουσιών και μηχανισμών κατά προσώπων, πλοίων ή λιμένων, (γ) τον καθορισμό των διαδικασιών εκκένωσης, (δ) την έγκριση των αντισταθμιστικών μέτρων που εμποδίζουν την μη εξουσιοδοτημένη πρόσβαση στο πλοίο, (ε) τον προσδιορισμό των ζωνών περιορισμένης πρόσβασης εντός του πλοίου, (στ) την δημιουργία ενός περιστατικού χειρισμού και αναφοράς πλαισίου, (ζ) την δημιουργία του διαδικαστικού πλαισίου, για την διασύνδεση με τις λιμενικές εγκαταστάσεις, (η) τον ορισμό των οδηγιών και κατευθύνσεων, σχετικά με την χρήση του συστήματος προειδοποίησης προστασίας του πλοίου.

Στο πλαίσιο αυτό, όλα τα πλοία, οι λιμενικές εγκαταστάσεις και οι ναυτιλιακές εταιρείες θα πρέπει να συμμορφωθούν με τον κώδικα ISPS, σχετικά με ένα σύνολο κανόνων και κυρίως τις υποχρεώσεις ασφάλειας. Ως εκ τούτου, θα επικεντρωθούν μόνο στις φυσικές απειλές και την αντιμετώπιση των κινδύνων μόνο σχετικά με την προστασία. Ωστόσο, θα πρέπει να σημειωθεί ότι, καθώς το ISPS

αδυνατεί να καλύψει κρίσιμες πτυχές του θαλάσσιου περιβάλλοντος ICT και της προστασίας στον κυβερνοχώρο, τα πλοία, οι ναυτιλιακές εταιρείες και τα λιμάνια δεν δίνουν προσοχή στις νέες και επερχόμενες απειλές (π.χ. εκτέλεση κακόβουλου κώδικα, διείσδυση στο δίκτυο, γνωστοποίηση των ιδιωτικών πληροφοριών, και άρνηση παροχής υπηρεσιών) της ψηφιακής εποχής.

Ευρωπαϊκός Οργανισμός για την Ασφάλεια στη Θάλασσα (EMSA)

Η EMSA είναι ένας οργανισμός της ΕΕ, που ιδρύθηκε το 2004 και αναλαμβάνει καθήκοντα και ευθύνες, σχετικά με την προστασία στην θάλασσα (μετά την έναρξη ισχύος του κανονισμού 724/2004/EC). Διαδραματίζει συμβουλευτικό ρόλο, εκ μέρους της Επιτροπής, στον τομέα της προστασίας στην θάλασσα και πρόληψης της ρύπανσης από τα πλοία, σε επιστημονικό και τεχνικό επίπεδο. Δίνει έμφαση στην δημιουργία του κατάλληλου νομικού και κανονιστικού καθεστώτος, παρακολουθεί την εφαρμογή και αξιολογεί την αποτελεσματικότητα των μέτρων που εφαρμόζονται από τους εμπλεκόμενους φορείς. Ο Οργανισμός παρέχει την δυνατότητα συνεργασίας μεταξύ των κρατών-μελών, ούτως ώστε να διερευνηθούν αμοιβαίως επωφελείς προσεγγίσεις, να διαδώσουν τις καλύτερες πρακτικές τους και να ανταποκριθούν σε συγκεκριμένα αιτήματα, σε σχέση με την πρακτική εφαρμογή της κοινοτικής νομοθεσίας.

Ειδικότερα, τα καθήκοντα του Οργανισμού απόκεινται στους ακόλουθους τομείς:

- να ασκεί τα καθήκοντα ελέγχου επικουρικά προς την Επιτροπή κατά την τήρηση της εφαρμογής του πλαισίου της ΕΕ ,σχετικά με την έρευνα και την πιστοποίηση των πλοίων (πιστοποίηση του εξοπλισμού των πλοίων, την ασφάλεια των πλοίων, την εκπαίδευση των ναυτικών και του Κρατικού Ελέγχου Λιμένος),
- να αναπτύσσει και να διατηρεί τις ναυτικές ηλεκτρονικές υπηρεσίες και συστήματα, σε ευρωπαϊκό επίπεδο. Ξεχωριστά παραδείγματα είναι:
- το σύστημα παρακολούθησης σκαφών *SafeSeaNet*, που επιτρέπει την πανευρωπαϊκή παρακολούθηση των πλοίων και των φορτίων τους, και τα συμβαίνοντα επί του σκάφους,

- το κέντρο δεδομένων LRIT της ΕΕ, που εξασφαλίζει την ταυτοποίηση και τον εντοπισμό πλοίων με σημαία ΕΕ, σε όλο τον κόσμο,
- τον συντονισμό των προσπαθειών για την πρόληψη, την ανίχνευση και την αντιμετώπιση της θαλάσσιας ρύπανσης, καθώς την συμβολή στην προστασία των ακτών και των υδάτων της ΕΕ, μέσω της συντήρησης και της λειτουργίας του Ευρωπαϊκού Δικτύου Απόκρισης Πλοίων, σε ενδεχόμενες πετρελαιοκηλίδες, και ενός ευρωπαϊκού δορυφορικού συστήματος παρακολούθησης πετρελαιοκηλίδων και των υπηρεσιών εντοπισμού σκαφών (CleanSeaNet),
- την παροχή βοήθειας προς την Επιτροπή, σε τεχνικό και επιστημονικό επίπεδο, στον τομέα της θαλάσσιας ασφάλειας και πρόληψης της ρύπανσης από τα πλοία.

Για να συνοψίσουμε, η EMSA ενεργεί ως πάροχος υπηρεσιών, στους τομείς της ασφάλειας της ναυσιπλοΐας, την φυσική προστασία και την πρόληψη της ρύπανσης σε ευρωπαϊκό επίπεδο, αναλαμβάνοντας την ευθύνη για την συλλογή, τον συσχετισμό και την κοινοποίηση των σχετικών πληροφοριών στην Επιτροπή, τα κράτη μέλη και άλλους σχετικούς φορείς της Ευρωπαϊκής Ένωσης.

Διεκτελεστικός Οργανισμός του Ευρωπαϊκού Δικτύου Μεταφορών (TEN-T EA)

Η TEN-T EA στοχεύει στη στήριξη της Ευρωπαϊκής Επιτροπής, με την εξασφάλιση της επιτυχούς υλοποίησης του Διευρωπαϊκού Δικτύου Μεταφορών (TEN-T) του προγράμματος. Στο πλαίσιο των δραστηριοτήτων του παρόντος προγράμματος, ένα σύνολο έργων, με σκοπό να εξασφαλιστεί η συνοχή, η διασύνδεση και η διαλειτουργικότητα του διευρωπαϊκού δικτύου μεταφορών, έχει ξεκινήσει. Οι πλωτές μεταφορές και οι ναυτιλιακές υποδομές αποτελούν σημαντικές πτυχές του δικτύου μεταφορών.

Τα έργα TEN-T που αφορούν τις πλωτές οδούς, μπορούν να ομαδοποιηθούν στις ακόλουθες κατηγορίες:

- *Εσωτερικές πλωτές οδοί*: Τα έργα αυτής της κατηγορίας αποσκοπούν στην ενίσχυση της επαφής μεταξύ ενδοχώρας και των παράκτιων

περιοχών (π.χ. λιμένες) που επικοινωνούν μέσω συνδέσμων, όπως τα ποτάμια και τα κανάλια.

- *Υπηρεσίες πληροφοριών εσωτερικής ναυσιπλοΐας (RIS)*: Τα εμπλεκόμενα έργα δίνουν έμφαση στην βελτιστοποίηση των υποδομών διαχείρισης της κυκλοφορίας, στο δίκτυο εσωτερικών πλωτών οδών, μέσω της καθιέρωσης ενός διαλειτουργικού, ευφυούς συστήματος κυκλοφορίας και μεταφορών.
- *Οι ναυτιλιακοί λιμένες*: Τα σχέδια αυτά στοχεύουν στην ανάπτυξη των ναυτιλιακών μεταφορών μέσω του σχεδιασμού, της υλοποίησης και της λειτουργίας ενός συνόλου υπηρεσιών, για την μεταφορά επιβατών και εμπορευμάτων, συμπεριλαμβανομένων των υπηρεσιών πορθμείου και ναυσιπλοΐας μικρών και των ναυτιλιακών υπηρεσιών μεγάλων αποστάσεων, της ακτοπλοΐας, που συνδέει τα κράτη μέλη της ΕΕ μεταξύ τους, καθώς και με τρίτες χώρες.
- *Το διευρωπαϊκό δίκτυο θαλάσσιων αρτηριών (MoS)*: Η σχετική εστίαση του έργου, για την ανάπτυξη των κατάλληλων λιμενικών εγκαταστάσεων, υποδομών και υπηρεσιών βασίζεται στην εκ νέου δημιουργία του οδικού και σιδηροδρομικού δικτύου στο νερό.

Συμβούλιο Ναυτιλιακής Προστασίας

Το Συμβούλιο Ναυτιλιακής Προστασίας, που ιδρύθηκε το 1988, ελέγχει αρκετά ζητήματα, για την προστασία των ΗΠΑ και της διεθνούς ναυτιλιακής κοινότητας. Συνεργάζεται με ένα σύνολο σχετικών με την ναυτιλιακή προστασία και την καταπολέμηση της τρομοκρατίας οργανισμών και την κυβέρνηση των Ηνωμένων Πολιτειών και ενεργεί, ως ναυτιλιακός σύμβουλος, της κυβέρνησης των ΗΠΑ και της διεθνούς υπηρεσίας INTERPOL της αστυνομίας.

Κύριος στόχος του είναι να υποστηρίξει την διεθνή ναυτιλιακή εμπορική κοινότητα, σε θέματα που σχετίζονται με εγκληματικές και τρομοκρατικές απειλές μέσω των ακόλουθων διαύλων:

- εκπροσώπηση ναυτιλιακών συμφερόντων πριν από τους κρατικούς φορείς,
- λειτουργία ως σύνδεσμος, μεταξύ της βιομηχανίας και της κυβέρνησης,
- διάδοση έγκαιρη ενημέρωσης, ενθάρρυνση και παροχή βοήθειας για την ανάπτυξη συγκεκριμένων τεχνολογιών στην βιομηχανία,
- σύγκληση των εκπαιδευτικών και ενημερωτικών συνεδρίων για την ένταξη τους και για τους κυβερνητικούς εταίρους.

Συγκεκριμένα, προσπαθεί να αποτρέψει την παράνομη διακίνηση ναρκωτικών, λαθρεπιβάτης, κλοπή, προστασία της ιδιωτικής ζωής, την τρομοκρατία και την πειρατεία. Ωστόσο, πρέπει να σημειωθεί ότι ο οργανισμός δεν ασχολείται άμεσα με θέματα ΤΠΕ ή το κυβερνοέγκλημα.

8.2. Προσεγγίσεις διαχείρισης προστασίας στην Ναυτιλία

Μια συλλογή από μερικές από τα πιο σημαντικές μεθοδολογίες, τις μεθόδους και τα συστήματα που χρησιμοποιούνται, για την ανάλυση και διαχείριση των κινδύνων των λιμένων και των ναυτιλιακών υποδομών (εφαρμογή του κώδικα ISPS), είναι οι εξής:

- *Εργαλείο Αξιολόγησης Κινδύνου Προστασίας Λιμένος (PSRAT)*: Η PSRAT είναι ένα εργαλείο για την αξιολόγηση της προστασίας, που αναπτύχθηκε από την Αμερικανική Ακτοφυλακή. Ο βασικός στόχος της PSRAT είναι η αξιολόγηση των υποδομών των λιμένων, με βάση τις απαιτήσεις ασφαλείας που καθορίζονται στον κώδικα ISPS. Είναι ένα εργαλείο που αξιολογεί τον κίνδυνο της τρομοκρατίας, τον οποίο αντιμετωπίζουν αυτές οι υποδομές, και βοηθά τους αναλυτές στην βελτίωση των στρατηγικών και στην σύνταξη τακτικών σχεδίων, για την θέσπιση ενός περιβάλλοντος ασφαλούς και αποτελεσματικής διακίνησης αγαθών, υπηρεσιών και ανθρώπων.
- *Μοντέλο Ανάλυσης Επικινδυνότητας Ναυτιλιακής Προστασίας (MSRAM)*: Το μοντέλο ανάλυσης επικινδυνότητας ναυτιλιακής προστασίας είναι ένα εργαλείο αξιολόγησης των κινδύνων της τρομοκρατίας, που αναπτύχθηκε από την Ακτοφυλακή των Ηνωμένων Πολιτειών (USCG). Η τελευταία

χρησιμοποιεί την MSRAM, για να αξιολογήσει τους κινδύνους που προέρχονται από τρομοκρατικές επιθέσεις και να θεσπίσει τα κατάλληλα σχέδια μετριασμού των επιπτώσεων βελτιώνοντας την προστασία των υποδομών, σε λιμένες και πλοία. Η MSRAM υποστηρίζει μια μέθοδο για την εκτίμηση και την πρόληψη κινδύνων, σε διαφορετικά είδη-στόχους, τους τρόπους επίθεσης, και τα γεωγραφικά επίπεδα (λιμένες, περιφέρειες, εθνικά δίκτυα). Οι τρομοκρατικές επιθέσεις, που γίνονται αντιληπτές ως απειλές, για την ναυτιλιακή προστασία, συνήθως διεξάγονται, αναφορικά με τους στόχους, πάνω ή κοντά σε ακτές και τις εθνικές πλωτές οδούς, από αρχετυπικούς τρόπους επίθεσης, όπως οι βόμβες σε φορτηγά, ο εμβολισμός από πειρατεία σκάφους, κλπ. Ωστόσο, η MSRAM είναι σε θέση να καλύψει ευρύτερες (μη τρομοκρατικές) απειλές που συνδέονται με την δημόσια προστασία, όπως τα ατυχήματα, οι πλημμύρες, οι πανδημίες ή άλλες φυσικές καταστροφές.

Οι συνέπειες που προέρχονται από μια επιτυχημένη επίθεση χωρίζονται σε πέντε επίπεδα: τον θάνατο και τον τραυματισμό, το πρωτοβάθμιο και το δευτεροβάθμιο οικονομικό αντίκτυπο, την συμβολική επίδραση, την εθνική προστασία και τις περιβαλλοντικές επιπτώσεις. Για να εξασφαλίζεται η ομοιομορφία, η MSRAM ορίζει τους αναμενόμενους παράγοντες κινδύνου ποσοτικά.

- *Μοντέλο Ανάλυσης Επικινδυνότητας Ναυτιλιακής Προστασίας PLUS/FORETELL (* MSRAM-PLUS *)* : Το μοντέλο MSRAM-PLUS προσπαθεί να επεκτείνει την στατική μέθοδο φυσικής ανάλυσης κινδύνου MSRAM, προσθέτοντας διάφορες δυνατότητες, όπως η υποστήριξη της ανάλυσης για το πώς οι στρατηγικές μετριασμού του υποψήφιου κινδύνου βελτιώνουν την ασφάλεια, επιτρέποντας συγκρίσεις των προβλεπομένων κόστων και των οφελών των ανταγωνιστικών στρατηγικών, παρέχοντας «κύκλο ζωής» υποστήριξης αποφάσεων, μέσω της παρακολούθησης των στρατηγικών και της εκτίμησης ότι οι αντιπάλους και τα άλλα ενδιαφερόμενα μέρη είναι πιθανό να ανταποκριθούν, σε μελλοντικούς στρατηγικές. Στο πλαίσιο αυτό, το MSRAM-PLUS βασίζεται σε μια δυναμική μεθοδολογία υποστήριξης αποφάσεων κινδύνου, η οποία στηρίζεται σε μοντελοποίηση και ανάλυση, που έχει σχεδιαστεί για να αξιοποιήσει τις μεθόδους MSRAM, τα μοντέλα, το λογισμικό και τα δεδομένα,

- *Αξιολόγηση Ναυτιλιακού κινδύνου (MARISA)* : το MARISA είναι ένα σύστημα λήψης αποφάσεων που ενσωματώνει μια συγκεχυμένη προσέγγιση, προκειμένου να αξιολογήσει την εκτίμηση των ναυτιλιακών κινδύνων. Εφαρμόζεται για την ναυτιλιακή προστασία και, πιο συγκεκριμένα, την πρόληψη της ρύπανσης στην ανοιχτή θάλασσα. Το MARISA δεν εξετάζει τις ICT ή την αξιολόγηση του κινδύνου στον κυβερνοχώρο. Ορίζει έναν παράγοντα κινδύνου για κάθε πλοίο, που καθορίζεται από την ασαφή προσέγγιση σύμφωνα με τα ακόλουθα στοιχεία:
- Τα στατικά χαρακτηριστικά. Τα δεδομένα εισόδου για αυτόν τον παράγοντα είναι τα εξής: σημαία, έτος κατασκευής, αριθμός των εταιρειών, ολική χωρητικότητα, διάρκεια των απαγορεύσεων απόπλου και είδος των πλοίων,
- μετεωρολογικές συνθήκες (π.χ. ταχύτητα του ανέμου, κατάσταση της θάλασσας, προβολή),
- δυναμική του πλοίου (π.χ. λόγω της κακής κατάστασης της θάλασσας ή λόγω της ρύπανσης, το πλοίο αλλάζει την πορεία του).
- *Περιεκτικό Σύστημα Ναυτιλιακής Επίγνωσης (CMA)*: Ο κύριος στόχος της CMA είναι να παρέχει μία μέθοδο και ένα εργαλείο που συγκεντρώνει, αναλύει και να συσχετίζει τις πληροφορίες που προέρχονται από πολλαπλές πηγές (συμπεριλαμβανομένης της Κοινής Επιχειρησιακής Εικόνας PACOM (COP), του Αυτοματοποιημένου Συστήματος Πληροφοριών (AIS), του Τμήματος Συστημάτων Άμυνας, των βάσεων δεδομένων του Υπουργείου Εμπορίου, των πληροφοριών του Τμήματος Εσωτερικής Ασφάλειας), με ένα αποτελεσματικό και αποδοτικό τρόπο, προκειμένου να εντοπιστούν ανωμαλίες που οδηγούν στον εντοπισμό των απειλών κατά της προστασίας. Στο πλαίσιο αυτό, η CMA είναι σε θέση να παρακολουθεί τις ναυτιλιακές μεταφορές, συμπεριλαμβανομένων των σκαφών, των ανθρώπων και του φορτίου· τον εντοπισμό δυνητικών απειλών· και την εστίαση της προτεραιότητας στην δράση.

Όλες οι παραπάνω μέθοδοι και τα συστήματα που αναλύθηκαν, όπως γίνεται αντιληπτό από τους στόχους τους, είναι σε θέση να ασχοληθούν μόνο με την προστασία των λιμένων και των συστημάτων PICT τους. Οι Απειλές ICT ή του κυβερνοχώρου δεν λαμβάνονται υπόψη και δεν αντιμετωπίζονται.

8.3. Οι εθνικές περιπτωσιολογικές μελέτες για τη διαχείριση της ναυτιλιακής προστασίας

Το τμήμα αυτό παρουσιάζει τρεις εθνικές μελέτες περιπτώσεων, που απεικονίζουν τις στρατηγικές αξιολόγησης κινδύνων και των συστημάτων που εγκρίθηκαν από συγκεκριμένους λιμένες, προκειμένου να αντιμετωπίσουν μια σειρά από θέματα ασφάλειας της ναυσιπλοΐας. Καμία από τις εθνικές περιπτωσιολογικές μελέτες αφορά τις απειλές ICT ή τον κυβερνοχώρο.

Μελέτη περίπτωσης της Εσθονίας

Κατά την τελευταία δεκαετία, οι αρχές της Εσθονίας ξεκίνησαν τον σχεδιασμό και την προμήθεια συστημάτων ραντάρ λιμένος, για την σύγχρονη εθνική επιτήρηση των ακτών, προκειμένου να βελτιωθεί το επίπεδο επίγνωσης της ναυτιλιακής κατάστασης. Στο πλαίσιο αυτό, υιοθετήθηκε μία ολοκληρωμένη δέσμη μέτρων, που συνοψίζονται ως εξής:

Α) Η ενσωμάτωση της Διαχείρισης Κυκλοφορίας Πλοίων και του Συστήματος Πληροφοριών (VTMIS, VTS), το Αυτοματοποιημένο Σύστημα Πληροφοριών Ξηράς (AIS) και οι δυνατότητες πληροφόρησης και επικοινωνίας, μέσω των ραντάρ παρακολούθησης (TETRA) διατίθενται από τα εθνικά συστήματα και τις αρμόδιες λιμενικές αρχές, για να βελτιώσουν την ικανότητα τους αντιμετώπισης απειλών,

Β) Η ασφαλής και έγκαιρη αυτοματοποιημένη επικοινωνία δεδομένων είναι απαραίτητη, ώστε να διασφαλίζεται η επιτυχία της αποστολής των λιμένων και η μείωση της απώλειας της ζωής και των ζημιών σε ακίνητα, ως συνέπειες ενός συμβάντος,

Γ) Η αξιοποίηση των στοιχείων του συστήματος COTS επιτρέπουν τον σχεδιασμό και την τοποθέτηση λύσεων σε λογικές τιμές, σε σύντομο χρονικό διάστημα.

Μελέτη περίπτωσης της Ιορδανίας

Οι αρχές του λιμένα της Άκαμπα, σε συνεργασία με έναν αναγνωρισμένο οργανισμό ασφάλειας και την Ναυτιλιακή Αρχή Ιορδανίας (JMA), μια εξειδικευμένη

διοίκηση υπό την αιγίδα του Υπουργείου Μεταφορών στην Ιορδανία, ως υπεύθυνοι για την εφαρμογή των διατάξεων της Σύμβασης SOLAS και του Κώδικα ISPS, ολοκλήρωσαν την αξιολόγηση των λιμενικών εγκαταστάσεων. Ο σκοπός της αξιολόγησης ήταν να ληφθούν όλα τα απαραίτητα μέτρα για να εξασφαλιστεί η προστασία του λιμένος και να αποφευχθεί οποιαδήποτε τρομοκρατική δράση.

Η αξιολόγηση καλύπτει όλες τις βασικές απαιτήσεις του κώδικα ISPS, που συνοψίζονται ως εξής:

- Προσδιορισμός και αξιολόγηση των κύριων στοιχείων του ενεργητικού και των υποδομών που πρέπει να προστατεύονται,
- Προσδιορισμός των πιθανών απειλών, για τα επενδυτικά αγαθά και υποδομές και της πιθανότητας εμφάνισης τους, για να καθιερώσουν και να ιεραρχήσουν τα μέτρα προστασίας,
- Προσδιορισμός, επιλογή και ιεράρχηση των αντισταθμιστικών μέτρων, διαδικαστικές αλλαγές του βαθμού αποτελεσματικότητάς τους, όσον αφορά την μείωση της ευπάθειας.
- Προσδιορισμός των αδυναμιών, συμπεριλαμβανομένου του ανθρώπινου παράγοντα, σε υποδομές, πολιτικές και διαδικασίες.
- Προετοιμασία έκθεσης που συνοψίζει το πώς η αξιολόγηση πραγματοποιήθηκε, συμπεριλαμβανομένης της περιγραφής των αντισταθμιστικών μέτρων που θα μπορούσαν να χρησιμοποιηθούν για την αντιμετώπιση των αδυναμιών του.

Μέσω αυτής της διαδικασίας, ο λιμένας της Άκαμπα συστήνει ένα κατάλληλο πλαίσιο προστασίας, σύμφωνα με την υιοθέτηση του κώδικα ISPS και την ενσωμάτωση των αντισταθμιστικών μέτρων που απαιτούνται για να εξασφαλιστεί η προστασία των λιμενικών εγκαταστάσεων, των πλοίων, των ατόμων και των αγαθών, από τους κινδύνους που προκύπτουν από τα ατυχήματα τα οποία απειλούν την προστασία.

Μελέτη περίπτωσης της Ρωσίας

Οι ρωσικές αρχές έχουν δημιουργήσει ένα περιφερειακό σύστημα ναυτιλιακής προστασίας, που λειτουργεί στο ανατολικό τμήμα του Κόλπου της Φινλανδίας. Αυτό

το σύστημα είναι ένα ενιαίο λογισμικό και σύνθετο υλικό, με υψηλό βαθμό ολοκλήρωσης των συστατικών που περιλαμβάνει τα συστήματα διαχείρισης της κυκλοφορίας πλοίων, τις διακλαδώσεις του δικτύου γραμμών μικροκυμάτων και πολυπλέκτες, τους σταθμούς ακτής UAIS, μία κοινή βάση δεδομένων, την παροχή ισχύος του αντικειμένου και τα υποσυστήματα υποστήριξης της ζωής, την εξ αποστάσεως παρακολούθηση της λειτουργίας του εξοπλισμού, των μετεωρολογικών σταθμών και άλλων υποσυστημάτων.

Με βάση αυτό το σύστημα αρθρωτής δομής, έχει αναπτυχθεί το Σύστημα Παράκτιας Επιτήρησης Navi-Monitor. Το Navi-Monitor είναι ένα σύστημα υψηλής τεχνολογίας επιτήρησης και έγκαιρης προειδοποίησης, προσαρμοσμένο στις ανάγκες των λιμανιών μικρού και μεσαίου μεγέθους, φρουρόντας τα παράκτια αντικείμενα και τις υπεράκτιες πλατφόρμες. Αυτό το σύστημα είναι ιδανικό για την κάλυψη των απαιτήσεων προστασίας λιμενικών εγκαταστάσεων, όπως ορίζονται στο Κεφάλαιο 11 της SOLAS-74 του κώδικα ISPS.

Επίσης, έχει αναπτυχθεί ένα Σύστημα Διαχείρισης Κρίσεων (CMS), το οποίο παρέχει μια αυτοματοποιημένη λύση για να παρακολουθεί και να αναλύει μια κατάσταση και να παρέχει την υποστήριξη λήψης αποφάσεων, για τις έκτακτες ανάγκες διαφόρων φύσεων και κλιμάκων. Αυτό το σύστημα ενσωματώνει εργαλεία, για την οπτική παρουσίαση των πληροφοριών (συμπεριλαμβανομένης της σε πραγματικό χρόνο παρακολούθηση του προσωπικού και των κινήσεων του οχήματος), τον σχεδιασμό, την αποθήκευση δεδομένων, και την αναζήτηση για δίκτυα πληροφόρησης και επικοινωνίας. Τα μέρη του συστήματος έχουν σχεδιαστεί για να υποστηρίξουν την εκτίμηση ζημιών, τον σχεδιασμό των δράσεων ανταπόκρισης και τον γενικό έλεγχο των ενεργειών καταπολέμησης της κρίσης.

8.4. Πρωτοβουλίες Έρευνας

Ένας αριθμός προπαρασκευαστικής δράσης, για προγράμματα έρευνας της ασφάλειας (PASR), και των προγραμμάτων Έρευνας για την Προστασία FP7, έχουν δρομολογηθεί, κατά την τελευταία δεκαετία, για την αντιμετώπιση των θεμάτων που σχετίζονται με την ενίσχυση της προστασίας των λιμένων ή / και των συστημάτων PICT τους. Τα περισσότερα από αυτά τα έργα έχουν μειωθεί σε τρεις κύριες κατηγορίες, όπως ακολούθως:

- *Βελτιωμένα συστήματα ναυτιλιακής επιτήρησης*, με την ενίσχυση της διαλειτουργικότητας των τοπικών και εθνικών συστημάτων επιτήρησης, μέσω της συνένωσης των διατομεακών πληροφοριών, για την παρακολούθηση και την σύντηξη τους, σε μια κεντρική βάση δεδομένων. Αντιπροσωπευτικά παραδείγματα είναι τα εξής:
- Το Έργο Αυτόνομου Συστήματος Ναυτιλιακής Επιτήρησης (AMASS) επικεντρώνεται στην ενίσχυση της ναυτιλιακής επιτήρησης και την καλύτερη ενσωμάτωση πληροφοριών και στοιχείων, μεταξύ των αρμόδιων φορέων. Ο στόχος ήταν η ανάπτυξη ενός συστήματος έγκαιρης προειδοποίησης αιχμής των ναυτιλιακών αρχών, που παρέχει, στις υπηρεσίες επιβολής του νόμου, πληροφορίες σχετικά με απόπειρες παράνομης μετανάστευσης, και άλλες εγκληματικές δραστηριότητες στην θάλασσα.
- Το πρόγραμμα Υποβρύχια Έρευνα Παράκτιας Ζώνης (UNCOSS) είναι μια οικονομικά αποδοτική ανταπόκριση ενισχύοντας την άμυνα κατά των νέων τρομοκρατικών επιθέσεων, ιδίως τις απειλές από υποβρυχίους αυτοσχέδιους εκρηκτικούς μηχανισμούς (IED). Παρέχει μια θεμελιώδη τεχνολογία, για το παγκόσμιο πρόβλημα της ναυτιλιακής επιτήρησης και τους λιμένες / ναυτική προστασία των υποδομών.
- Το πρόγραμμα επιτήρησης των συνόρων, των ακτών και των λιμένων (SOBCAH) προσπάθησε να συνδυάσει και να μεγιστοποιήσει την χρήση των υφιστάμενων τεχνολογιών επιτήρησης στο στις πιο αποτελεσματικές επιχειρησιακές διαδικασίες του μοντέλου, για την ενίσχυση της επιτήρησης των συνόρων, των ακτών και των λιμένων.
- Το έργο ναυτιλιακής επιτήρησης των συνόρων (SEABILLA) έχει ως στόχο να καθορίσει την οικονομικά αποδοτική αρχιτεκτονική των ευρωπαϊκών συστημάτων επιτήρησης των θαλασσίων συνόρων, να ενσωματώνει τον χώρο, την γη, την θάλασσα και τον αέρα, συμπεριλαμβανομένων των συστημάτων μετάδοσης των επενδυτικών αγαθών. Το έργο είναι η εφαρμογή προηγμένων τεχνολογικών λύσεων, για την βελτίωση της απόδοσης των λειτουργιών επιτήρησης.

Η διαλειτουργικότητα των συστημάτων PICT ενισχύει την ικανότητα να συλλέγουν και να συγχωνεύουν τα ναυτιλιακά συναφή δεδομένα, σε μια κοινή και ολοκληρωμένη εικόνα που πρέπει να μοιράζεται μεταξύ των σχετικών οργανισμών.

Τα έργα της κατηγορίας αυτής είναι τα ακόλουθα:

- Το σχέδιο διαλειτουργικής προσέγγισης, για την προστασία της ασφάλειας στην θάλασσα (OPERAMAR), της Ευρωπαϊκής Ένωσης προσπάθησε να λύσει το πρόβλημα του κατακερματισμού μεταξύ των κρατών-μελών, πρόβλημα που προκαλείται από την εμμονή των εθνικών ειδικών διαδικασιών, τις νομοθεσίες και τα συστήματα που παρεμποδίζουν τη διαλειτουργικότητα, την μεγαλύτερη ανταλλαγή πληροφοριών και την βελτίωση του συντονισμού.
- Το πρόγραμμα ανίχνευσης δεδομένων SECCONDD σχεδιάστηκε για την διεθνή προτυποποίηση των τεχνικών διασύνδεσης ανάμεσα σε έναν ασφαλή περιέκτη ή το όχημα, και για την ανάγνωση δεδομένων σε λιμένα ή κατά την διέλευση των συνόρων. Η διασύνδεση θα επιτρέψει, στους υπαλλήλους του εμπορίου, την επιβολή του νόμου και να διαβάσουν τα δεδομένα προστασίας, συμπεριλαμβανομένων των αποθηκευμένων πληροφοριών από εσωτερικούς αισθητήρες προστασίας.

Προστασία των κρίσιμων ναυτιλιακών υποδομών, μετριάζοντας τους κινδύνους των περιστατικών ναυτιλιακής προστασίας. Ένας αξιοσημείωτος κατάλογος προγραμμάτων είνα οι ακόλουθος:

- Το πρόγραμμα "σύστημα προστασίας για τις ναυτιλιακές υποδομές, τους λιμένες και Παράκτιες Ζώνες" (SECTRONIC) προσπάθησε να βελτιώσει την ασφάλεια των στρατιωτικών πλοίων (επιβατηγά και φορτηγά πλοία), των πλατφόρμων και των εγκαταστάσεων παραγωγής ενέργειας, καθώς και των λιμένων μέσω της προηγμένης πληροφόρησης, των αισθητήρων και των τεχνολογιών απάντησης. Είχε ως στόχο να αναπτύξει ένα ολοκληρωμένο σύστημα προστασίας που συνδυάζει την επιτήρηση, την ανίχνευση εισβολέων, καθώς και την απάντηση, στα γεγονότα και τα περιστατικά.
- Η Αναβάθμιση της Ασφάλειας των Λιμένων (SUPPORT) στοχεύει να αυξήσει το τρέχον επίπεδο προστασίας των λιμένων, με την ενσωμάτωση συστημάτων

μετάδοσης στους λιμένες, με νέα συστήματα παρακολούθησης και διαχείρισης πληροφοριών. Επιπλέον, το έργο ΥΠΟΣΤΗΡΙΞΗ δίδει μια ιδιαίτερη έμφαση στον έλεγχο των συνόρων, με στόχο να εξασφαλίσει την αδιάλειπτη ροή φορτίων και επιβατών, ενώ επιτρέπει την αποτελεσματική πάταξη της παράνομης μετανάστευσης και της εμπορίας.

Βιβλιογραφία

1. AbeleWigert I., Dunn M., "Απογραφή των είκοσι εθνικών και διεθνών πολιτικών και των έξι Κρίσιμων Υποδομών Προστασίας"
2. AS / NZS 4360. Πρότυπα διαχείρισης κινδύνου στην Αυστραλία.
3. Adler R., Fuller J., " Ένα ολοκληρωμένο πλαίσιο για την εκτίμηση και τον περιορισμό των κινδύνων στις θαλάσσιες υποδομές ζωτικής σημασίας"
4. Balmat J., Lafont F., Maifret R., Pessel N., "Αξιολόγηση θαλάσσιου κινδύνου (MARISA): μια συγκεχυμένη προσέγγιση για τον ορισμό ενός ανεξαρτήτου παράγοντα κινδύνου του πλοίου", Ocean Engineering
5. BitNami Φιλοξενία νεφών για εφαρμογές Ανοιχτής Πηγής,
6. Bohren, J.. Et al .. 2005. "Γλώσσα Εμπιστοσύνης Υπηρεσιών Διαδικτύου (WS-Trust)",
7. Πρότυπο BSI 100-1. (2005). Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).
8. Πρότυπο BSI 100-2. (2005). Μεθοδολογία IT-Grundszchutz.

9. Πρότυπο BSI 100-3. (2005). Η ανάλυση κινδύνου βασίζεται στην μεθοδολογία IT-Grundszchutz.

10. Cloud Computing. Λογισμικό από Eucalyptus

11. Club de la Securite de L' Information Français Methods Commision, Οδηγός Ανάλυσης και Αντιμετώπισης Mehari Κινδύνου 2010

12. collectd, σύστημα συλλογής στατιστικών

13. Crespo F., Gomez M., Candau J., Manas JA, "MAGERIT - έκδοση 2, Μεθοδολογία Ανάλυσης Κινδύνου Συστημάτων και Διαχείρισης Πληροφοριών, Βιβλίο I - Η μέθοδος",

14. Crespo F., Gomez M., Candau J., Manas JA, "Magerit - έκδοση 2, Μεθοδολογία Ανάλυσης Κινδύνου Συστημάτων και Διαχείρισης Πληροφοριών, Βιβλίο II - Κατάλογος των Στοιχείων",

15. Crespo F., Gomez M., Candau J., Manas JA, "Magerit - έκδοση 2, Μεθοδολογία Ανάλυσης Κινδύνου Συστημάτων και Διαχείρισης Πληροφοριών, Βιβλίο III - Τεχνικές",

16. Downs B., "Το Μοντέλο Ανάλυσης της Αντιμετώπισης Ναυτιλιακού Κινδύνου", in: US Coast Guard Proc. of the Marine Safety and Security Council,

17. ENISA (Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών), "Διαχείριση Κινδύνων: Αρχές υλοποίησης και Αποθέματα για τις μεθόδους αξιολόγησης Διαχείρισης Κινδύνων / κινδύνου και των εργαλείων",

18. ENISA, εργαστήριο για θέματα ασφάλειας στον κυβερνοχώρο, στον ναυτιλιακό τομέα

19. ENISA, Έκθεση "Ανάλυση των πτυχών της ασφάλειας στον κυβερνοχώρο, στον ναυτιλιακό τομέα

20. Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας,

21. Ευρωπαϊκός Οργανισμός για την Ασφάλεια στη Θάλασσα

22. Ευρωπαϊκό Σχέδιο Αντιμετώπισης της Μετανάστευσης 2.0

23. Έκφραση των αναγκών και εντοπισμός των Στόχων προστασίας PREMIER,

24. eyeOS, ένα σύνολο των ιθαγενών εφαρμογές cloud

25. Haavel R., OIT M., Usk A., "Η διαθεσιμότητα των πληροφοριών θαλάσσιας επιτήρησης στην Εσθονία", E. Shahbazian, et al. (Εκδ.), Προστασία λιμένος μέσω των τεχνολογιών της σύντηξης δεδομένων,

26. Πληροφορίες Αξιολόγησης Ασφάλειας & Μέθοδος Παρακολούθησης (ISAMM).

27. Διεθνής Ναυτιλιακός Οργανισμός

28. Insight Consulting, CRAMM Οδηγός χρήσης, Τεύχος 5.1

29. ISO / IEC. Η τεχνολογία της πληροφορίας - τεχνικές ασφάλειας - Προδιαγραφή για ένα Σύστημα Διαχείρισης Προστασίας Πληροφοριών, ISO / IEC 27001, 2005.

30. ISO / IEC. Η τεχνολογία της πληροφορίας - τεχνικές ασφάλειας - κώδικας πρακτικής για τη διαχείριση Προστασίας των πληροφοριών, ISO / IEC 27002, 2005.

31. ISO / IEC. Πληροφορική - Τεχνικές Ασφάλειας - Ασφάλεια Διαχείρισης Κινδύνων Πληροφοριών, ISO / IEC 27005, 2008.

32. Kakish B., «Προστασία λιμένος στην ιορδανική λιμάνι της Άκαμπα", E. Shahbazian, et al. (Εκδ.), Προστασία λιμένος μέσω των τεχνολογιών της σύντηξης δεδομένων

33. Karantjias, A., και Πολέμη, N. "Μια καινοτόμος αρχιτεκτονική πλατφόρμα για Περίπλοκες Ασφαλείς e / m Κυβερνητικές Υπηρεσίες"

34. Σχέδιο "Λευκή Βίβλος" της Liberty Alliance: Liberty Alliance & WS-Federation:

35. Lockhart, H., et al (2006). "Γλώσσα Ομοσπονδίας Διαδικτυακών Υπηρεσιών (WS-Federation)",

36. Luiijf E., Burger H., Klaver M., "Προστασία Υποδομής Ζωτικής Σημασίας στην Ολλανδία: Μια γρήγορη ματιά"

37. "Κοινότητα Ενδιαφέροντος του Ναυτιλιακού Τομέα Ευαισθητοποίησης για την Κοινοποίηση Δεδομένων

38. Υπουργείο Εσωτερικών και Σχέσεων του Βασιλείου, Οδηγός Μεθόδου Εθνικής Αξιολόγησης του κινδύνου 2008. Εθνικό Πρόγραμμα Ασφάλειας

39. Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, οδηγός διαχείρισης κινδύνων για τα συστήματα τεχνολογίας των πληροφοριών

40. Nimbus είναι το cloud computing για την επιστήμη

41. Novikov Σ., «Η εφαρμογή του κώδικα ISPS στην Ρωσική Ομοσπονδία: Πλοία και Λιμένες», E. Shahbazian, et al. (Εκδ.), Προστασία λιμένος μέσω των τεχνολογιών της σύντηξης δεδομένων

42. Ntouskas T., Kotzanikolaou P. και N. Polemi: Αξιολόγηση των επιπτώσεων μέσω Συνεργατικής Asset Μοντελοποίηση: Η προσέγγιση STORM-RM, 1ο Διεθνές Συμπόσιο & 10ο Βαλκανικό Συνέδριο Επιχειρησιακής Έρευνας,

43. Ntouskas T., Kotzanikolaou P. και N. Polemi: "Εμπιστευτικές συνεργατικές υπηρεσίες για τη διαχείριση της ασφάλειας πληροφορικής των ΜΜΕ / ΚΟΑ",

44. Ntouskas T., Kotzanikolaou P. και N. Polemi: "Μια συνεργατική υπηρεσία διαχείρισης προστασίας που προσφέρει το σύστημα για τα ΜΜΕ / ΚΟΑ"

45. Ntouskas T., Pentafronimos G. και Papastergiou G., "STORM - Συνεργατικό Περιβάλλον Διαχείρισης Προστασίας»,

46. Ntouskas, T., Polemi, N., «Ένα ασφαλές, συνεργατικό περιβάλλον για την διαχείριση προστασίας των λιμενικών πληροφοριακών συστημάτων", Πρακτικά του Πέμπτου Διεθνούς Συνεδρίου για το Διαδίκτυο και τις διαδικτυακές εφαρμογές και υπηρεσίες,

47. Ntouskas, T., Polemi, N., «STORM-RM: Μια συλλογική και πολυκριτηριακή μεθοδολογία διαχείρισης κινδύνου»,

48. Ntouskas, T., Polemi, N., Συνεργατικές υπηρεσίες διαχείρισης προστασίας για τα πληροφοριακά συστήματα λιμένος, in: International Conference on e-Business,

49. Oasis Standard. Γλώσσα Προστασίας Ισχυρισμού σήμανσης (SAML) V2.0,

50. OCTAVE Οδηγός Μεθόδου Εφαρμογής Έκδοση 2.0,

51. OpenNebula: Η Λύση Ανοικτού Κώδικα για το Κέντρο Εικονικοποίησης Δεδομένων,

52. Το λογισμικό ανοιχτού κώδικα για την κατασκευή ιδιωτικών και δημοσίων νεφών,

53. Polemi, N., Pentafronimos, G., Ntouskas, T. "IMP2.0 Συνεργατική Πλατφόρμα Μετανάστευσης και ηλεκτρονικές υπηρεσίες"

54. Pentafronimos, G., Karantjias, A. & Polemi, N. (2010), ODYSSEUS: Ένα προηγμένο, συνεργατικό και Εμπιστευτικό Πλαίσιο Παροχής Υπηρεσιών Μετανάστευσης, Πρακτικά Πέμπτου Διεθνούς Συνεδρίου για το Διαδίκτυο και τις Εφαρμογές και Υπηρεσίες Δικτύου (ICIW), IEEE Κοινωνία Ψηφιακής Βιβλιοθήκης Υπολογιστών

55. TL Saaty. Λήψη αποφάσεων με την αναλυτική διαδικασία ιεράρχησης. SafeSeaNet: ευρωπαϊκό σύστημα ανταλλαγής ναυτιλιακών πληροφοριών

56. Sokolov A., "Βήματα για τη βελτίωση παράκτιου λιμένος και της προστασίας λιμένος: Η Ανάπτυξη των Περιφερειακών Συστημάτων Προστασίας της Ναυσιπλοΐας για την Ρωσική Ομοσπονδία", E. Shahbazian, et al. (Εκδ.), Προστασία λιμένος μέσω τεχνολογιών συγχώνευσης δεδομένων,

57. S-PORT "Ένα ασφαλές, αυτοματοποιημένο περιβάλλον συνεργασίας για την δημιουργία των μεθοδολογιών αξιολόγησης του κινδύνου, την παραγωγή της επιχειρησιακής συνέχειας και την ανάκαμψη από καταστροφή σχέδια για τα Συστήματα Πληροφοριών Λιμένος", που χρηματοδοτείται από τη ΓΓΕΤ

(Γενική Γραμματεία Έρευνας και Τεχνολογίας του Υπουργείου Ανάπτυξης) το εθνικό ερευνητικό πρόγραμμα «ΣΥΝΕΡΓΑΣΙΑ» (ΕΣΠΑ 2007-2013)

58. Διεκτελεστικός Οργανισμός του Ευρωπαϊκού Δικτύου Μεταφορών

59. Ubuntu, πλατφόρμα

60. Υπουργείο Ενέργειας των ΗΠΑ, Εγχειρίδιο Πόρων για Αξιολόγηση Κινδύνου Μεταφορών DOE. Έκθεση DOE/EM/NTP/HB-01, Εθνικό Πρόγραμμα Μεταφορών

61. Yusta JM, Correa GJ, Lacal-Arántegui R., "Μεθοδολογίες και εφαρμογές για την προστασία των κρίσιμων υποδομών

62. Zambon, E., Etalle, S., Wieringa, RJ & Hartel, PH (2011). "Μοντέλο με βάση την ποιοτική αξιολόγηση των κινδύνων για τη διαθεσιμότητα των υποδομών πληροφορικής",

63. http://bitnami.org/cloud

64. www.bsi.bund.de

65. http://www.eucalyptus.com/ .

66. http://www.clusif.asso.fr/fr/- production/ouvrages/pdf/MEHARI-2010 Κίνδυνος-ανάλυση-και-Θεραπεία-Guide.pdf

67. http://collectd.org/related.shtml

68. http://www.uscg.mil/proceedings/

69. http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final. pdf

70. http://www.enisa.europa.eu/act/-res/workshops-1/2011/cyber-security-aspects-in-the-maritime-sector .

71. http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector/cyber-security-aspects-in-themaritime- sector-1

72. http://www.easa.europa.eu

73. http://www.emsa.europa.eu/

74. http://www.immigrationpolicy2.eu/

75. www.ssi.gouv.fr

76. http://www.eyeos.org/

77. http://www.telindus.com

78. http://www.imo.org/Pages/home.aspx

79. http://www.projectliberty.org/resources/whitepapers/ .

80. http://www.uscg.mil/acquisition/nais/ RFP / SectionJ / MDA-COI-vocab.pdf .

81. http://www.minbzk.nl//bzk2006uk/subjects/public-safety/publications/115647/ / national risk

82. http://www.nimbusproject.org/

83. http://www.cert.org/octave/

84. http://opennebula.org/ .

85. http://openstack.org/ .

86. http://s-port.unipi.gr/ .

87. http://tentea.ec.europa.eu/

88. http://www.ubuntu.com/cloud