ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική και Υπολογιστική Βιοϊατρική»

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΕΡΓΑΣΙΑ

ΤΟΥ

ΚΩΝΣΤΑΝΤΙΝΟΥ ΚΩΝΣΤΑΝΤΟΠΟΥΛΟΥ
(AM:M012016100, mail: kokonstant@uth.gr, kkonstantopoulos@outlook.com)

ΣΤΟ ΜΑΘΗΜΑ

ΝΑΥΤΙΛΙΑΚΗ ΠΛΗΡΟΦΟΡΙΚΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΡ. ΙΩΑΝΝΗΣ ΦΙΛΙΠΠΟΠΟΥΛΟΣ

ΛΑΜΙΑ, ΙΑΝΟΥΑΡΙΟΣ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Σκοπός της παρούσας εργασίας είναι να παρουσιάσει με όσο το δυνατόν απλούστερο τρόπο την σημαντικότητα της Ασφάλειας ενός Πληροφοριακού Συστήματος και κατ' επέκταση την εφαρμογή της στον ζωτικό χώρο της Ναυτιλίας.

Στο πρώτο κεφάλαιο γίνεται μια σύντομη αναφορά στις έννοιες της Ναυτιλίας και της Ναυτιλιακής Επιχείρησης.

Στο δεύτερο κεφάλαιο γίνεται ανάλυση ως προς τις έννοιες, τη δομή, τις κατηγορίες και τέλος τα πλεονεκτήματα και μειονεκτήματα ενός Πληροφοριακού Συστήματος.

Στη συνέχεια αναλύονται τα Πληροφοριακά Συστήματα στο χώρο της Ναυτιλίας, οι κατηγορίες τους και η εξέλιξή τους, καθώς και οι σύγχρονες ανάγκες μιας Ναυτιλιακής Επιχείρησης.

Τέλος στο τέταρτο κεφάλαιο αναλύεται η ασφάλεια ενός Πληροφοριακού Συστήματος, γίνεται εκτενής αναφορά στον τρόπο σχεδιασμού και υλοποίησης καθώς και στην εφαρμογή της σε μια ναυτιλιακή επιχείρηση με βάση το πρότυπο ISO 27001.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ναυτιλία, Ναυτιλιακή Επιχείρηση, Πληροφοριακό Σύστημα, Ασφάλεια, Κυβερνοαπειλή, Πρότυπα Ασφαλείας, ISO 27001.

ΚΕΦΑΛΑΙΟ 1: ΝΑΥΤΙΛΙΑ - ΝΑΥΤΙΛΙΑΚΗ ΕΠΙΧΕΙΡΗΣΗ

1.1 Ορισμός - Έννοια της Ναυτιλίας

Λέγοντας «ναυτιλιακή βιομηχανία» ή γενικότερα «ναυτιλία», εννοούμε όλες τις δραστηριότητες που συνδέονται και υποστηρίζουν τις θαλάσσιες μεταφορές ανθρώπων και αγαθών. Πρόκειται για αναπόσπαστο στοιχείο των ειρηνικών διεθνών εμπορικών συναλλαγών της ανθρωπότητας. Πλοία διαφόρων τύπων, μεταφέρουν ανθρώπους, ξηρά και υγρά φορτία συσκευασμένα ή σε χύμα μορφή, καθώς επίσης οχήματα, ζώα κ.ά. σε όλα τα πλάτη και μήκη της γης. Το σύνολο των εμπορικών πλοίων τα οποία φέρουν τη σημαία ενός κράτους αποτελούν το Εμπορικό Ναυτικό του κράτους αυτού.

Χρησιμοποιούμε τον όρο «ναυτιλία» και όταν αναφερόμαστε στην ίδια τη λειτουργία του πλοίου, που είναι η επιστήμη και η τέχνη της διακυβέρνησης (γέφυρα) και της πρόωσης (μηχανής) αλλά και της φόρτωσης του, ώστε να πλέει με ασφάλεια από ένα σημείο σε άλλο.

Η λέξη «ναυτιλία» υποδηλώνει και τη ναυτιλιακή βιομηχανία μιας χώρας που είναι το σύνολο των δραστηριοτήτων γύρω από τις θαλάσσιες μεταφορές. Και φυσικά αποκαλούμε «παγκόσμια ναυτιλία» όλες τις εθνικές βιομηχανίες οι οποίες λειτουργούν και ελέγχονται μέσω ναυτιλιακής νομοθεσίας που θεσπίζεται στο Διεθνή Ναυτιλιακό Οργανισμό (IMO - International Maritime Organization). Ο Οργανισμός είναι τεχνικός τομέας του ΟΗΕ, εδρεύει στο Λονδίνο και έχει μέλη του κράτη που ψηφίζουν Διεθνείς Συμβάσεις, Κώδικες και Κανονισμούς σε τρεις κύριους τομείς:

(α) Εκπαίδευση και Πιστοποίηση ναυτικών

(β) Ασφάλεια ανθρώπινης ζωής και Περιουσίας στη Θάλασσα (επιβαίνοντες-πλοίο-φορτίο)

(γ) Προστασία του Θαλάσσιου Περιβάλλοντος από τη ρύπανση των εμπορικών πλοίων

Τα πολεμικά πλοία δεν υπόκεινται στη ναυτιλιακή νομοθεσία. Οι θαλάσσιες μεταφορές αποτελούν αναπόσπαστο μέρος των ειρηνικών διεθνών εμπορικών συναλλαγών που είναι η ίδια η πηγή ζωής του κόσμου, όπως αναφέρει και η Ιδρυτική Διακήρυξη Εθελοντικής Δέσμευσης της HELMEPA που υπέγραψαν Έλληνες ναυτικοί και πλοιοκτήτες το 1982 στον Πειραιά.

Τα πάνω από 60.000 εμπορικά πλοία της παγκόσμιας ναυτιλίας μεταφέρουν το 99,6% των εμπορευμάτων με ασφάλεια στον προορισμό τους με πιο χαμηλό κόστος. Το εμπορικό πλοίο είναι το πλέον αποτελεσματικό, οικονομικό και περιβαλλοντικά φιλικό μέσο μεταφοράς που εξακολουθεί να διαθέτει η ανθρωπότητα.

1.2 Δομή και Περιβάλλον Λειτουργίας μιας Ναυτιλιακής Επιχείρησης

Για να επιτευχθεί ο καλύτερος δυνατός συντονισμός, οι ναυτιλιακές επιχειρήσεις είναι οργανωμένες σε διάφορα τμήματα που το καθένα έχει αναλάβει και διαφορετικό αλλά εξίσου σημαντικό έργο. Ο αριθμός και η επάνδρωση των τμημάτων εξαρτάται βεβαίως τόσο από το μέγεθος της επιχείρησης, όσο και από τις επιλογές της να αναθέτει κάποιες λειτουργίες της σε εξωτερικούς συνεργάτες (managers, πράκτορες).

<u>Στελέχη μιας ναυτιλιακής επιχείρησης</u>

Γενική Διεύθυνση (General Management)

Το κέντρο επιχειρήσεων και στρατηγικών αποφάσεων της ναυτιλιακής Εταιρείας. Δίνει κατευθύνσεις, συντονίζει και συνεργάζεται με όλα τα τμήματα της επιχείρησης. Καθορίζει τις σχέσεις της Εταιρείας με τον ευρύτερο ναυτιλιακό χώρο (κράτος σημαίας, τράπεζες, ασφαλιστικούς οργανισμούς κλπ). Έχει επικεφαλής ένα έμπειρο στέλεχος, πού μπορεί να είναι και ο ίδιος ο πλοιοκτήτης, πλαισιωμένο από επιτελείο με σφαιρική αντίληψη του ναυτιλιακού χώρου.

Τμήμα επιχειρήσεων(Operations department)

Ασχολείται με την ομαλή και αποτελεσματική λειτουργία των πλοίων της Εταιρείας σύμφωνα με τις συμβατικές τους υποχρεώσεις απέναντι στους Ναυλωτές. Η παρακολούθηση των πλοίων γίνεται με επικεφαλής ένα έμπειρο στέλεχος, κατά κανόνα Α΄ πλοίαρχο Ε.Ν.

Τεχνικό τμήμα (Technical department)

Έχει την ευθύνη της παρακολούθησης της καλής λειτουργίας και της συντήρησης των πλοίων ώστε αυτά να είναι πάντα σε πλήρη επιχειρησιακή ετοιμότητα. Πρωτοστατεί στις

ναυπηγήσεις, τους δεξαμενισμούς και τις επισκευές των πλοίων της Εταιρείας. Έχει επικεφαλής συνήθως έναν πολύ έμπειρο Ναυπηγό ή Α΄ μηχανικό Ε.Ν., τον Αρχιμηχανικό και στελεχώνεται από ναυπηγούς, τεχνικούς και μηχανικούς Ε.Ν. διαφόρων ειδικοτήτων.

Τμήμα ναυλώσεων (Chartering and brokering department)

Ασχολείται με την αναζήτηση ναύλων για τα πλοία από τη διεθνή ναυλαγορά. Στελεχώνεται από στελέχη εξειδικευμένα σε θέματα ναυλώσεων που περιλαμβάνουν και πλοιάρχους Ε.Ν.. Υπάρχουν όμως και μεγάλα ναυτικά γραφεία, που ασχολούνται αποκλειστικά με τις ναυλώσεις πλοίων διαφόρων εταιρειών, τα αποκαλούμενα ναυλομεσιτικά γραφεία. Πολλές ναυτιλιακές εταιρείες συνεργάζονται με αυτά.

Τμήμα Ποιότητας και Ασφαλείας (Quality and Safety department)

Το τμήμα αυτό καθιερώθηκε από τα μέσα της δεκαετίας του ’90, προκειμένου να τηρούνται οι κανόνες ποιότητας και οι διαδικασίες πού ορίζει ο Διεθνής Κώδικας Ασφαλούς Διαχειρίσεως (ISM Code) του Διεθνούς Ναυτιλιακού Οργανισμού (IMO). Στελεχώνεται κυρίως από άτομα με γνώσεις από όλες τις δραστηριότητες της Εταιρείας, συμπεριλαμβανομένων και έμπειρων πλοιάρχων και μηχανικών Ε.Ν.

Τμήμα ασφαλίσεων (Insurance and claims department)

Ασχολείται με την ασφαλιστική κάλυψη κάθε πλοίου και των επιβαινόντων σε αυτό καθώς και με τη διεκπεραίωση όλων των υποθέσεων που έχουν σχέση με την ασφάλιση (διεκδικήσεις από και προς τρίτα μέρη). Στελεχώνεται από νομικούς εξειδικευμένους σε θέματα ναυτικού δικαίου και ναυτασφαλίσεων καθώς και από πλοιάρχους Ε.Ν.

Νομικό Τμήμα (Legal department)

Συναντάται κυρίως στις μεγάλες ναυτιλιακές επιχειρήσεις και στελεχώνεται από δικηγόρους εξειδικευμένους σε θέματα ναυτικού δικαίου.

Τμήμα προμηθειών (Purchasing department)

Έχει την ευθύνη του εφοδιασμού των πλοίων με τρόφιμα και κάθε είδους αναλώσιμα υλικά καθώς και ανταλλακτικά. Στελεχώνεται συνήθως από πλοίαρχο ή μηχανικό Ε.Ν. καθώς και από στελέχη έμπειρα στο χώρο των προμηθειών ναυτικών και άλλων υλικών.

Τμήμα πληρωμάτων (Crew management ή Marine department)

Έχει τη σημαντική ευθύνη της επιλογής αξιωματικών και πληρωμάτων για την επάνδρωση των πλοίων. Έχει επικεφαλής σχεδόν πάντα ένα πλοίαρχο Ε.Ν. κατά κανόνα παλαιό στέλεχος της εταιρείας, με εμπειρία στη διαχείριση ανθρώπινου δυναμικού, τον Αρχικαπετάνιο της Εταιρείας, όπως κοινώς αποκαλείται.

Τμήμα γραμματείας - λογιστηρίου

Ασχολείται με τη διεκπεραίωση της αλληλογραφίας και της επικοινωνίας της εταιρείας με τα πλοία και με άλλους οργανισμούς και εταιρείες.

Το λογιστήριο ασχολείται με οικονομικές δραστηριότητες που αφορούν την εταιρεία, τα γραφεία της και τα πλοία με τα πληρώματά τους.

ΚΕΦΑΛΑΙΟ 2: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ (Π/Σ)

2.1 Ορισμός

Ως πληροφοριακό σύστημα (Information Systems - IS), ορίζεται ένα σύνολο από διαδικασίες, οι οποίες αποσκοπούν στις εξής ενέργειες: συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση των πληροφοριών. Οι διαδικασίες αυτές, δεν είναι μονοσήμαντες, αλλά αναφέρονται τόσο στο ανθρώπινο δυναμικό, όσο και στην εφαρμογή των υπολογιστικών συστημάτων. Τα συστήματα αυτά περιλαμβάνουν λογισμικό και υλικό μέρος, ενώ πολλές φορές υποστηρίζουν και το τηλεπικοινωνιακό σκέλος. Τα τελευταία χρόνια, ο τομέας των τεχνολογιών και της πληροφορικής έχει σημειώσει πολύ μεγάλη πρόοδο, με αποτέλεσμα, ο εργασιακός τομέας και οι εργασίες που πραγματοποιούνται από το ανθρώπινο δυναμικό, να είναι στην πλειοψηφία τους αυτοματοποιημένες. Η αυτοματοποίηση της παραγωγής καθορίζεται λοιπόν σε μεγάλο βαθμό από την ανάπτυξη όχι μόνο της τεχνολογίας, αλλά και των πληροφοριακών συστημάτων.

Τα πληροφοριακά συστήματα, αποτελούν ένα εργαλείο που χρησιμοποιείται σήμερα σχεδόν από κάθε επιχείρηση ή οργανισμό. Για να φτάσουν στο σημείο οι επιχειρήσεις να θεωρούν απαραίτητη την εφαρμογή πληροφοριακών συστημάτων, διαπιστώνεται ότι ο ανταγωνισμός μεταξύ αυτών είναι πολύ μεγάλος. Προκειμένου οι επιχειρήσεις να επιβιώσουν μέσα σε ένα έντονα ανταγωνιστικό περιβάλλον θα πρέπει να προβούν σε ενέργειες για τον σχεδιασμό και την εφαρμογή ενός άρτια εξοπλισμένου πληροφοριακού συστήματος.

Τα πληροφοριακά συστήματα αποτελούν το μέσο για την αρμονική συνεργασία ανθρώπινου δυναμικού, δεδομένων, διαδικασιών και τεχνολογιών πληροφορίας και επικοινωνιών. Σήμερα τα πληροφοριακά συστήματα διδάσκονται ως ειδίκευση τόσο σε προπτυχιακό όσο και μεταπτυχιακό επίπεδο.

Ένα καλά σχεδιασμένο πληροφοριακό σύστημα, το οποίο θα εφαρμοστεί με τον βέλτιστο δυνατό τρόπο και θα υποστηρίξει στο άρτιο τις λειτουργίες κάθε επιχείρησης, θα πρέπει να παρέχει και τις ακόλουθες προϋποθέσεις:

- ύπαρξη καλά ορισμένων διαδικασιών
- σωστός προσδιορισμός των αναγκαίων δεδομένων
- κατάλληλη κατάρτιση του ανθρώπινου δυναμικού
- ύπαρξη κατάλληλου υλικού
- διαθεσιμότητα κατάλληλου λογισμικού.

2.2 Πληροφοριακά Συστήματα βασισμένα σε Η/Υ

Η εισαγωγή των Η/Υ στα πληροφοριακά συστήματα έγινε στα μέσα της δεκαετίας του 1950 και έκτοτε, επεκτάθηκε με ιλιγγιώδεις ρυθμούς. Αυτό είχε σαν αποτέλεσμα τη δημιουργία συστημάτων ικανών να επεξεργάζονται τεράστιο όγκο δεδομένων. Τα μηχανογραφημένα πληροφοριακά συστήματα που χρησιμοποιούν σήμερα οι επιχειρήσεις θεωρούνται πιο αξιόπιστα αφού οι λειτουργίες τους εκτελούνται μέσω Η/Υ. Με τον όρο "Μηχανογραφημένο Πληροφοριακό Σύστημα" δεν εννοούμε πλήρη αυτοματοποίηση του κύκλου εργασιών. Όπως προκύπτει από τον ορισμό του πληροφοριακού συστήματος, ένα πληροφοριακό σύστημα αποτελείται από μηχανήματα, ανθρώπους, προγράμματα και διαδικασίες. Έτσι ενώ ορισμένες εργασίες εκτελούνται από το μηχάνημα, υπάρχουν και κάποιες που εκτελούνται από τον άνθρωπο με βάση βέβαια συγκεκριμένες οδηγίες. Δεν θα πρέπει να ξεχνάμε ότι ο ανθρώπινος νους αποτελεί την κύρια μορφή επεξεργασίας δεδομένων των χειρόγραφων πληροφοριακών συστημάτων, τα οποία παρά την ιλιγγιώδη ανάπτυξη των μηχανογραφημένων υπερτερούν έναντι αυτών κυρίως στην κριτική ικανότητα. Ειδικότερα στις περιπτώσεις εκείνες των αποφάσεων που απαιτείται κρίση, το ανθρώπινο μυαλό είναι αναντικατάστατο.

2.3 Δομή ενός Πληροφοριακού Συστήματος

2.3.1 Οι άνθρωποι

Η επιτυχημένη ή όχι εφαρμογή και λειτουργία ενός πληροφοριακού συστήματος, εξαρτάται κατά κύριο λόγο από τον ανθρώπινο παράγοντα. Κάτι τέτοιο είναι σαφές από το γεγονός ότι, οι άνθρωποι- χρήστες, είναι αυτοί που θα θέσουν σε λειτουργία το πληροφοριακό σύστημα και θα συνεχίσουν την απρόσκοπτη λειτουργία του.

Σημειώνεται ότι, το ανθρώπινο δυναμικό που περιγράφεται ως καθοριστικός παράγοντας της λειτουργίας ενός πληροφοριακού συστήματος, είναι το σύνολο του εργατικού δυναμικού που έχει στην διάθεσή της κάθε επιχείρηση. Για παράδειγμα, το σύνολο των ανθρώπων που μπορεί να συμβάλλουν στις καθημερινές λειτουργίες μιας επιχείρησης, μπορεί να είναι: οι χρήστες, οι διαχειριστές, οι υπεύθυνοι λειτουργίας, οι προϊστάμενοι, άλλοι υπάλληλοι, κλπ.

Συνοψίζοντας, η καλή συνεργασία ανθρώπου και υπολογιστικού συστήματος προσδιορίζει την αποτελεσματικότητα της λειτουργίας μιας επιχείρησης που χρησιμοποιεί τα πληροφοριακά συστήματα.

2.3.2 Οι διαδικασίες

Οι διαδικασίες αποτελούν το σύνολο των εντολών και οδηγιών που δίνονται από την διοίκηση μίας επιχείρησης, στο ανθρώπινο δυναμικό, το οποίο επεμβαίνει με οποιοδήποτε τρόπο στην εφαρμογή και την λειτουργία του πληροφοριακού συστήματος.

Θα πρέπει να σημειωθεί ότι, ο βαθμός πολυπλοκότητας των διαδικασιών μεταβάλλεται ανάλογα με το είδος του συστήματος.

2.3.3 Τα δεδομένα (Data)

Οι βάσεις δεδομένων αποτελούν έναν ακόμη βασικό παράγοντα στον οποίο στηρίζεται η αποτελεσματική λειτουργία του πληροφοριακού συστήματος. Στην ουσία, μία βάση δεδομένων είναι μία οργανωμένη συλλογή από συσχετιζόμενα δεδομένα που χρησιμοποιούνται από όλες τις εφαρμογές του οργανισμού ή της επιχείρησης.

Με την χρησιμοποίηση των βάσεων δεδομένων, μία επιχείρηση είναι σε θέση να διασφαλίσει έναν καθολικό τρόπο αποθήκευσης των δεδομένων της. Τα δεδομένα που αποθηκεύονται σε μια βάση δεδομένων, καταμερίζονται με τέτοιο τρόπο, ώστε να είναι προσπελάσιμα από διάφορους χρήστες και για διάφορες εφαρμογές.

Όσον αφορά τα πλεονεκτήματα, που παρέχονται από την χρησιμοποίηση μιας βάσης δεδομένων από μία επιχείρηση, το κυριότερο είναι ότι, ο χώρος αποθήκευσης στο δίσκο καθώς ο χρόνος για ενημέρωση των δεδομένων μειώνονται σημαντικά.

2.3.4 Το λογισμικό (Software)

Το λογισμικό είναι το σύνολο των εντολών που ρυθμίζουν την λειτουργία ενός υπολογιστικού συστήματος και καθοδηγούν τον υπολογιστή να εκτελέσει διάφορες διεργασίες. Αποτελεί δηλαδή ένα σύνολο προγραμμάτων και διαδικασιών που συμβάλλουν στην λειτουργία του πληροφοριακού συστήματος.

2.3.5 Το υλικό (Hardware)

Ο υλικός εξοπλισμός, περιλαμβάνει τα είδη των πληροφοριακών συστημάτων που μπορούν να δημιουργηθούν για την κάλυψη των λειτουργιών κάθε επιχείρησης και ανήκει συνήθως σε μια από τις ακόλουθες κατηγορίες:

- SCMS: Συστήματα Διαχείρισης Αλυσίδας Εφοδιασμού
- DSS: Συστήματα Υποστήριξης Απόφασης
- OAS: Συστήματα Αυτοματοποίησης Γραφείου
- TPS: Συστήματα Επεξεργασίας Συναλλαγών
- ERP: Συστήματα Ενδο-επιχειρησιακού Σχεδιασμού
- ESS: Συστήματα υποστήριξης Διοίκησης
- KMS: Συστήματα Διαχείρισης Γνώσης
- MIS: Διοικητικά Συστήματα Πληροφόρησης.

2.3.6 Το Δίκτυο (Network)

Ως δίκτυο ορίζεται ένα σύνολο από αυτόνομους ή μη διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν υπάρχει η δυνατότητα κάποιος υπολογιστής να ελέγξει τη λειτουργία κάποιου άλλου.

2.4 Κατηγορίες Πληροφοριακών Συστημάτων

Τα πληροφορικά συστήματα κατατάσσονται στις ακόλουθες κατηγορίες, ανάλογα με τα επίπεδα οργάνωσης μιας επιχείρησης ή ενός οργανισμού που καλύπτουν:

Συστήματα Λειτουργικού Επιπέδου: τα συγκεκριμένα πληροφοριακά συστήματα, είναι σχεδιασμένα για τα στελέχη μίας επιχείρησης ή ενός οργανισμού και συμβάλλουν στην παρακολούθηση του συνόλου των δραστηριοτήτων που εκτελούνται σε καθημερινή βάση. Ορισμένες από τις δραστηριότητες που

παρακολουθούνται μέσω των συστημάτων λειτουργικού επιπέδου είναι, οι πωλήσεις, οι εισπράξεις, οι καταθέσεις, η μισθοδοσία, οι πιστωτικές αποφάσεις , η ροή των υλικών σε ένα εργοστασιακό χώρο, κ.λπ. Με την ανάπτυξη συστημάτων λειτουργικού επιπέδου, επιδιώκεται από την διοίκηση της επιχείρησης να αντλούνται πληροφορίες που θα απαντούν σε τρέχουσες ερωτήσεις και θα παρακολουθούν τη ροή των συναλλαγών του οργανισμού.

Συστήματα Επιπέδου Γνώσης: τα συστήματα επιπέδου γνώσης, σχεδιάζονται προς το εξειδικευμένο προσωπικό μίας επιχείρησης ή ενός οργανισμού. Ο λόγος κατασκευής των συγκεκριμένων πληροφοριακών συστημάτων είναι ότι, συμβάλλουν στην αφομοίωση νέας επιχειρηματικής γνώσης και τον έλεγχο της γραφειοκρατίας, προς όφελος της επιχείρησης.

Συστήματα Διοικητικού Επιπέδου: τα συγκεκριμένα συστήματα εξυπηρετούν την παρακολούθηση, τον έλεγχο, την λήψη αποφάσεων και τις διοικητικές δραστηριότητες των μεσαίων στελεχών. Επιπλέον, τα συστήματα διοικητικού επιπέδου, εκδίδουν περιοδικές αναφορές και όχι άμεσες λειτουργικές πληροφορίες.

Συστήματα Στρατηγικού Επιπέδου: τα συστήματα στρατηγικού επιπέδου χρησιμοποιούνται από τα ανώτερα στελέχη μίας επιχείρησης και δίνουν σε αυτούς την δυνατότητα να παρακολουθήσουν και να αντιμετωπίσουν στρατηγικά ζητήματα και τάσεις, τόσο μέσα στην επιχείρηση όσο και στο εξωτερικό περιβάλλον της.

2.5 Πλεονεκτήματα - Μειονεκτήματα Πληροφοριακών Συστημάτων

Ο σχεδιασμός, η ανάπτυξη και η υλοποίηση των πληροφοριακών συστημάτων παρουσιάζει αρκετά πλεονεκτήματα. Ωστόσο, πέρα από τις θετικές επιπτώσεις που αυτά φέρουν, διαπιστώνονται και ορισμένα μειονεκτήματα.

Ένα πρώτο πλεονέκτημα των πληροφοριακών συστημάτων είναι ότι, έχουν βοηθήσει πολύ τον άνθρωπο να εξελιχθεί στον εργασιακό του χώρο και να απλοποιήσει τις καθημερινές του διαδικασίες. Πιο συγκεκριμένα, η εφαρμογή πληροφοριακών συστημάτων σε μία επιχείρηση, δίνει την δυνατότητα σε αυτή να λάβει πληροφορίες για ενδεχόμενες ελλείψεις και να προβεί στις απαραίτητες ενέργειες, να μετρήσει τις προμήθειες που έχει στην αποθήκη τους, κ.λπ. Επιπλέον, μέσω των πληροφοριακών συστημάτων, οι έλεγχοι που πραγματοποιούνται είναι ταχύτατοι και ακριβείς, ενώ παράλληλα, το κόστος είναι πολύ μικρότερο σε σύγκριση με τον παραδοσιακό τρόπο εργασίας. Επιπρόσθετα, οι επιχειρήσεις ενημερώνονται σε έγκαιρο χρόνο για τις αλλαγές που πρέπει να κάνουν ή να εφαρμόσουν μέσω των πληροφοριακών συστημάτων. Η διαχείριση των παραστατικών, της αποθήκης, της διοίκησης της παραγωγής, τα τιμολόγια είναι μια διαδικασία που στηρίζεται αποκλειστικά στα πληροφοριακά συστήματα.

Από την άλλη πλευρά, οι αρνητικές επιπτώσεις από τον σχεδιασμό των πληροφοριακών συστημάτων, περιγράφονται ως εξής: Όταν ένα πληροφοριακό σύστημα χρησιμοποιείται σε περιβάλλον με πολλούς χρήστες, η επίδοσή του μειώνεται αισθητά. Επίσης η δημιουργία των πληροφοριακών συστημάτων έχει επιφέρει και κάποιες αρνητικές επιπτώσεις στον ανθρώπινο παράγοντα. Μία από αυτές είναι ότι εκλείπουν πολλά παραδοσιακά επαγγέλματα εξαιτίας της αδυναμίας τους να ακολουθήσουν την αλματώδη τεχνολογική εξέλιξη και κατ' επέκταση την εφαρμογή νέων τεχνολογιών. Αυτό έχει σαν αποτέλεσμα την συνεχή αύξηση των ποσοστών ανεργίας. Επίσης, διακρίνονται δυσκολίες στην κοινωνικοποίηση των ατόμων στις σύγχρονες κοινωνίες, καθώς με την χρήση των υπολογιστικών συστημάτων απομονώνονται από τον κοινωνικό περίγυρο. Τέλος, σημειώνεται ότι, ορισμένα πληροφοριακά συστήματα είναι δύσκολο να εφαρμοστούν στην πράξη, ενώ ενδεχόμενη διακοπή της λειτουργίας τους, μπορεί να παύσει σημαντικές δραστηριότητες και να παραλύσει ολόκληρες κοινότητες.

ΚΕΦΑΛΑΙΟ 3: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΝΑΥΤΙΛΙΑ

3.1 Ιστορική αναδρομή - Εξέλιξη

Πριν διακόσια χρόνια οι πληροφορίες για τις ναυτιλιακές υπηρεσίες μέχρι την επιστροφή του πλοίου ήταν ελάχιστες, καθώς το μοναδικό μέσω επικοινωνίας ήταν η δια χειρός αλληλογραφία. Τα πλοία βασιζόταν στους αξιωματούχους επόπτες εργασίας, που έλεγχαν τα τις εργασίες και κανόνιζαν τον αναλογούν ναύλο. Οι πλοιοκτήτες χειριζόταν τα ζητήματα, που αφορούσαν το πλοίο, όσο εκείνο ήταν μακριά χωρίς να υπάρχει γνώση για το πότε και εάν θα επιστρέψει.

Τον 18ο αιώνα δημιουργήθηκαν Προσωπικά Ναυτιλιακά Δίκτυα. Ένα δίκτυο πληροφοριών διαμορφώθηκε με κύρια σημεία αναφοράς τα καφενεία. Κατά την διάρκεια του αιώνα τα καφενεία έγιναν πόλοι έλξης για όσους σχετίζονταν με την ναυτιλία (π.χ. πλοιοκτήτες, αξιωματούχοι κ.α.) με αποτέλεσμα να πάρουν μια μορφή «κέντρου πληροφοριών» για κάθε λιμάνι.

Η εξάπλωση των ευρωπαϊκών αυτοκρατοριών και η ταχύτατη ανάπτυξη του εμπορίου αποτέλεσε μεγάλη ανάγκη η βελτίωση της επικοινωνίας με Αμερική και Ινδία. Οι πρώτες προσπάθειες ξεκίνησαν το 1841 με τεράστιες επενδύσεις. Από το 1841 έως το 1897 μεσολάβησαν πολλές αποτυχημένες προσπάθειες. Το 1987 162,000 ναυτικά μίλια καλωδίων εγκαταστάθηκαν, ορίζοντας την Ναυτιλία στην παγκόσμια αγορά και η άμεση επικοινωνία για πρώτη φορά ήταν εφικτή.

Τα πληροφοριακά συστήματα πρωτοεμφανίστηκαν στον Β΄ Παγκόσμιο πόλεμο, με την ραγδαία και αναγκαία ανάπτυξη τους, μηχανικά αλλά και ηλεκτρονικά. Οι εφαρμογές των πληροφοριακών συστημάτων στις επιχειρηματικές δραστηριότητες άρχισαν στις αρχές της δεκαετίας του 1950. Οι υπολογιστές χρησιμοποιούνταν για μεγάλο όγκο επαναλαμβανόμενων συναλλακτικών εργασιών. Οργάνωναν επί της ουσίας τα αριθμητικά δεδομένα στους τομείς του λογιστηρίου, της χρηματοδότησης και της διαχείρισης ανθρώπινων πόρων που στην πορεία ονομάστηκαν Συστήματα Επεξεργασίας Συναλλαγών (TPS - Transaction Processing Systems). Μέχρι το 1960 οι διαχειριστές αντάλλασαν πληροφορίες με το τηλέγραφο ή το τηλέφωνο αυξάνοντας το λειτουργικό κόστος και παράλληλα η ταχύτητα του μηνύματος δεν ήταν ιδιαίτερα μεγάλη. Μετά τον 2ο Παγκόσμιο Πόλεμο μειώθηκε το κόστος επικοινωνίας και αυξήθηκαν οι ταχύτητες ανταλλαγής πληροφοριών καθώς εισήλθαν ο τηλέγραφος, το telex, οι άμεσες τηλεφωνικές συνδιαλέξεις και το φαξ.

Η δεκαετία του ΄60 αποτέλεσε σταθμό για τα πληροφοριακά δίκτυα, με τους ηλεκτρονικούς υπολογιστές να ξεκινούν μια επανάσταση στην αποθήκευση, διαχείριση και πρόσβαση της πληροφορίας. Με τη χρήση Η/Υ ξεκινά τόσο η αυτοματοποίηση των συστημάτων πληροφόρησης όσο και η παροχή online πληροφοριών.

Το 1970 η ζήτηση για πληροφοριακά συστήματα μεγάλωνε καθώς επικρατούσε όλο και περισσότερο η ηλεκτρονική επικοινωνία και ο υπολογισμός μέσω δικτύων σε επιχειρήσεις και βιομηχανίες. Αυτό ήταν αφορμή για την εμφάνιση συστημάτων αυτοματισμού γραφείου, επεξεργασίας κειμένων καθώς και σχεδίασης και παροχής βοήθειας Η/Υ. Οι δυνατότητες των Η/Υ αυξάνονταν και το κόστος όλο ένα και μειωνόταν με αποτέλεσμα την εξάπλωσή του και σε άλλους τομείς.

Η μηχανογραφημένη υποστήριξη στην λήξη αποφάσεων ήταν πραγματικότητα με τα Συστήματα Υποστήριξη Λήξης Αποφάσεων (DSS – Decision Support Systems). Το κόστος των DSS μειωνόταν αλλά δεν ήταν ικανοποιητικά, για την εποχή παράμενε μεγάλο. Η εμφάνιση των μικροϋπολογιστών την δεκαετία του 1980 άλλαξε τα δεδομένα. Το κόστος μειώθηκε κι άλλο με τους υπολογιστές γραφείου. Η εξέλιξη όμως των DSS έφερε σαν αποτέλεσμα την διάσπασή τους στις εξής δυο κατευθύνσεις:

- Συστήματα Υποστήριξης Ομάδων (GSS – Group Support Systems)
- Εταιρικά Πληροφοριακά Συστήματα (EIS – Enterprise Information Systems).

Στα μέσα της δεκαετίας του 1980 ξεκίνησε η χρήση προγραμμάτων, από επιχειρήσεις, που ήταν σε θέση να εκτελέσουν πράξεις συμβολικής λογικής για την επίλυση προβλημάτων και ονομάστηκαν προγράμματα Τεχνητής Νοημοσύνης (AI – Artificial Intelligence). Η εφαρμογή των προγραμμάτων AI οδήγησαν στην ανάπτυξη των Έμπειρων Συστημάτων (ES –Expert Systems). Τα ES ήταν συστήματα που μπορούσαν να προσφέρουν την τεχνογνωσία εμπειρογνωμόνων στους τελικούς

χρήστες με αποτέλεσμα αυτοί να μπορούν να λύσουν πολύπλοκα προβλήματα.

Τη δεκαετία του ΄90 με το διαδίκτυο (World Wide Web), ως οικονομικό, εύκολο και ταχύτατο τρόπο επικοινωνίας, δόθηκε η δυνατότητα δωρεάν πρόσβασης σε μεγάλες διαδικτυακές βάσεις δεδομένων. Η Ηλεκτρονική Μετάδοση Πληροφοριών (Electronical Data Interchange) ορίστηκε ως η ηλεκτρονική μεταφορά κωδικοποιημένων εμπορικών πληροφοριών και τυποποιημένων μηνυμάτων, χρησιμοποιώντας συμφωνημένους κανόνες. Οι μεταδόσεις πραγματοποιούνταν από ένα σύστημα ηλεκτρονικών υπολογιστών σε ένα άλλο με ηλεκτρονικά μέσα. Πλέον ως απαραίτητο εργαλείο, για τους επαγγελματίες στο χώρο της ναυτιλίας, που παρείχε την δυνατότητα καταχώρησης στοιχείων και πληροφοριών στον Η/Υ και διάθεση αυτών σε οποιονδήποτε χρήστη για να τα επεξεργαστεί ή να τα συμπληρώσει. Σημαντικό πλεονέκτημα για τους πλοιοκτήτες ήταν η μείωση και αποφυγή σε λειτουργικά κόστη όπως αυτό της γραφειοκρατίας.

Από το 2000 τα πληροφοριακά συστήματα πέρασαν στο επίπεδο του διαδικτύου με την ολοκληρωμένη πληροφοριακή πλατφόρμα (IP- Informative Platform). Πλέον ο χώρος που δραστηριοποιούνται τα συστήματα είναι το διαδίκτυο και η εξάπλωση ήταν ραγδαία σε όλους τους τομείς.

3.2 Προβλήματα στην υλοποίηση

Η ανάπτυξη ενός ΠΣ ανεξάρτητα από το μέγεθος και την πολυπλοκότητά του είναι ένα έργο δύσκολο. Τα συνήθη προβλήματα που έχουν διαπιστωθεί κατά καιρούς είναι τα εξής:

- Αναπτύσσονται σύνθετα συστήματα που δεν βοηθούν λόγω της πολυπλοκότητάς τους.
- Οι απαιτήσεις του χρήστη είναι σε κάποιες περιπτώσεις δύσκολο να καθοριστούν πλήρως στη σχεδίαση του συστήματος.
- Η αναβάθμιση και η ανάπτυξη του λογισμικού απαιτεί μεγάλη προσοχή και λεπτομερή σχεδίαση, γιατί οι οποιεσδήποτε μελλοντικές τροποποιήσεις είναι αρκετά δύσκολο να υλοποιηθούν και σε περιπτώσεις που πραγματοποιούνται το κόστος είναι υψηλό.

3.3 Σύγχρονες ανάγκες των Ναυτιλιακών Επιχειρήσεων

Ένας από τους πλέον βασικούς άξονες στους οποίους κινούνται οι ναυτιλιακές επιχειρήσεις και κατ' επέκταση η βιομηχανία της ναυτιλίας στο σύνολό της, είναι η γρήγορη, χωρίς προβλήματα και μεταβολές πληροφόρηση και επικοινωνία. Τόσο ο όγκος, όσο και ο ρυθμός μετάδοσης της πληροφορίας που απαιτείται σε καθημερινή βάση, είναι τεράστιος και εξακολουθεί να αυξάνεται εκθετικά. Αυτό το γεγονός καθιστά απαραίτητη τη χρήση προηγμένων μηχανογραφικών Πληροφοριακών Συστημάτων, ικανών να ανταπεξέλθουν στις σύγχρονες ανάγκες και απαιτήσεις.

3.4 Μηχανογραφημένα Π/Σ στη Ναυτιλία

Τα πιο σημαντικά Πληροφοριακά Συστήματα που χρησιμοποιούνται στο χώρο της Ναυτιλιακής Βιομηχανίας είναι τα εξής:

Γεωγραφικά Πληροφοριακά Συστήματα (GIS)

Ένα Γεωγραφικό Πληροφοριακό Σύστημα έχει την δυνατότητα να συλλέξει, να αποθηκεύσει, να διαχειριστεί, να επεξεργαστεί, να αναλύσει και να φέρει σε μορφή εικόνας σε ψηφιακό περιβάλλον τα δεδομένα του γεωγραφικού χώρου που ενδιαφέρουν την επιχείρηση ή τον οργανισμό.

Στο επίπεδο των ναυτιλιακών, καθώς και των οργανισμών λιμένων κάθε πλοίο έχει ένα συγκεκριμένο κωδικό και σε τακτά χρονικά διαστήματα εντοπίζεται η γεωγραφική θέση του. Οι πληροφορίες που λαμβάνονται δηλαδή ο κωδικός, ο χρόνος και η γεωγραφική θέση δημιουργούν μια βάση δεδομένων. Με τα τρία αυτά στοιχεία παράγονται πληροφορίες χρήσιμες για σχεδιασμό – προγραμματισμό, την επίλυση προβλημάτων και σαφώς την λήψη αποφάσεων. Τα δεδομένα αυτά αντλούνται από το διαδίκτυο, από κυβερνητικούς οργανισμούς, από ιδιωτικές έρευνες ή από την ίδια την επιχείρηση. Η δημιουργία τους βασίζεται στην τεχνολογία των Συστημάτων Δορυφορικού Εντοπισμού (Global Positioning System – GPS) και των συστημάτων αναγνώρισης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification – RFID).

Το GPS είναι ένα σύστημα, ασύρματο, που με την χρήση δορυφόρων δίνει την δυνατότητα στον χρήστη κάθε στιγμή να

γνωρίζει την θέση του. Οι κύριοι τομείς εφαρμογής του είναι η ναυτιλία και η αεροναυτιλία. Η αξιοπιστία του αυξάνεται συνεχώς καθώς παρατηρείται η εμφάνισή του ως εφαρμογή ακόμα και σε απλές συσκευές κινητής τηλεφωνίας. Αυτή η εξέλιξη και παράλληλα η χρήση του σε συσκευές καθημερινής χρήσης είχε σαν αποτέλεσμα και την μείωση του κόστους. Η εξέλιξη των συστημάτων GPS και GIS είχαν σαν αποτέλεσμα την συνεργασία τους και την δημιουργία συστημάτων σε διάφορους τομείς. Στον τομέα της ναυτιλίας έχει εδραιωθεί η χρήση του για την εύρεση και χάραξη πορείας των πλοίων. Αυτό έδωσε την δυνατότητα, στα πλοία και στις ναυτιλιακές, υπάρχει περισσότερη ασφάλεια στα ταξίδια των πλοίων και παράλληλα την μείωση του χρόνου και του κόστους της διαδρομής. Τον παραπάνω συνδυασμό ακολούθησε και η άντληση δεδομένων από μετεωρολογικούς σταθμούς και η δημιουργία μετεωρολογικών χαρτών. Ο συνδυασμός άντλησης δεδομένων από το GPS και από τους μετεωρολογικούς χάρτες κάνει τις πορείες των πλοίων πιο ασφαλείς ειδικά σε δυσμενείς καιρικές συνθήκες.

Οι πληροφορίες που αντλούνται από τους παραπάνω συνδυασμούς δίνουν συνεχή και ακριβή εικόνα σε μία ναυτιλιακή για τη θέση, την κατάσταση και για την ταχύτητα του πλοίου. Τα δεδομένα απεικονίζονται με ειδικά προγράμματα ώστε να είναι εύκολο για τον χρήστη να αντλήσει πληροφορίες. Τα παραπάνω δεδομένα μπορεί να τα λάβει υπόψη η ναυτιλιακή εταιρία που θα το εγκαταστήσει και συνδυάζοντας τις πληροφορίες να βγάλει κρίσιμα συμπεράσματα και να προχωρήσει στη λήψη αποφάσεων.

Πληροφοριακά Συστήματα Διαχείρισης Κυκλοφορίας Σκαφών (VTMIS)

Το πληροφοριακό σύστημα διαχείρισης κυκλοφορίας σκαφών (Vessel Traffic Management and Information Systems – VTMIS) χρησιμοποιείται από τους χρήστες για να έχουν απεικόνιση των κινήσεων και των αλληλεπιδράσεων του πλοίου σε πραγματικό χρόνο. Το VTMIS μπορεί και ενσωματώνει ποικίλα συστήματα πληροφοριών και τηλεματικής, που έχουν δημιουργηθεί για να ενισχύσουν την ασφάλεια και την αποτελεσματικότητα της θαλάσσιας κυκλοφορίας. Χρησιμοποιείται πλέον σε όλους τους εμπορικούς δρόμους και λιμένες της υφηλίου και η συμβολή του είναι πολύ σημαντική στην ασφάλεια της ναυσιπλοΐας και στην προστασία του περιβάλλοντος. Το Πληροφοριακό Σύστημα Διαχείρισης Κυκλοφορίας Πλοίων συγκεντρώνει, αξιολογεί και διανέμει τα δεδομένα των πλοίων σχετικά με την κυκλοφορία και τις μεταφορές τους στοχεύοντας στη βελτίωση της ασφάλειας και αποδοτικότητας της ναυτιλίας και στην προστασία του περιβάλλοντος. Το σύστημα VTMIS συνεργάζεται βασικά με τις VTS που καλύπτουν υπηρεσίες σχετικές με:

- Πληροφορίες
- Ναυτιλιακή Βοήθεια, περιλαμβανομένης και της παράκτιας ναυσιπλοΐας
- Οργάνωση και διαχείριση κυκλοφορίας
- Συνεργασία με τις σχετικές υπηρεσίες (λιμενικές, υπηρεσίες επειγόντων και παρακείμενες VTS)
- Υπηρεσίες μεταφορών

Το σύστημα VTMIS εποπτεύει και διαχειρίζεται σε πραγματικό χρόνο τη θαλάσσια κυκλοφορία, παρέχοντας τη δυνατότητα άμεσης επικοινωνίας και αλληλεπίδρασης με τα πλοία, ενώ είναι σε θέση να δίνει λύσεις στα προβλήματα ασφάλειας που δημιουργούνται στην περιοχή ευθύνης του. Οι πληροφορίες συλλέγονται από τα κατά τόπους κέντρα VTS, επεξεργάζονται κεντρικά και διανέμονται στους ενδιαφερόμενους σε τοπικό, εθνικό και διεθνές επίπεδο.

Συστήματα σχεδιασμού επιχειρηματικών πόρων (ERP)

Τα ERP είναι πακέτα λογισμικού που ενσωματώνουν όλες τις εσωτερικές διαδικασίες μιας επιχείρησης σε μία ενιαία διαχειριστική πλατφόρμα. Η πλατφόρμα αυτή είναι ευέλικτη ως προς κάθε εταιρία, με τις εσωτερικές διαδικασίες να μεταβάλλονται, να αφαιρούνται ή να προστίθενται άλλες, ανάλογα το αντικείμενο της εταιρίας. Ο κύριος σκοπός των ERP είναι η ενοποίηση όλων των τμημάτων και των λειτουργιών ολόκληρης της εταιρίας σε ένα ψηφιακό σύστημα που να εξυπηρετεί τις ανάγκες όλων των τμημάτων. Τα πλεονεκτήματα σε μία σωστή εφαρμογή ενός συστήματος ERP είναι πάρα πολλά, καθώς προσφέρει ευελιξία, ως προς την προσαρμογή του, στις οργανωτικές δομές της επιχείρησης. Το ERP έχει δυνατότητα να παρέχει πληροφορίες σε όποιο τμήμα της επιχείρησης τις χρειάζεται σε επίπεδο επιχειρηματικό, εθνικό αλλά και παγκόσμιο. Δίνει επιπλέον την δυνατότητα στους χρήστες του να επιλέγουν μεταξύ πολλών και διαφορετικών πληροφοριακών εφαρμογών, ενώ παράλληλα

είναι συμβατό με πλατφόρμες διαφορετικού επιπέδου πληροφοριακού εξοπλισμού.

Συστήματα επικοινωνίας και πληροφόρησης

Κατά τη διάρκεια του εικοστού αιώνα η τηλεπικοινωνία στην θάλασσα έχει υποστεί ριζικές αλλαγές, με την βοήθεια της ηλεκτρονικής επικοινωνίας. Μετά την χρήση των ραδιοφώνων και των ραδιοτηλεγραφημάτων, η επικοινωνία έγινε αυτοματοποιημένη και δεν χρειαζόταν προσωπικό να είναι σε συνεχή παρακολούθηση. Ο κώδικας Μορς χρησιμοποιήθηκε από την ραδιοτηλεγραφία για την θαλάσσια επικοινωνία στις αρχές του 20ου αιώνα. Η επικοινωνία μεταξύ των πλοίων με την στεριά πραγματοποιείται με τη βοήθεια συστημάτων που υπάρχουν στα πλοία και τα οποία μέσω των σταθμών στη στεριά αλλά και μέσω των δορυφόρων αναμεταδίδουν το σήμα. Από πλοίο σε πλοίο η επικοινωνία μπορεί να πραγματοποιηθεί από VHF με την Ψηφιακή Επιλεκτική Κλήση (DSC), η οποία μέσω ψηφιακών εντολών μεταδίδει η λαμβάνει σήματα κινδύνου, επείγοντα σήματα, σήματα ασφαλείας, μηνύματα ρουτίνας ή προτεραιότητας. Η επικοινωνία πλοίου με πλοίο μπορεί επίσης - για μεγάλες αποστάσεις - να πραγματοποιηθεί και με τα MF (μεσαία κύματα) και HF (βραχέα κύματα). Οι ελεγκτές DSC μπορούν πλέον να ενσωματωθούν με το ραδιόφωνο VHF σύμφωνα με την SOLAS. Οι δορυφορικές υπηρεσίες – επικοινωνίες χρησιμοποιούν τους γεωστατικούς δορυφόρους για την μετάδοση και λήψη σημάτων. Οι δορυφόροι χρησιμοποιούνται σε περιοχές που τα επίγεια συστήματα επικοινωνίας δεν μπορούν να λάβουν ή να στείλουν σήμα λόγω απόστασης. Οι υπηρεσίες αυτές παρέχονται από το Inmarsat και το Cospas – Sarsat. Το σύστημα Inmarsat-C είναι ένα ψηφιακό σύστημα ανταλλαγής μηνυμάτων κειμένου το οποίο είναι παγκόσμια αναγνωρισμένο από τον International Maritime Organization (IMO) ως σύστημα ασφάλειας της ζωής και της περιουσίας στη θάλασσα, καλύπτοντας τις απαιτήσεις του Global Maritime Distress and Safety System (GMDSS) μέσω του οποίου έχουν καθοριστεί διεθνώς οι διαδικασίες, ο εξοπλισμός και τα πρωτόκολλα επικοινωνίας ώστε να αυξηθεί η ασφάλεια και να διευκολυνθεί η διάσωση για πλοία, σκάφη και αεροπλάνα. Αποτελεί το καλύτερο ψηφιακό σύστημα αποθήκευσης-και- προώθησης μηνυμάτων (store-and-forward messaging), καθώς επίσης και εφαρμογών τηλεμετρίας και ανίχνευσης (tracking) με εξαιρετικά χαμηλό κόστος. Το σύστημα Inmarsat-C δεν μπορεί να χρησιμοποιηθεί για επικοινωνία φωνής.

ΚΕΦΑΛΑΙΟ 4: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

4.1 Έννοια της Ασφάλειας Πληροφοριακών Συστημάτων

4.1.1 Ορισμός

Ασφάλεια Πληροφοριών - και κατ' επέκταση Πληροφοριακών Συστημάτων - ονομάζεται το σύνολο των μηχανισμών, πολιτικών, διαδικασιών και οργανωτικών δομών, προκειμένουν να διασφαλιστεί ότι ικανοποιούνται οι απαιτήσεις ασφαλείας ενός οργανισμού. Η πληροφορία σε οποιαδήποτε μορφή (προφορική, έντυπη, ηλεκτρονική) αποτελεί έναν πόρο, ένα περιουσιακό στοιχείο του οργανισμού και χρειάζεται συνεχή και επαρκή προστασία.

Η ασφάλεια ενός πληροφοριακού συστήματος υλοποιείται σε τρεις διαστάσεις με βάση το τρίγωνο CIA (Confidentiality - Integrity - Availability)

- **Εμπιστευτικότητα (Confidentiality):** Εμπιστευτικότητα σημαίνει πως μόνο συγκεκριμένα - και εξουσιοδοτημένα - άτομα μπορούν να έχουν πρόσβαση σε συγκεκριμένες ευαίσθητες πληροφορίες.
- **Ακεραιότητα (Integrity):** Η Ακεραιότητα αφορά στη διατήρηση της μορφής και των δεδομένων ενός Π/Σ, την αποφυγή τροποποίησής τους από μη εξουσιοδοτημένα άτομα καθώς και την αποτροπή χρήσης ή πρόσβασης πόρων του συστήματος από άτομα χωρίς την σχετική άδεια.
- **Διαθεσιμότητα (Availability):** Διαθεσιμότητα σε ένα Π/Σ σημαίνει την εξασφάλιση ότι οι πόροι του συστήματος (δεδομένα, δίκτυο, υπολογιστές κλπ) είναι στη διάθεση των χρηστών οποιαδήποτε στιγμή απαιτηθεί.

4.1.2 Χρησιμότητα - Αναγκαιότητα της Ασφάλειας Πληροφοριών

Η τήρηση του μοντέλου CIA (Confidentiality - Integrity - Availability) είναι εξαιρετικά σημαντική για έναν οργανισμό ή μια επιχείρηση σε διάφορους τομείς όπως τα κέρδη - έσοδα, το εταιρικό προφίλ, τη συμμόρφωση με τα ισχύοντα θεσμικά κείμενα και τη διατήρηση κάποιων πλεονεκτημάτων συγκριτικά με τον ανταγωνισμό.

Τα πληροφοριακά συστήματα των οργανισμών - επιχειρήσεων αντιμετωπίζουν καθημερινά ένα μεγάλο φάσμα απειλών για την ασφάλειά τους οι οποίες μπορεί να είναι ιοί, ηλεκτρονική απάτη, Denial of Service (DoS attacks), hacking, cracking, βανδαλισμοί, φυσικές καταστροφές, κλπ. Γίνεται εύκολα αντιληπτό ότι η οποιαδήποτε δυσλειτουργία ή παράνομη διείσδυση σε ένα πληροφοριακό σύστημα μπορεί να σημάνει οικονομικές απώλειες, μειωμένη αποδοτικότητα και - ανάλογα τη σημαντικότητα του Π/Σ - να προκαλέσει θέμα τοπικής ή και εθνικής ασφάλειας.

Είναι επομένως μείζονος σημασίας ζήτημα το να αναγνωρίζουμε τις ευπάθειες ενός Π/Σ και τους κινδύνους που εγκυμονούν αυτές έτσι ώστε να είναι ευκολότερη η εύρεση λύσεων για την αντιμετώπισή τους.

4.2 Ασφάλεια Πληροφοριακών Συστημάτων και Ναυτιλία

4.2.1 Κυβερνοαπειλή - Κυβερνοπόλεμος - Κυβερνοεπιθέσεις

Η πρόοδος που παρουσίασε η τεχνολογία της πληροφορικής και η εκθετική αύξηση της χρήσης και του μεγέθους του διαδικτύου τις τελευταίες δύο δεκαετίες, έφεραν στο προσκήνιο μία νέα απειλή ασφαλείας, τις επιθέσεις μέσω ή εναντίον του Κυβερνοχώρου ή Κυβερνοεπιθέσεις. Όλες οι χώρες οι οποίες εξαρτώνται σε μεγάλο βαθμό από την πληροφοριακή υποδομή και τα δίκτυα υπολογιστών για τη λειτουργία των κρίσιμων υποδομών τους, όπως ο οικονομικός τομέας, η ενέργεια, οι τηλεπικοινωνίες, τα δίκτυα πετρελαίου και φυσικού αερίου, οι μεταφορές, τα δίκτυα ύδρευσης των πόλεων, οι υπηρεσίες εκτάκτων αναγκών και η ηλεκτρονική διακυβέρνηση, αντιμετωπίζουν αυτή την απειλή. Για μια χώρα, οι πιθανές επιπτώσεις των Κυβερνοεπιθέσεων είναι σοβαρές, από τη διατάραξη της καθημερινότητας των πολιτών της μέχρι την υπονόμευση της κυριαρχίας της.

Σε ένα άναρχο σύστημα όπως ο Κυβερνοχώρος, οι δράστες οι οποίοι επιδίδονται

σε παράνομες δραστηριότητες, ομαδοποιούνται γενικώς σε κατηγορίες, κυρίως με βάση το σκοπό για τον οποίο δραστηριοποιούνται. Οι κατηγορίες των δραστών, κατά αυξανόμενο επίπεδο απειλής, είναι:

- Χάκερ (Hackers)
- Ακτιβιστές-χάκερ (Hactivists)
- Οργανωμένο έγκλημα
- Δράστες βιομηχανικής κατασκοπίας
- Εσωτερικοί δράστες
- Εξωτερικοί συνεργάτες/σύμβουλοι
- Τρομοκρατικές οργανώσεις
- Χώρες

Το μεγαλύτερο μέρος της δραστηριότητας που παρατηρείται σήμερα στον Κυβερνοχώρο ποικίλει από την απλή εισβολή σε ένα σύστημα και τον έλεγχό του για λόγους πρόκλησης και περιέργειας, μέχρι την εισβολή σε ένα σύστημα για λόγους εκδίκησης, κλοπής πληροφοριών, πρόκλησης, παρενόχλησης, υπεξαίρεσης χρημάτων ή πρόκλησης εσκεμμένης τοπικής βλάβης σε υπολογιστές ή καταστροφής μεγαλύτερης έκτασης σε υποδομές. Οι επιπτώσεις της κατηγορίας αυτής των Κυβερνοεπιθέσεων που εκδηλώνονται από χάκερ, ακτιβιστές χάκερ, το οργανωμένο έγκλημα, τη βιομηχανική κατασκοπία και τους εσωτερικούς δράστες, οι οποίες μπορεί να είναι ιδιαίτερα σοβαρές και δεν πρέπει να υποτιμώνται, χαρακτηρίζονται ως χάκινγκ, κυβερνοβλάβες, κλοπή, εκδίκηση, κατασκοπία, οργανωμένο έγκλημα και εμπίπτουν στη δικαιοδοσία της επιβολής του νόμου και της απονομής δικαιοσύνης και δεν εξετάζονται στα πλαίσια της παρούσας μελέτης.

Υπάρχουν δύο μέσα τα οποία μια χώρα, μια οργάνωση ή κάποιο άτομο θα μπορούσε να χρησιμοποιήσει για την εκδήλωση Κυβερνοεπιθέσεων εντός ή μέσω του Κυβερνοχώρου· ο υπολογιστής και τα κακόβουλα προγράμματα. Στη διεθνή βιβλιογραφία και αρθρογραφία, τα μέσα αυτά αποκαλούνται Κυβερνοόπλα (Cyber weapons).

Τα Κυβερνοόπλα μπορούν να χρησιμοποιηθούν σε διάφορους συνδυασμούς για να υλοποιήσουν μια ποικιλία τεχνικών προσβολής κάποιου στόχου. Η επιλογή της τεχνικής που θα χρησιμοποιηθεί για την προσβολή εξαρτάται από διάφορους παράγοντες, όπως οι δεξιότητες και η εμπειρία του χρήστη, οι δυνατότητες των όπλων, η φύση του στόχου και άλλους. Οι πλέον συνηθισμένες γνωστές τεχνικές Κυβερνοεπιθέσεων είναι οι ακόλουθες.

- Denial of Service (DoS) Attack
- Backdoor
- E-mail spoofing
- IP Address spoofing
- Logic Bomb
- Digital manipulation

Η χρήση των Κυβερνοόπλων και οι τεχνικές για την προσβολή διαφόρων στόχων δεν αποτελούν αυτοσκοπό. Οι Κυβερνοεπιθέσεις διεξάγονται για την επίτευξη κάποιου συγκεκριμένου σκοπού. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικώς όμως ανήκει σε μία από τις παρακάτω κατηγορίες:

- **Εκμετάλλευση (exploitation)**
  Στην περίπτωση της εκμετάλλευσης βασικός στόχος του δράστη είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών που είναι συνδεδεμένες με αυτόν.
- **Παραπλάνηση (deception)**
  Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις πληροφορίες τις οποίες αυτός συλλέγει, αναλύει ή παράγει, στοχεύοντας ουσιαστικά στο σύστημα λήψης αποφάσεων του αντιπάλου.
- **Καταστροφή (destruction)**
  Στην περίπτωση της καταστροφής ο επιτιθέμενος, μέσω της χρήσης πληροφοριακών συστημάτων, καθιστά αδύνατη τη λειτουργία του στόχου, καταστρέφοντας τον ίδιο ή τα συστήματα υποστήριξης που είναι απαραίτητα για τη λειτουργία του. Στην περίπτωση αυτή πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου, αλλά η κρίσιμη υποδομή του.
- **Διακοπή λειτουργίας ή εξουδετέρωση (denial of service ή disruption)**
  Στην περίπτωση επιθέσεων διακοπής λειτουργίας (DoS) ή εξουδετέρωσης ο επιτιθέμενος δεν καταστρέφει το στόχο αλλά τον θέτει εκτός λειτουργίας ή τον καθιστά αναξιόπιστο για κάποια χρονική περίοδο, απαγορεύοντας στους νόμιμους χρήστες την εξυπηρέτησή τους ή την πρόσβαση σε πηγές πληροφοριών.

4.2.2 Ανάλυση Κινδύνων

Μια ναυτιλιακή επιχείρηση αποτελεί έναν σύνθετο και ταυτόχρονα πολύπλοκο

οργανισμό καθώς απαιτεί την συνύπαρξη και συνεργασία πολλών διαφορετικών τμημάτων για την επίτευξη των στόχων της. Γίνεται λοιπόν κατανοητό ότι και τα πληροφοριακά συστήματα ενός τέτοιου οργανισμού αποτελούν εξίσου πολύπλοκες οντότητες με τεράστιο εύρος εφαρμογών. Το γεγονός αυτό δημιουργεί πρόσφορο έδαφος σε κάθε είδους "εισβολείς" (hackers, πειρατές κλπ) οι επιθέσεις των οποίων έχουν αυξηθεί κατακόρυφα τα τελευταία χρόνια.

Η ναυτιλιακή δραστηριότητα αποτελεί σημαντικό παράγοντα της οικονομικής ζωής που σχετίζεται κυρίως με την εφοδιαστική αλυσίδα. Η διευκόλυνση που παρέχουν οι πληροφορίες έχει αναδείξει και μια σειρά κινδύνους με κυριότερο την ασφάλεια. Το πλοίο και τα λιμάνια όλο και περισσότερο εξαρτώνται από υπολογιστές, αφού χρησιμοποιούν τεχνολογίες διαδικτύου στην καθημερινές δραστηριότητες τους και μια σειρά από συστήματα ζωτικής σημασίας, με αποτέλεσμα να αντιμετωπίζουν κινδύνους κυβερνοεπιθέσεων.

Αρχικά, θα πρέπει να εξεταστούν τα ειδικά χαρακτηριστικά του ναυτιλιακού τομέα και κυρίως το βασικό εργαλείο οικονομικής δραστηριότητας, που είναι το εμπορικό πλοίο. Οι δύο μεγάλες κατηγορίες είναι τα πλοία μεταφοράς φορτίου και τα πλοία μεταφοράς επιβατών. Τα πλοία ναυλώνονται από τρίτους για την εκτέλεση συγκεκριμένου μεταφορικού έργου. Πολλές φορές, οι ναυλωτές απαιτούν ειδικά πληροφορικά συστήματα, όπως γίνεται στην περίπτωση των εμπορευματοκιβωτίων όπου ο πλοιοκτήτης και το πλήρωμα δεν έχουν τον πλήρη έλεγχο.

Τα πλοία λειτουργούν κυρίως offline, με αποτέλεσμα το επίπεδο ασφάλειας να μην μπορεί να ελεγχθεί με αποφυγή διασύνδεσης, είτε με παροχή βοήθειας από το γραφείο. Υπάρχουν σειρά από κρίσιμα δεδομένα σχετικά με το φορτίο που περνούν από μεγάλο αριθμό συστημάτων ξηράς (λιμάνια, εμπορευματικά κέντρα κ.λπ.), όπου εκεί γίνεται ευκολότερη η διείσδυση κακόβουλου λογισμικού ή υποκλοπής/τροποποίησης δεδομένων. Στην όλη αλυσίδα μεταφοράς υπάρχουν υψηλής αξιοπιστίας συστήματα όπως είναι οι ηλεκτρονικοί χάρτες (ECDIS – Electronic Chart Display Information Systems) και δορυφορικοί δέκτες που κάνουν το πλοίο πιο ευάλωτο σε κυβερνοεπιθέσεις.

Το πλοίο είναι μια ανεξάρτητη μονάδα και μια κυβερνοεπίθεση μπορεί να δημιουργήσει κινδύνους στην ασφάλειά του, όπως η επίδραση σε συστήματα ναυσιπλοΐας ή ευστάθειας, στο περιβάλλον επιδρώντας στα συστήματα εξαγωγής αποβλήτων/έρματος ή τέλος, προκαλώντας εσκεμμένο ατύχημα. Δεν θα πρέπει να ξεχνάμε ότι μια κυβερνοεπίθεση προξενεί σημαντικό πρόβλημα στην επιχειρηματική δραστηριότητα της πλοιοκτήτριας εταιρείας με σημαντικές οικονομικές απώλειες αλλά το κυριότερο, επιφέρει πλήγμα στην αξιοπιστία της, που είναι καίριο για την ναυτιλιακή κοινότητα.

Όσον αφορά το πλήρωμα που επανδρώνει ένα πλοίο, θα πρέπει να διευκρινιστεί ότι οι κυβερνοεπιθέσεις είναι μια νέα απειλή και παρόλο που υπάρχουν διαδικασίες προβλεπόμενες από αντίστοιχες διεθνείς συμβάσεις του Διεθνούς Ναυτιλιακού Οργανισμού IMO (International Maritime Organization), δεν αντιμετωπίζονται από αυτές συμβάντα αυτού του είδους. Η κυβερνοασφάλεια ενός πλωτού (πλοίου ή πλατφόρμας) εξαρτάται κύρια από το προσωπικό του γραφείου και μόνο πρόσφατα εμφανίστηκε ή ανάγκη επάνδρωσης πλοίων με εξειδικευμένο προσωπικό σε ηλεκτρολογικά/ηλεκτρονικά συστήματα (ETO, Electro technical Officer). Επιπρόσθετα, υπάρχει αριθμός λογισμικών προγραμμάτων που είναι ιδιωτικά και σε πολύ μικρό βαθμό το πλήρωμα μπορεί να επέμβει και η μόνη διέξοδος είναι η επικοινωνία για παροχή οδηγιών από την ξηρά.

Με γνώμονα την παραπάνω κατάσταση, υπάρχει σημαντική δραστηριότητα στο πλαίσιο του IMO, να εκδοθούν σε πρώτο στάδιο οδηγίες αντιμετώπισης κυβερνοεπιθέσεων στην ναυτιλία και σε δεύτερο στάδιο, να γίνει τροποποίηση των αντιστοίχων παγκοσμίως οδηγιών για αντιμετώπιση ασφάλειας στη Ναυτιλία, ώστε να περιλαμβάνουν και τα νέα δεδομένα κινδύνων που προέρχονται από τον κυβερνοχώρο.

4.2.3 Κυβερνοαπειλές - Κυβερνοεπιθέσεις στο χώρο της Ναυτιλίας

Στις ναυτιλιακές επιχειρήσεις και κατ' επέκταση στα πλοία ιδιοκτησίας τους, υπάρχει μια σειρά συστημάτων που είναι ζωτικής σημασίας για τη λειτουργία τους και ταυτόχρονα αποτελούν στόχους κυβερνοεπιθέσεων:

Συστήματα Ελέγχου Πλοίου και Πρόωσης: περιλαμβάνει τις κύριες μηχανές πρόωσης του πλοίου, τις μηχανές παραγωγής ηλεκτρικής

ενέργειας, τους πίνακες διανομής, σειρά βοηθητικών μηχανημάτων και τα αντίστοιχα ηλεκτρονικά και ηλεκτρικά συστήματα ελέγχου.

Συστήματα ναυσιπλοΐας περιλαμβανομένων μεταξύ άλλων το σύστημα προσδιορισμού θέσεως GPS, (Global Positioning System) το σύστημα αναφορών AIS, (Automatic Identification System) Ηλεκτρονικούς Χάρτες ECDIS, αυτόματο πιλότο, σύστημα radar, γυροσκοπική πυξίδα, συστήματα δυναμικού προσδιορισμού θέσεως (dynamic positioning, συστήματα καταγραφής δεδομένων (μαύρο κουτί), VDR (Vessel Data Regorder) κ.λπ.

Βιομηχανικά συστήματα ελέγχου πλοίου όπως πρόωσης, πηδαλιουχίας, διαχείρισης έρματος (ballast-water management), ηλεκτρικά συστήματα, κλιματισμός, συστήματα ευστάθειας, φορτίου, εντοπισμού πυρκαγιάς.

Επικοινωνίες (επίγειες και δορυφορικές) και συστήματα παρακολούθησης, όπως κάμερες ασφάλειας, συστήματα ειδοποίησης, επικίνδυνων αερίων και ελέγχου ρύπανσης περιβάλλοντος.

Ενδεικτικά αναφέρονται παρακάτω κάποιες περιπτώσεις κυβερνοεπιθέσεων στον ναυτιλιακό τομέα:

Κλοπή χρημάτων με κυβερνοεπίθεση: Η φύση αυτού του τύπου συμβάντων είναι ήδη γνωστή και από άλλους τομείς και αφορά τη μεταφορά χρημάτων από ένα τραπεζικό λογαριασμό σε άλλο, που ελέγχεται από τους επιτιθέμενους χρησιμοποιώντας παραπλανητικές ηλεκτρονικές μεθόδους. Το είδος αυτό της επίθεσης, δεδομένου ότι περιέχει όχι μόνο τεχνικές διαδικασίες, αλλά εμπίπτει και στο τραπεζικό απόρρητο, είναι αρκετά δύσκολο να αντιμετωπιστεί. Η επίθεση κυρίως γίνεται με τη διείσδυση ενός τρίτου στην επικοινωνία ηλεκτρονικού ταχυδρομείου, μεταξύ δύο εταιρειών και την αποστολή μηνυμάτων. Κάθε μια από τις εμπλεκόμενες εταιρείες νομίζει ότι επικοινωνεί με τον αντίστοιχο εταίρο, αλλά στην πραγματικότητα παρεμβάλλεται και ο υποκλοπέας. Για τη δημιουργία τέτοιου τύπου επιθέσεων απαιτείται η πρόσβαση λογισμικού στα ηλεκτρονικά συστήματα μιας εκ των δύο εταιρειών και στη συνέχεια, παρακολούθηση της ηλεκτρονικής αλληλογραφίας. Στη συνέχεια, παρακολουθούνται τα νόμιμα μηνύματα χρηματικών απαιτήσεων και ανάλογα παρεμβαίνει ο χρήστης τροποποιώντας την ροη των χρημάτων. Τέτοια συμβάντα αφορούν κυρίως σχέση της εταιρείας με προμηθευτές πετρελαίου και με ναυπηγεία και τον Δεκέμβριο του 2013, σύμφωνα με αμερικανικές αρχές κόστισαν παράνομες μεταφορές χρημάτων ύψους 2 εκατ. δολαρίων σε τρία μόνο συμβάντα.

Λαθρεμπόριο ναρκωτικών και διαγραφή εμπορευματοκιβωτίων από λιμάνι: Η επίθεση που έγινε το 2011 αφορά παρέμβαση στα δεδομένα εμπορευματοκιβωτίων και διαγραφή όλων των στοιχείων που αφορούν φορτίο, ημερομηνία φόρτωσης, αριθμό φορτίου και λιμένα προορισμό. Αυτό είχε σαν αποτέλεσμα να μη γνωρίζει κανείς τα εμπορευματοκιβώτια τι περιέχουν, τον προορισμό τους και τα στοιχεία αποστολέα παραλήπτη. Η κατάσταση αυτή δημιούργησε διαδικαστική δυσλειτουργία στην διαχείριση των εμπορευματοκιβωτίων με αποτέλεσμα σημαντικές οικονομικές απώλειες. Έχουν αναφερθεί επίσης προσπάθειες παρεμβολής στα στοιχεία επιθεωρήσεως, που τηρούνται από τα ηλεκτρονικά συστήματα, υπόπτων για μεταφορά ναρκωτικών εμπορευματοκιβωτίων που εμφανίζονται ηλεκτρονικά ότι αυτά έχουν ελεγχθεί, ενώ στην πραγματικότητα συμβαίνει το αντίθετο.

Zombie Zero: Η περίπτωση αυτής της επίθεσης μάς δείχνει την επίδραση του ναυτιλιακού τομέα στην συνολική εφοδιαστική αλυσίδα. Αφορά κυβερνοεπίθεση από μια ηλεκτρονική συσκευή σάρωσης (barcode scanner) που χρησιμοποιείτο από μια εφοδιαστική εταιρεία για την καταγραφή και έλεγχο των εμπορευματοκιβωτίων. Το κακόβουλο λογισμικό είχε τοποθετηθεί πριν την αγορά της συσκευής και κατά τη λειτουργία του και τη μεταφορά δεδομένων, πετύχαινε πρόσβαση στο πληροφοριακό σύστημα της εταιρείας και δημιουργούσε σύνδεση με απομακρυσμένο server στην Κίνα, όπου γίνονταν διάφορες παρεμβάσεις τροποποίησης δεδομένων. Το συμβάν, που ονομάστηκε Zombie Zero, ανακαλύφθηκε το 2014 στα συστήματα τουλάχιστον οκτώ διαφορετικών εταιρειών και βρέθηκαν μολυσμένοι 16 από τους συνολικά 48 σαρωτές κωδικών φορτίου που χρησιμοποιούνταν.

Icefog: Η γνωστή εταιρεία ασφάλειας ηλεκτρονικών συστημάτων Kaspersky δημοσιοποίησε πληροφορίες για μια επίθεση που ονομάστηκε Icefog και στόχο είχε ιαπωνικές και κορεάτικες εταιρείες και ναυπηγεία. Η επίθεση έδινε πρόσβαση backdoor σε συγκεκριμένες εταιρείες, με σκοπό την υποκλοπή εγγράφων, την υποκλοπή κωδικών πρόσβασης με σκοπό την

πρόσβαση σε τμήματα του εταιρικού δικτύου. Οι επιθέσεις αυτές συνήθως είναι μόνιμες μέχρι να γίνουν αντιληπτές. Στην περίπτωση, όμως, των ναυπηγείων γίνονταν για λίγες ώρες και με συγκριμένο στόχο από μέρους των παρανόμων.

Λιμάνι της Αμβέρσας, επίθεση από έμπορους ναρκωτικών: Στο τέλος του 2013, το λιμάνι της Αμβέρσας ανακοίνωσε την περίπτωση επίθεσης στα πληροφοριακά του συστήματα διαχείρισης εμπορευματοκιβωτίων, όπου είχε αποκτηθεί απομακρυσμένη πρόσβαση από αγνώστους στους τερματικούς σταθμούς, με αποτέλεσμα να φορτώνουν εμπορευματοκιβώτια σε δικά τους φορτηγά χωρίς την ενημέρωση του κεντρικού σταθμού. Επίσης, σε δεύτερο στάδιο την παράκαμψη ηλεκτρονικής καταγραφής ελέγχων ασφάλειας για διευκόλυνση εμπόρων ναρκωτικών. Όταν η επίθεση αυτή αποκαλύφθηκε, η αστυνομία ανακάλυψε ένα τόνο κοκαΐνη, όπλα και 1,5 εκατ. ευρώ σε χαρτονομίσματα. Εκτός από αυτά, η επίθεση αυτή εντόπιζε φορτία μεγάλης οικονομικής αξίας που γίνονταν στόχος κλοπής.

Παράκαμψη των Αυστραλιανών τελωνείων: Η επίθεση αφορά πρόσβαση στα ηλεκτρονικά συστήματα των τελωνείων της Αυστραλίας μέσω του πληροφοριακού συστήματος μιας ιδιωτικής εταιρείας φόρτωσης εκφόρτωσης. Η επίθεση ανακαλύφθηκε το 2012 και αφορά έλεγχο και ειδοποίηση τρίτων για εμπορευματοκιβώτια που είχαν χαρακτηριστεί ύποπτα από την αστυνομία ή το τελωνείο. Αποτέλεσμα αυτού ήταν εμπορευματοκιβώτια με τα λαθραία υλικά να εγκαταλείπονται ή να τροποποιούνται τα δεδομένα τους ώστε να μην ελέγχονται.

AIS spoofing: Το ναυτιλιακό σύστημα αυτόματης αναγνώρισης (AIS, Automatic Identification System) αποτελεί βασικό σύστημα εντοπισμού του πλοίου και έγκαιρης ειδοποίησης, σε περίπτωση συμβάντων ασφάλειας κύρια σε περιπτώσεις διάπλου σε περιοχές υψηλού κινδύνου, όπως είναι περιοχές με μεγάλο αριθμό συμβάντων ναυτικής πειρατείας. Το σύστημα στέλνει σε τακτά χρονικά διαστήματα σειρά πληροφοριών στην ξηρά και σε άλλα πλοία. Το πλήρωμα και ο πλοιοκτήτης είναι οι μόνοι που επιτρέπεται να μεταβάλουν τα δεδομένα που αποστέλλονται. Τον Οκτώβριο του 2013, η εταιρεία Trend Micro έκανε επίδειξη πώς ένα τέτοιο σύστημα μπορεί να παρεμβληθεί με μια συσκευή που κόστισε μόλις 200 δολάρια. Πιο συγκεκριμένα, σε αυτού του είδους τις επιθέσεις μπορούσε να επιτευχθεί, τροποποίηση της θέσης, φορτίου, ταχύτητας και ονόματος του πλοίου, δημιουργία ενός ανυπάρκτου «πλοίου φαντάσματος», αποστολή ψευδών μετεωρολογικών δεδομένων και στοιχείων έρευνας και διάσωσης, προειδοποίηση για πιθανό ναυτικό ατύχημα, με αποτέλεσμα την αλλαγή πορείας του πλοίου κλπ. Το βασικό μειονέκτημα του AIS είναι ότι δεν έχει ενσωματωμένο σύστημα ασφάλειας, οπότε όλες οι πληροφορίες που μεταδίδονται θεωρούνται αυθεντικές. Σε παγκόσμιο επίπεδο, γίνεται προσπάθεια θωράκισης του συστήματος ώστε να αποφευχθούν τέτοιου είδους επιθέσεις οι οποίες είναι πλέον συνηθισμένες.

Τα κοινωνικά δίκτυα ως πηγή πληροφοριών για πειρατές: Η μεγάλη εξάπλωση των κοινωνικών δικτύων ήταν επόμενο να επηρεάσει και τον ναυτιλιακό τομέα και κύρια τους ναυτικούς που βρίσκονται μεγάλα χρονικά διαστήματα πάνω στα πλοία. Από την άλλη, η εξέλιξη της ναυτικής πειρατείας στις περιοχές μεγάλου κινδύνου (Κόλπος Aden) έχει κάνει τους πειρατές, εκτός από το να επιτίθενται στα συστήματα AIS, να συλλέγουν πληροφορίες μέσω του Facebook και κυρίως στοιχεία (φωτογραφίες κ.λπ.) που αφορούν θέσεις ασφάλειας στο πλοίο, καταφύγια σε περίπτωση πειρατικής επίθεσης κ.ά. προετοιμάζοντας έτσι τους πειρατές για μεγαλύτερες πιθανότητες επιτυχούς επίθεσης. Όπως γίνεται αντιληπτό, η παραπάνω περίπτωση δεν αποτελεί ακριβώς κυβερνοεπίθεση, αλλά αναφέρεται στα πλαίσια της γενικότερης ηλεκτρονικής ασφάλειας στο πλοίο.

Διακοπή λειτουργίας πλωτής πλατφόρμας από κακόβουλο λογισμικό: Το 2010 αναφέρθηκε επίθεση σε θαλάσσια πλατφόρμα εξαγωγής πετρελαίου στην διάρκεια πλου από την Νότια Κίνα προς Νότια Αμερική. Κρίσιμα συστήματα ελέγχου επηρεαστήκαν από κακόβουλο λογισμικό με αποτέλεσμα να ακινητοποιηθεί για 19 μέρες μέχρι να αποκατασταθεί πλήρως. Σύμφωνα με τον Αγγλικό νηογνώμονα Lloyds Register αυτό το περιστατικό είναι ένα από τα 6 που έχουν εντοπιστεί σε εξέδρες offshore τα τελευταία χρόνια.

Κακόβουλος έλεγχος ναυσιπλοΐας: Τον Ιούλιο του 2013 μια ερευνητική ομάδα από πανεπιστήμιο του Τέξας απέκτησε έλεγχο του συστήματος ναυσιπλοΐας στην μεσόγειο ενός γιοτ αξίας 80 εκατομμυρίων δολαρίων χρησιμοποιώντας συσκευή αξίας μόλις 3.000

δολαρίων για την κατασκευή της. Η επίθεση έγινε με ράδιο σήματα που το πλοίο έλαβε μέσω της κεραίας GPS και έδωσε πρόσβαση από την ξηρά στο σύστημα ναυσιπλοΐας.

Παρεμβολή GPS: Σήμερα, υπάρχουν στην αγορά και πωλούνται παράνομα συσκευές παρεμβολής GPS που κοστίζουν λίγες χιλιάδες δολάρια. Με την συσκευή αυτή είναι δυνατή η παρεμβολή του GPS από αποστάσεις που φθάνουν μέχρι περίπου 500 μέτρα. Το GPS αποτελεί βασική συσκευή για το πλοίο δεδομένου ότι δίνει χρονισμό και δεδομένα αναφοράς σε σειρά συστημάτων όπως είναι οι ηλεκτρονικοί χάρτες, το ραντάρ, η γυροπυξίδα κλπ. Μια τέτοια παρεμβολή είναι σίγουρο ότι θα δημιουργήσει σημαντικά προβλήματα στη λειτουργία του πλοίου και θα κάνει σημαντικά δύσκολη τη διαχείρισή του ειδικά σε περιοχές με υψηλή ναυτιλιακή κίνηση.

Τροποποίηση δεδομένων ηλεκτρονικών χαρτών: Το σύστημα ECDIS – (Electronic Chart Display and Information System) είναι ένα υπολογιστικό σύστημα που συνήθως βρίσκεται στη γέφυρα ενός πλοίου και χρησιμοποιείται από τους αξιωματικούς ναυσιπλοΐας για την πλοήγηση του πλοίου, παράλληλα με τους παραδοσιακούς ναυτικούς χάρτες τους οποίους αναμένεται να αντικαταστήσει σε λίγα χρόνια. Το ECDIS δίνει πληροφορίες σε σειρά συστημάτων του πλοίου, τα οποία με τη σειρά τους συνδέονται στο δίκτυο αισθητήρων του πλοίου που έχει πρόσβαση στην πύλη εξόδου του πλοίου στο διαδίκτυο. Οι ενημερώσεις των ναυτιλιακών χαρτών γίνεται συνήθως είτε μέσω διαδικτύου είτε από το προσωπικό με φορητά μέσα αποθήκευσης. Υπάρχουν επίσης και μια σειρά άλλων θεμάτων ασφάλειας όπως η δυνατότητα ανάγνωσης, αντικατάστασης, διαγραφής κ.λπ. σε συστήματα που χρησιμοποιούνται από τους ωκεανικούς χάρτες. Από τη στιγμή που κάποιος αποκτήσει κακόβουλη πρόσβαση στο σύστημα, είναι προφανές ότι υπάρχει δυνατότητα να επηρεάσει όλες τις συσκευές που διασυνδέονται με τους ηλεκτρονικούς χάρτες.

4.3 Σχεδιασμός Ασφαλείας

4.3.1 Καταγραφή υφιστάμενης κατάστασης

Στη φάση αυτή θα καταγραφεί η υπολογιστική και επικοινωνιακή υποδομή της επιχείρησης, δηλαδή όλων των περιουσιακών στοιχείων (assets) της εταιρείας. Τα περιουσιακά στοιχεία μιας εταιρείας μπορεί να χωριστούν στις παρακάτω κατηγορίες:

- **Δεδομένα (Data assets):** Στην κατηγορία αυτή ανήκουν κάθε είδους δεδομένα, από δεδομένα προσωπικού χαρακτήρα σε μια βάση δεδομένων μέχρι και οι καταχωρήσεις σε έναν DNS server.

- **Υπηρεσίες (End User Services):** Στην κατηγορία αυτή ανήκουν οι υπηρεσίες που επιτρέπουν στον τελικό χρήστη πρόσβαση στα δεδομένα. Για παράδειγμα η υπηρεσία πρόσβασης σε μια βάση δεδομένων που επιτρέπει στους χρήστες να προσπελάσουν τα δεδομένα που αυτή περιέχει.

- **Υλικά Στοιχεία:** Η κατηγορία αυτή περιλαμβάνει τα υλικά στοιχεία που αποτελούν το υπολογιστικό σύστημα, δηλαδή τους υπολογιστές, το δίκτυο, μέσα αποθήκευσης κτλ.

- **Τοποθεσίες:** Στην κατηγορία αυτή περιλαμβάνονται τα δωμάτια, κτίρια ή ακόμα και οικόπεδα τα οποία ανήκουν στον οργανισμό και περιέχουν μέρη των υπολογιστικών συστημάτων.

- **Λογισμικό (software):** Η κατηγορία αυτή μπορεί να χρησιμοποιηθεί σε οργανισμούς που παράγουν λογισμικό και επομένως είναι υψίστης σημασίας η προστασία του κώδικα.

Εφόσον γίνει η καταγραφή της υφιστάμενης κατάστασης, έπειτα αναλύονται οι πληροφοριακές διαδικασίες στη λειτουργία της εταιρείας και προσδιορίζεται ο ρόλος όλων των χρηστών, κατατάσσοντας τους σε κατηγορίες. Καταγράφονται επίσης όλες οι διαδικασίες της εταιρείας που σχετίζονται με την ασφάλεια του πληροφοριακού συστήματος και στη συνέχεια γίνεται η αξιολόγηση όλων των στοιχείων καθώς και η αξιολόγηση των υφιστάμενων μέτρων ασφαλείας τους. Τέλος, αναλύονται οι ιδιαιτερότητες του πληροφοριακού συστήματος, όσον αφορά τα ευαίσθητα προσωπικά δεδομένα που τηρούνται από την εταιρεία.

4.3.2 Αναγνώριση τρωτών σημείων - ευπαθειών

Στη φάση αυτή και εφόσον έχει γίνει η ακριβής εκτίμηση και καθορισμός των περιουσιακών στοιχείων (assets) της εταιρείας και έχει εκτιμηθεί η αξία τους προς την εταιρεία, θα πρέπει να γίνει ανάλυση της επικινδυνότητας.

Ένα πολύ σημαντικό βήμα για την χάραξη της πολιτικής που θα ακολουθήσει η εταιρεία για την υλοποίηση της ασφαλείας του Πληροφοριακού της Συστήματος (Π.Σ.). Για την ακρίβεια, εδώ γίνεται μελέτη των εκθέσεων σε κινδύνους (exposures) του συστήματος, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του συστήματος με βάση τον υφιστάμενο έλεγχο (control).

Πιο συγκεκριμένα, η ανάλυση επικινδυνότητας (Risk Analysis) του πληροφοριακού συστήματος αποτελείται από τα εξής βήματα:

- **Η αναγνώριση των απειλών (threats) κατά του πληροφοριακού συστήματος:** Για κάθε κατηγορία περιουσιακών στοιχείων υπάρχουν και μια σειρά από απειλές. Στο βήμα αυτό αναγνωρίζονται οι απειλές για κάθε στοιχείο και οι επιπτώσεις που αυτές επιφέρουν.

- **Η αναγνώριση των επιμέρους ευπαθειών (vulnerabilities):** Ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά.

- **Η αναγνώριση των πιθανών κατηγοριών απωλειών (losses):** Η κατηγοριοποίηση γίνεται βάσει του βαθμού κινδύνου που υπολογίζεται ξεχωριστά για κάθε απειλή και είναι συνάρτηση όλων των παραπάνω, δηλαδή των επιπτώσεων μιας απειλής, που έχουν σχέση με την αξία του περιουσιακού στοιχείου, και της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή.

- **Η εκτίμηση της πιθανότητας να συμβεί μια απώλεια:** Αφού τελειώσει το στάδιο της αντιστοίχησης των απειλών τότε πρέπει να γίνει η αξιολόγηση της πιθανότητας να συμβεί μια απειλή σε κάθε περιουσιακό στοιχείο, καθώς και η ευπάθεια του προς την απειλή αυτή.

- **Προσδιορισμός των απαραίτητων προφυλάξεων για την αντιμετώπιση των κινδύνων:** Υπάρχουν 3 τρόποι αντιμετώπισης του κινδύνου η αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα, η αποδοχή του κινδύνου και η μείωση του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας). Κατά το βήμα αυτό αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στην εταιρεία.

4.3.3 Πολιτικές Ασφαλείας

Σκοπός της πολιτικής ασφάλειας πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η πολιτική ασφάλειας καθορίζεται από την διοίκηση του οργανισμού και θα πρέπει να υποστηρίζεται έμπρακτα από την ίδια. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού.

Επιγραμματικά η φάση αυτή περιλαμβάνει την καταγραφή και εκπόνηση του συνόλου των νόμων, κανόνων και πρακτικών που ρυθμίζουν πως τα στοιχεία διαχειρίζονται, προστατεύονται και κατανέμονται μέσα σε έναν οργανισμό χρηστών. Η εκπόνηση θα γίνει με βάση τη διάκριση των υποκειμένων (ενεργά στοιχεία του συστήματος όπως χρήστες, διεργασίες και προγράμματα) και αντικειμένων (αρχεία, κατάλογοι, συσκευές, υποδοχές – sockets κ.α.), στηριγμένη στο σύστημα των ρόλων και αρμοδιοτήτων (roles and responsibilities). Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από τη διοίκηση του οργανισμού. Στη συνέχεια θα πρέπει να δημοσιοποιηθεί σε όλους τους χρήστες του οργανισμού. Θα πρέπει να αναφέρει τη δέσμευση της διοίκησης και τον τρόπο προσέγγισης του οργανισμού σε θέματα ασφάλειας.

Η πολιτική ασφαλείας θα περιλαμβάνει τα παρακάτω στοιχεία:

- **Αγαθά (Assets):** Καθορισμός των αγαθών του οργανισμού, αφηρημένων και μη.

- **Ρόλους και αρμοδιότητες (Roles and Responsibilities):** Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.

- **Στόχους (Security policy objectives):** Τους στόχους της ασφαλείας και τον καθορισμό περιορισμών.

- **Πεδίο εφαρμογής της πολιτικής ασφαλείας (Scope of Security Policy):** Τον ορισμό της ασφάλειας των πληροφοριών, το

σκοπό της και τη σπουδαιότητά της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών. Γενικά, τον καθορισμό την εμβέλειας της πολιτικής ασφαλείας.

- **Οδηγίες, κατευθυντήριες γραμμές (Guidelines):** Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιεί ο οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.

- **Κουλτούρα, άλλες πολιτικές, νομοθεσία (Culture, legislation, other policies):** Το σύνολο πεποιθήσεων, αξιών, αρχών πολιτικών, κωδίκων δεοντολογίας και νόμων που συνθέτουν την κουλτούρα του οργανισμού.

- **Υλοποίηση και εφαρμογή - Ενημέρωση και συμμόρφωση (Implementation and application of the security policy – Awareness, enforcement, breach):** Πρόκειται για το οργανωτικό πλαίσιο για την υλοποίηση και την εφαρμογής της πολιτικής ασφαλείας καθώς και ενημέρωση του προσωπικού και συμμόρφωση με τις ενέργειες που λαμβάνονται σε περίπτωση παραβίασης της πολιτικής ασφαλείας.

- **Επισκόπηση και αναθεώρηση της πολιτικής (Review and audit):** Πρόκειται για την επισκόπηση και αναθεώρηση της πολιτικής, ανά τακτικά χρονικά διαστήματα ανάλογα και με τις συνθήκες, έτσι ώστε να καλύπτει τις ανάγκες του οργανισμού.

Οι κανόνες (rules) που θα καθορίσουν την πολιτική ασφαλείας θα εκφράζουν γενικότερες αρχές της εταιρείας, θα ικανοποιούν τα χαρακτηριστικά απλότητας (χωρίς περιττούς τεχνικούς όρους και εξειδικευμένες αναφορές), της σαφήνειας, της εύκολης εφαρμογής, θα είναι γενικεύσιμοι και επεκτάσιμοι και θα απαιτούν συμμόρφωση από όλο το προσωπικό της εταιρείας, στο οποίο θα είναι διαθέσιμοι.

Σε δεύτερο επίπεδο, στη φάση αυτή θα ολοκληρωθεί η εκπόνηση των απαιτήσεων ασφαλείας του πληροφοριακού συστήματος, σύμφωνα με την ανάλυση επικινδυνότητας και την πολιτική ασφαλείας που έχει εκπονηθεί. Στη φάση αυτή θα επιλεγούν και τα κατάλληλα μοντέλα ασφαλείας του πληροφοριακού συστήματος (των επάλληλων στρωμάτων, του κιβωτισμού κλπ.) που θα χρησιμοποιηθούν ως βάση για την δημιουργία των μηχανισμών και των μέτρων προστασίας.

4.3.4 Πρότυπα Πολιτικών Ασφαλείας

Η σχεδίαση - υλοποίηση της πολιτικής ασφαλείας ενός πληροφοριακού συστήματος βασίζεται σε διεθνώς αναγνωρισμένα πρότυπα, εκ των οποίων τα σημαντικότερα είναι τα εξής:

ITIL (IT Infrastructure Library)

Όταν το 1982 η Μάργκαρετ Θάτσερ αντιμετώπισε την κρίση των νησιών Φώκλαντ δυσανασχέτησε (κατά κόρο) με την χαμηλή απόδοση των μηχανογραφικών υπηρεσιών του Βρετανικού κράτους, με αποτέλεσμα να διατάξει την άμεση κατάρτιση τμήματος προς βελτίωση της κατάστασης. Το αποτέλεσμα ήταν η θέσπιση της μεθόδου *ITIL*. Μετά από πολυετή μελέτη και καταγραφή δημοσιεύθηκε το 1989-96 με το όνομα **ITIL V1** (αγγλ. **η βιβλιοθήκη *ITIL, έκδοση Α΄*)** που αποτελείτο από 30 και πλέον τόμους.

Η μέθοδος ITIL αναπτύχθηκε στην δεκαετία του 1980 από την υπηρεσία *Central Computing and Telecommunications Agency* (CCTA), η οποία μέχρι το 2010 ονομάζονταν *Office of Government Commerce* (OGC) και σήμερα *Cabinet Office*. Μεταξύ 1989 και 1998 συγκεντρώθηκαν συνολικά 34 βιβλία που αργότερα εκδόθηκαν υπό την ονομασία Version 1. Ακολούθησαν επιμελημένες εκδόσεις από το 1999 ως το 2003 που ονομάστηκαν Version 2, και από το 2007 η νέα ITIL V3.

Το ITIL κυκλοφορεί σήμερα (*V3, έκδοση Γ΄*) σε πέντε τόμους:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement (CSI)

Η IT Infrastructure Library απευθύνεται σε άτομα και επιχειρήσεις που είναι υπεύθυνα για τον σχεδιασμό, την παρακολούθηση και διαχείριση υψηλών ποιότητας υπηρεσιών της πληροφορικής. Η μέθοδος περιγράφει σε ένα σύνολο βιβλίων, κυρίως τις διαδικασίες και τους ρόλους, καθώς και το τι πρέπει να γίνει και όχι πως πρέπει να γίνει. Είναι κατάλληλη για

οργανισμούς κάθε μεγέθους, είτε του δημόσιου είτε του ιδιωτικού τομέα, και χρησιμοποιείται σήμερα σε όλο τον κόσμο.

Το έργο που περιγράφεται στην βιβλιοθήκη ITIL ως «Best Practices», με επίκεντρο την βελτίωση λειτουργίας των υπηρεσιών πληροφορικής για σταθερές οικονομικές επιδόσεις μιας επιχείρησης, σκοπεύει σε:

- Υποστήριξη για την ανάπτυξη μεθόδων, διαδικασιών και οδηγιών εργασίας.
- Αύξηση της παραγωγικότητας και μόχλευση της γνώσης και της εμπειρίας.
- Αύξηση της ικανοποίησης των πελατών.
- Ποιοτικό σύστημα διαχείρισης των IT υπηρεσιών.
- Βελτίωση της επικοινωνίας και ενημέρωσης μεταξύ του προσωπικού και των πελατών του.
- Αύξηση της ικανοποίησης των εργαζομένων και μείωση του κύκλου εργασιών του προσωπικού.

Η εφαρμογή της μεθόδου ITIL αποτελεί προϋπόθεση για την πελατοκεντρική αυτοματοποίηση των διαδικασιών και υπηρεσιών της πληροφορικής. Η ITIL παίζει επίσης σε διεθνές επίπεδο για την υποστήριξη εξωτερικών αναθέσεων ένα ολοένα και πιο σημαντικό ρόλο, αφού οι υπηρεσίες πληροφορικής δεν παράγονται πλέον σε τοπικό επίπεδο, αλλά σε ένα διεθνές δίκτυο από διαφορετικές εταιρείες με διαφορετικές κουλτούρες και ικανότητες. Κεντρικό στοιχείο όμως, που παραμένει σε ολόκληρη την αλυσίδα του δικτύου, είναι η σωστή εξυπηρέτηση των αναγκών του πελάτη.

Ως υπηρεσία σύμφωνα με την μέθοδο ITIL εννοείται η παροχή προστιθέμενης αξίας από τους Παρόχους Τεχνολογίας Πληροφοριών και Επικοινωνίας χωρίς ο παραλήπτης να επιβαρύνεται με επιπλέον κόστος ή με την ανάληψη κινδύνων σε περίπτωση μη εκπλήρωσης.

COBIT (Control Objectives for Information and related Technology)

Τα πλεονεκτήματα της βέλτιστης χρήσης των πληροφοριακών συστημάτων για την επίτευξη υψηλής αξίας προς ένα οργανισμό έχουν πολλαπλώς αναγνωριστεί στην εποχή μας. Η σημαντική αλληλεπίδραση μεταξύ επιχειρησιακών διαδικασιών και συστημάτων πληροφορικής, η ανάγκη συμμόρφωσης με νομικές / κανονιστικές απαιτήσεις και τα πλεονεκτήματα μια αποτελεσματικής προσέγγισης διαχείρισης κινδύνων αποτελούν χαρακτηριστικά των σύγχρονων επιχειρήσεων. Στην προσπάθειά του να υποστηρίξει τις προκλήσεις αυτές ο ISACA, σε συνεργασία με το IT Governance Institute® (ITGI) έχει δημιουργήσει το πρότυπο COBIT®, το οποίο βρίσκεται στην έκδοση 4.1.

Το πρότυπο COBIT καλύπτει όλες τις ανάγκες ελέγχου πληροφοριακών συστημάτων που περιέχονται στο πλαίσιο του συστήματος εσωτερικού ελέγχου COSO και αποτελεί κοινό σημείο αναφοράς για οποιονδήποτε επαγγελματία του οποίου οι υποχρεώσεις και οι αρμοδιότητες απαιτούν την αναγνώριση και αντιμετώπιση των κινδύνων που απορρέουν από τη χρήση των πληροφοριακών συστημάτων.

Οι διοικήσεις των εταιρειών αξιοποιούν το πρότυπο COBIT ώστε να επιτύχουν επιπρόσθετη αξία στις επενδύσεις στα πληροφοριακά συστήματα, καθώς επίσης και για να εξισορροπήσουν τους κινδύνους με τις απαιτούμενες δικλείδες ασφαλείας. Τα ανώτερα στελέχη των επιχειρήσεων και των οργανισμών αναγνωρίζουν την ανάγκη της συμμόρφωσης με το πρότυπο COBIT, ώστε να διασφαλίσουν την αποδεκτή διαχείριση και τον επαρκή έλεγχο των υπηρεσιών της πληροφορικής. Τα στελέχη των διευθύνσεων της πληροφορικής λειτουργούν σύμφωνα με το πρότυπο COBIT, ώστε να εγγυώνται τις απαραίτητες υπηρεσίες, σύμφωνα με τις επιχειρησιακές ανάγκες. Κάθε ελεγκτής πληροφοριακών συστημάτων οφείλει να γνωρίζει επαρκώς το πρότυπο COBIT για τη διαμόρφωση και την τεκμηρίωση της επαγγελματικής του γνώμης σε σχετικά θέματα.

Τα βασικά συστατικά του προτύπου COBIT, είναι τα ακόλουθα:

- CobiT Framework
- Control Objectives
- Management Guidelines
- Maturity Models

ISO 27001

Το ISO 27001: 2013 αποτελεί το μόνο επιθεωρημένο Διεθνές Πρότυπο για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Το πρότυπο αυτό απαιτεί από τις επιχειρήσεις να αξιολογούν τους

κινδύνους για τις πολύ σημαντικές πληροφορίες που διαθέτουν και να επιλέξουν τους κατάλληλους ελέγχους ασφαλείας για τον περιορισμό των κινδύνων αυτών. Το πρότυπο αυτό παρέχει επίσης και μια λίστα με τους ελέγχους ασφαλείας που πρέπει να χρησιμοποιούν οι επιχειρήσεις. Το ISO 27002 παρέχει οδηγίες σχετικά με την εφαρμογή των διαδικασιών ασφαλείας που αναφέρονται στο πρότυπο ISO 27001: 2013. Το ISO 27001: 2013 δίνει τη δυνατότητα στις επιχειρήσεις να ενσωματώνουν διάφορες απαιτήσεις από πολλαπλούς κανονισμούς (π.χ. SOX, HIPAA) σε ένα ενιαίο Σύστημα Διαχείρισης Ασφάλειας των Πληροφοριών (ISMS) και όχι να διαχειρίζονται πολλαπλά μεμονωμένα συστήματα.

Το ISO 27001:2013 μπορεί να εφαρμοστεί απ' όλους τους τύπους των επιχειρήσεων, ανεξάρτητα από το μέγεθος, την πολυπλοκότητα και τη γεωγραφική τους θέση. Αυτό είναι ιδιαίτερα σημαντικό για τις επιχειρήσεις που ασχολούνται με εμπιστευτικές πληροφορίες, συμπεριλαμβανομένων των τραπεζικών και των χρηματοπιστωτικών επιχειρήσεων, οργανισμών υγειονομικής περίθαλψης, ναυτιλιακών επιχειρήσεων και εταιρειών υπηρεσιών πληροφορικής.

4.3.5 Σχεδιασμός Μέτρων Ασφαλείας

Η φάση αυτή αφορά την βασική υλοποίηση του Σχεδίου Ασφαλείας με τον σχεδιασμό των μέτρων που θα ικανοποιήσουν τις απαιτήσεις ασφαλείας του συστήματος.

Τα μέτρα που σχεδιάζονται θα καλύπτουν τις παρακάτω βασικές κατηγορίες:

- Οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος
- Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος
- Φυσική ασφάλεια
- Ασφάλεια δεδομένων
- Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής

Τα μέτρα που αφορούν την οργάνωση και τη διαχείριση του Π.Σ. πιο συγκεκριμένα αφορούν τον σχεδιασμό της ασφάλειας του Π.Σ., τον κώδικα δεοντολογίας του οργανισμού, μέτρα ως προς τον έλεγχο και την εποπτεία της ασφάλειας του Π.Σ. αλλά και ως προς τους ρόλους και τις αρμοδιότητες για την διαχείριση της ασφάλειας. Επίσης, περιλαμβάνει και μέτρα για τη εκπαίδευση και ενημέρωση των χρηστών για τις διαδικασίες και γενικότερα για τις λειτουργίες σχετικά με την ασφάλεια του Π.Σ.

Τα μέτρα που αφορούν την ασφάλεια ανάπτυξης και την συντήρηση του Π.Σ. περιλαμβάνουν μέτρα ανάπτυξης και συντήρησης εφαρμογών (Application development and maintenance), μέτρα διαχείρισης και υποστήριξης υλικού και λογισμικού από προμηθευτές (Vendor support-contracts reliability), καθώς και μέτρα απογραφής του υλικού και λογισμικού και διαχείρισης των αλλαγών (hardware and software inventory).

Μέτρα για την φυσική ασφάλεια αποτελούν τα μέτρα για την ασφάλεια των κτιριακών εγκαταστάσεων, του εξοπλισμού πληροφορικής αλλά και της τηλεπικοινωνιακής υποδομής όπως και μέτρα ως προς τις φυσικές καταστροφές.

Άλλη μια σημαντική κατηγορία μέτρων είναι αυτή για την ασφάλεια των δεδομένων και περιλαμβάνει τους μηχανισμούς εξασφάλισης της ακεραιότητας και της εμπιστευτικότητας των δεδομένων και τα μέτρα για την κατηγοριοποίηση και ταξινόμηση των δεδομένων (Classification of data).

Όσον αφορά την ασφάλεια υπολογιστικής και τηλεπικοινωνιακής υποδομής εδώ συγκαταλέγονται τα εξής: οι διαδικασίες διαχείρισης εφεδρικών αντιγράφων ασφαλείας, οι διαδικασίες αντιμετώπισης ιών, οι διαδικασίες διαχείρισης συνθηματικών και έλεγχου προσπέλασης στα Π.Σ. καθώς και καταγραφής παραβιάσεων. Επίσης, και όλα τα μέτρα για την ασφάλεια των εφαρμογών, των βάσεων δεδομένων , των δικτύων καθώς της ασφάλειας κατά της σύνδεσης στο διαδίκτυο.

4.3.6 Τρόποι Ασφαλείας σε Υλικό - Λογισμικό - Δεδομένα

Κατά καιρούς έχουν προταθεί διάφορα μοντέλα ασφάλειας ενός πληροφοριακού συστήματος. Τα μοντέλα αυτά χρησιμοποιούνται στη συνέχεια ως βάση για τη δημιουργία των μηχανισμών και των μέτρων προστασίας. Στη συνέχεια αναφέρονται τα πιο γνωστά από τα μοντέλα αυτά.

- Μοντέλο του Κιβωτισμού
- Μοντέλο του Καταλόγου

- Μοντέλο του Πίνακα
- Μοντέλο του Φίλτρου
- Μοντέλο των Επάλληλων Στρωμάτων

Το μοντέλο του κιβωτισμού έχει το πλεονέκτημα ότι στα διάφορα περιβλήματα μπορούμε να δώσουμε διάφορα ονόματα (φυσική ασφάλεια, λογική ασφάλεια, κ.λ.π.), οπότε έχουμε ένα μοντέλο με ευρεία εφαρμογή. Όμως έχει δύο σημαντικά μειονεκτήματα:

- Πιστή τήρηση των μέτρων προφύλαξης σε ένα επίπεδο δίνει την εντύπωση ότι μπορεί να δώσει απόλυτη ασφάλεια σε ολόκληρο το σύστημα.
- Είναι ένα στατικό μοντέλο, αφού δεν προβλέπει κάτι, ούτε στηρίζεται στις υπάρχουσες σχέσεις αλληλεξάρτησης μεταξύ των στοιχείων του συστήματος.

Τόσο το μοντέλο του καταλόγου όσο και αυτό του πίνακα δίνουν έμφαση στις πρακτικές πλευρές εφαρμογής των μέτρων ασφάλειας, χωρίς να φωτίζουν την σχέση των μέτρων και των συνθηκών απειλής. Το μειονέκτημα αυτό φαίνεται να αμβλύνεται στο μοντέλο του φίλτρου. Όμως, και τα τρία αυτά μοντέλα εξακολουθούν να εξετάζουν το σύστημα στατικά. Το μοντέλο των επάλληλων στρωμάτων δέχεται ότι η ασφάλεια είναι πολυπαραγοντική και με αλληλεπιδράσεις και αντιμετωπίζει το θέμα με μία συστηματική διαδικασία, δηλαδή με καλά διατεταγμένα και ακριβώς ορισμένα βήματα μετάβασης από επίπεδο σε επίπεδο. Όμως είναι γνωστό ότι η συστηματική προσέγγιση, ειδικά στην ανάπτυξη πληροφοριακών συστημάτων δεν δίνει πάντα ικανοποιητικά αποτελέσματα. Η προσέγγιση αυτή θα πρέπει να συμπληρωθεί ώστε να αμβλυνθούν τα μειονεκτήματα που παρουσιάζει.

4.3.7 Σχέδιο ανάκαμψης από καταστροφές (Disaster Recovery Plan)

Το Σχέδιο Ανάκαμψης από Καταστροφές συμπληρώνει το σχέδιο ασφαλείας, καταγράφοντας τις διαδικασίες και υλοποιώντας μέτρα που εξασφαλίζουν την εταιρεία στην αντιμετώπιση τέτοιας έκτασης καταστροφών που ουσιαστικά είναι αδύνατη η άμεση (ή έστω εντός λίγων ωρών ή/και ημερών) επαναλειτουργία του πρωτεύοντος πληροφοριακού συστήματος. Αφορά δύο βασικές κατηγορίες:

α) περιπτώσεις δυσλειτουργίας

β) περιπτώσεις ολικής καταστροφής.

Το Σχέδιο Ανάκαμψης από Καταστροφές θα πρέπει να περιλαμβάνει:

- Προσδιορισμό πιθανών κινδύνων και κριτηρίων για ενεργοποίηση του σχεδίου. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον οργανισμό σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν ανάκληση του σχεδίου.

- Προσδιορισμό των σημαντικών λειτουργιών και των αντίστοιχων συστημάτων (critical functions and systems) της εταιρείας,

- Καθορισμό της στρατηγικής προστασίας (protection strategy),

- Ιεράρχηση των δραστηριοτήτων και καθορισμός προτεραιοτήτων για την ενεργοποίησή τους στο εναλλακτικό σύστημα,

- Πλάνο Υλοποίησης με αρμοδιότητες προσωπικού και χρονοπρογραμματισμό ενεργειών αποκατάστασης. Το σχέδιο πρέπει να περιέχει μια κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν από την επιχείρηση για τη συνέχιση της λειτουργίας της.

Το Σχέδιο Ανάκαμψης από Καταστροφές θα πρέπει να πραγματεύεται και την ανάκαμψη της λειτουργίας της υπολογιστικής και επικοινωνιακής υποδομής μετά από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κτλ.). Επιπλέον, εκτός από το λεπτομερειακό σχέδιο αποκατάστασης λειτουργίας της εταιρείας, δύναται να εκπονηθεί ένα σχέδιο ανάκαμψης από καταστροφή που θα προβλέπει και εφεδρική εγκατάσταση (disaster recovery facility), ενώ εξετάζεται και το θέμα της διάθεσης εναλλακτικής τοποθεσίας (alternate site).

4.4 Υλοποίηση Ασφαλείας

4.4.1 Έλεγχος Πρόσβασης Χρηστών

Στόχος είναι να εξασφαλισθεί η προσπέλαση από εξουσιοδοτημένους χρήστες και

να προληφθεί η μη-εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα. Θα πρέπει να υπάρχουν αυστηρές διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα πληροφοριακά συστήματα και τις υπηρεσίες. Οι διαδικασίες αυτές θα πρέπει να καλύπτουν ολόκληρο τον κύκλο της πρόσβασης των χρηστών, από την αρχική δήλωση του χρήστη στο σύστημα, μέχρι και τη διαγραφή του από αυτό. Ειδική προσοχή απαιτείται στον καθορισμό των δικαιωμάτων των χρηστών, ώστε να μην μπορούν να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος. Προτεινόμενα μέτρα:

- Διαδικασία εγγραφής χρηστών
- Διαχείριση προνομίων χρηστών
- Διαχείριση διαπιστευτηρίων (credentials) των χρηστών
- Επιθεώρηση προνομίων των χρηστών

4.4.2 Προσπέλαση - Επεξεργασία δεδομένων

Σκοπός είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες που χρησιμοποιούνται από τις διάφορες εφαρμογές. Θα πρέπει να χρησιμοποιούνται ειδικά μέσα ασφάλειας για τον περιορισμό της πρόσβασης στις εφαρμογές. Η λογική πρόσβαση σε λογισμικό και πληροφορίες εφαρμογών θα πρέπει να περιορίζεται μόνο στους εξουσιοδοτημένους χρήστες. Οι εφαρμογές θα πρέπει να:

- Ελέγχουν την πρόσβαση των χρηστών σε διάφορες πληροφορίες και λειτουργίες των
- εφαρμογών, σύμφωνα με την καθορισμένη πολιτική ελέγχου πρόσβασης του οργανισμού,

- Παρέχουν προστασία από μη εξουσιοδοτημένη προσπέλαση μέσω οποιασδήποτε υπηρεσίας, λογισμικού λειτουργικού συστήματος και κακόβουλου λογισμικού, που είναι ικανά να παρακάμψουν τα μέτρα προστασίας του συστήματος,

- Μην διακυβεύουν την ασφάλεια άλλων συστημάτων, με τα οποία διαμοιράζονται

4.4.3 Προστασία Βάσεων Δεδομένων

Όσον αφορά την ασφάλεια βάσεων δεδομένων, θα πρέπει να λαμβάνεται υπ' όψιν ότι η βάση δεδομένων είναι ένα σύστημα που εκτελείται σε έναν υπολογιστή, πάνω από ένα λειτουργικό σύστημα, και έτσι επηρεάζεται άμεσα από τους μηχανισμούς ασφάλειας που παρέχει ο συνδυασμός αυτός υλικού/λογισμικού. Αν για παράδειγμα το λειτουργικό σύστημα δεν παρέχει επαρκείς μηχανισμούς διακρίβωσης ταυτότητας, η βάση δεδομένων θα πρέπει να υλοποιήσει δικούς της. Επίσης, αν η βάση δεδομένων αποθηκεύεται σε αρχεία που δεν προστατεύονται επαρκώς από το λειτουργικό σύστημα, οι μηχανισμοί ελέγχου πρόσβασης που υλοποιούνται από τη βάση δεδομένων μπορούν να παρακαμφθούν, απλά διαβάζοντας ή τροποποιώντας τα αρχεία σε επίπεδο λειτουργικού συστήματος.

Βασικοί κανόνες για την προστασία των βάσεων είναι ότι τόσο κατά τη φάση της επεξεργασίας των πληροφοριών όσο και κατά τη φάση της μετάδοσης πρέπει αφενός να εκτελεστούν στο σύνολο τους όλες οι δοσοληψίες και αφετέρου ότι να εφαρμόζονται όλοι οι κανόνες ακεραιότητας που έχουν ορισθεί για τη βάση δεδομένων.

Σε γενικές γραμμές μία βάση δεδομένων θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών την παρέχοντα πρόσβαση σε εξουσιοδοτημένους χρήστες, την ακεραιότητα των πληροφοριών της καθώς και την διαθεσιμότητα τους. Η εμπιστευτικότητα των πληροφοριών επιτυγχάνεται με τον έλεγχο πρόσβασης στις ΒΔ, ώστε να διαπιστώνεται αν ένας χρήστης έχει το δικαίωμα να χρησιμοποιήσει το σύστημα βάσεων δεδομένων ή όχι. Για διακρίβωση της ταυτότητας των χρηστών χρησιμοποιούνται οι παρακάτω τεχνικές:

- **Διακρίβωση ταυτότητας με όνομα χρήστη-συνθηματικό.**
  Η βάση δεδομένων διαθέτει κατάλογο με τις έγκυρες αντιστοιχίες ονομάτων χρηστών και συνθηματικών ώστε να αποφασίζει για το αν τα παρουσιασθέντα διαπιστευτήρια είναι έγκυρα. Η τεχνική

αυτή είναι χρήσιμη όταν το λειτουργικό σύστημα δεν παρέχει αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας των χρηστών ή όταν πραγματοποιούνται συνδέσεις μέσω δικτύου στη βάση δεδομένων, οπότε η ταυτότητα του χρήστη στο λειτουργικό σύστημα δεν είναι διαθέσιμη ή αξιόπιστη.

- **Διακρίβωση ταυτότητας από το λειτουργικό σύστημα.**
  Σ' αυτή την περίπτωση η πρόσβαση στην ΒΔ στηρίζεται στους μηχανισμούς του λειτουργικού συστήματος για την διακρίβωση ταυτότητας. Από τη στιγμή που ένας χρήστης έχει αναγνωριστεί από το λειτουργικό σύστημα και ο χρήστης λειτουργικού συστήματος είναι εξουσιοδοτημένος να χρησιμοποιεί τη βάση δεδομένων, δεν ζητάται κανένα πρόσθετο στοιχείο για την προσπέλαση του χρήστη στη βάση δεδομένων. Η τεχνική αυτή δεν μπορεί να χρησιμοποιείται ως αποκλειστικός μηχανισμός διακρίβωσης ταυτότητας σε συστήματα όπου επιτρέπεται δικτυακή πρόσβαση στη βάση δεδομένων, καθώς χρειάζεται κάθε χρήστης να έχει λογαριασμό στο λειτουργικό σύστημα. Επίσης, πρέπει να χρησιμοποιείται μόνον όταν το λειτουργικό σύστημα έχει επαρκώς αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας.

- **Διακρίβωση ταυτότητας μέσω καθολικών υπηρεσιών καταλόγου.**
  Ο χρήστης εισάγει ένα όνομα και ένα συνθηματικό και για διακρίβωση του το σύστημα διασυνδέεται με καθολικές υπηρεσίες καταλόγου. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι προωθεί τη χρήση κεντρικού σημείου φύλαξης των διαπιστευτηρίων σύνδεσης. Έχοντας ένα κεντρικό σημείο φύλαξης, είναι δυνατόν όλες οι ενότητες λογισμικού που απαιτούν πιστοποίηση (λειτουργικό σύστημα, βάση δεδομένων κ.λπ.) να συνδιαλέγονται με το σημείο αυτό, ούτως ώστε κάθε χρησιμοποιεί ένα μόνο ζεύγος διαπιστευτηρίων για προσπέλαση σε όλους τους πόρους.

Η ακεραιότητα των δεδομένων στα συστήματα βάσεων δεδομένων αποτελεί βασική προϋπόθεση για αυτό και τα δεδομένα πρέπει να διασώζονται σε περιπτώσεις βλαβών υλικού και δυσλειτουργιών του λογισμικού, οι τροποποιήσεις πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και κάθε φορά να επιστρέφονται τα δεδομένα που έχουν αποθηκευτεί. Σε περίπτωση παραβίασης της ακεραιότητας, οι ενδιαφερόμενοι χρήστες πρέπει τουλάχιστον να ειδοποιούνται.

Η φυσική ακεραιότητα της βάσης δεδομένων συσχετίζεται με τη φθορά που μπορούν να υποστούν τα μαγνητικά μέσα αποθήκευσης από διακοπές ρεύματος, βλάβες κυκλωμάτων ή φυσιολογική φθορά. Το σύστημα θα πρέπει να παρέχει μηχανισμούς ανάκαμψης από το σφάλμα και ανάκτησης των δεδομένων. Ένα τρόπος διαφύλαξης της φυσικής ακεραιότητας είναι η τήρηση εφεδρικών αντιγράφων. Για τα εφεδρικά αντίγραφα είναι σημαντικό να μπορούν να λαμβάνονται ενόσω η βάση δεδομένων βρίσκεται εν λειτουργία.

4.4.4 Προστασία Δικτύων

Στόχος είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης στις δικτυακές υπηρεσίες. Η πρόσβαση σε εσωτερικές αλλά και σε εξωτερικές δικτυακές υπηρεσίες θα πρέπει να είναι ελεγχόμενη. Αυτό είναι απαραίτητο προκειμένου να εξασφαλισθεί ότι οι χρήστες των δικτυακών υπηρεσιών δεν μπορούν να απειλήσουν την ασφάλεια αυτών των υπηρεσιών. Για αυτό θα πρέπει να εξασφαλισθεί ότι:

- Υπάρχουν οι κατάλληλες διεπαφές (interfaces) μεταξύ του δικτύου του οργανισμού και των δικτύων άλλων οργανισμών ή δημόσιων δικτύων.

- Υπάρχουν κατάλληλοι μηχανισμοί αυθεντικοποίησης χρηστών και εξοπλισμού.

- Επιβάλλεται ελεγχόμενη πρόσβαση των χρηστών στις προσφερόμενες υπηρεσίες.

Η χωρίς προστασία παροχή υπηρεσιών επιτρέπει την εκμετάλλευση πιθανών υπαρκτών αδυναμιών από τρίτους, με σκοπό την παραβίαση της ασφάλειας. Για το λόγο αυτό, κρίνεται απαραίτητη η υλοποίηση εξειδικευμένων μηχανισμών ασφάλειας όπως Firewall, Web

Access Systems, Mail Security Systems, Network IPS/IDS.

Η εταιρεία εξασφαλίζει την προστασία των δικτύων της μέσω ενός ολοκληρωμένου πακέτου ασφαλείας το End Point Security System, το οποίο στοχεύει στην υλοποίηση υπηρεσιών ασφάλειας στην πύλη του δικτύου (Gateway Security) από και προς το διαδίκτυο. Οι βασικές υπηρεσίες ασφαλείας είναι:

- Firewall
- Antivirus
- Antispyware
- Antispam
- URL Filtering
- DMZ (De Military Zone)
- Intrusion Detection / Prevention Systems

4.5 Εφαρμογή του προτύπου ISO 27001 στη Ναυτιλία

4.5.1 Πλεονεκτήματα του προτύπου ISO 27001

Το ISO 27001:2013 είναι ένα διεθνώς αναγνωρισμένο πρότυπο το οποίο προσδιορίζει τις προδιαγραφές για την διαχείριση της ασφάλειας των πληροφοριών. Μπορεί να χρησιμοποιηθεί από εταιρίες, που επιθυμούν να εγκαταστήσουν και να βελτιώσουν την ασφαλή διαχείριση των δεδομένων τους και των πελατών τους. Μερικά από τα πλεονεκτήματα από την εφαρμογή και την πιστοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών βάσει του ISO 27001 είναι:

- Εξασφαλίζει συμμορφώσεις σε μια σειρά απαιτούμενων κανονισμών, όπως HIPAA, FISMA, GLBA, κ.λπ.
- Καθιερώνει απαιτούμενους γενικούς ελέγχους που απαιτούνται για επιθεωρήσεις τύπου SOX, SSAE16.
- Αναγνωρίζεται παγκοσμίως ως ένα πρότυπο για τη Διαχείριση Ασφάλειας των Πληροφοριών (ISMS).
- Μπορεί να εφαρμοστεί απ’ όλες τις επιχειρήσεις ανεξαρτήτως μεγέθους, είδους ή φύσης.
- Η συνεχής αξιολόγηση βοηθά στην διατήρηση της αποτελεσματικότητας των ελέγχων ασφαλείας.
- Αυξάνει την εμπιστοσύνη των πελατών.
- Παρέχει τη δυνατότητα γρήγορου εντοπισμού και απομόνωσης οποιωνδήποτε παραβιάσεων ασφαλείας.

4.5.2 Σχεδιασμός ISMS

Η ναυτιλιακή επιχείρηση πρέπει να κάνει τις εξής κινήσεις:

- Να καθορίσει το αντικείμενο και τα όρια του ISMS από πλευράς χαρακτηριστικών της επιχείρησης, της θέσης της, των στοιχείων τεχνολογίας καθώς και να συμπεριλάβει τυχόν λεπτομέρειες εξαιρέσεων από το αντικείμενο, τις οποίες θα αιτιολογήσει.

- Να καθορίσει πολιτική ISMS βασισμένη στα χαρακτηριστικά της επιχείρησης, στη θέση της, στο ενεργητικό της και στην τεχνολογία της, η οποία:

  - Θα περιλαμβάνει ένα πλαίσιο καθορισμού στόχων και θα καθιερώνει γενικές κατευθύνσεις και αρχές για την ανάληψη δράσης με γνώμονα την ασφάλεια πληροφοριών.

  - Θα λαμβάνει υπόψη τη δουλειά και τις νομικές ή κανονιστικές απαιτήσεις και τις συμβατικές υποχρεώσεις ασφαλείας.

  - Θα ευθυγραμμίζεται με τη στρατηγική διαχείρισης κινδύνων της επιχείρησης, στα πλαίσια της οποίας θα υλοποιηθεί η εγκατάσταση του ISMS.

  - Θα καθορίζει τα κριτήρια με βάση τα οποία θα γίνει αξιολόγηση κινδύνου.

  - Θα έχει λάβει την έγκριση της διοίκησης.

- Να καθορίσει την "προσέγγιση εκτίμησης κινδύνου" με βάση τα εξής:

  - Θα προσδιορίσει μια μεθοδολογία αξιολόγησης κινδύνων, κατάλληλη για το ISMS, για την ασφάλεια των πληροφοριών, για τις νομικές και κανονιστικές απαιτήσεις.

  - Θα ορίσει κριτήρια αποδοχής κινδύνων και θα προσδιορίσει τα επίπεδα αποδοχής τους.

- Να προβεί σε εντοπισμό των κινδύνων ως εξής:
  - Θα εντοπίσει τα περιουσιακά στοιχεία του αντικειμένου εφαρμογής του ISMS καθώς και τους ιδιοκτήτες τους.
  - Θα προσδιορίσει τις απειλές για τα περιουσιακά στοιχεία.
  - Μέσω της ανάλυσης των απειλών θα προσδιορίσει τα τρωτά σημεία που ενδέχεται να προκύψουν.
  - Θα προσδιορίσει τις επιπτώσεις που ενδέχεται να έχει η απώλεια του τριγώνου CIA (Confidentiality - Integrity - Availability) στα περιουσιακά στοιχεία.
- Να αναλύσει και να αξιολογήσει τους κινδύνους (Risk Assessment)
  - Αξιολόγηση των επιπτώσεων που μπορεί να προκύψουν λόγω αποτυχιών στη διαχείριση της ασφάλειας.
  - Αξιολόγηση της ρεαλιστικής πιθανότητας να συμβούν αποτυχίες στη διαχείριση της ασφάλειας δεδομένων των τρωτών σημείων και των υπαρχουσών απειλών.
  - Να αποφασιστεί αν οι κίνδυνοι είναι αποδεκτοί ή αν απαιτούν διορθωτικές ενέργειες με βάση τα κριτήρια αποδοχής τους.
- Να προσδιορίσει και να αξιολογήσει εναλλακτικές επιλογές για την αντιμετώπιση των κινδύνων.
- Να επιλέξει στόχους ελέγχων καθώς και τους ελέγχους για την αντιμετώπιση των κινδύνων.
- Να λάβει την έγκριση της διοίκησης σχετικά με τους προτεινόμενους εναπομείναντες κινδύνους.
- Να λάβει την έγκριση της διοίκησης για την υλοποίηση και λειτουργία του ISMS.
- Να συντάξει Δήλωση Εφαρμοσιμότητας.

4.5.3 Εφαρμογή του ISMS

Η ναυτιλιακή επιχείρηση πρέπει να κάνει τις εξής κινήσεις:

- Να διατυπώσει σχέδιο μείωσης κινδύνου, το οποίο, θα προσδιορίζει την σωστή διαχείριση, τους πόρους, τις ευθύνες και τις προτεραιότητες διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών.
- Να εφαρμόσει το σχέδιο μείωσης κινδύνου προκειμένου να επιτευχθούν οι προκαθορισμένοι στόχοι ελέγχων.
- Να εφαρμόσει τους ελέγχους που έχουν προεπιλεγεί και εγκριθεί ώστε να ικανοποιηθούν οι στόχοι τους.
- Να καθορίσει τον τρόπο μέτρησης της αποτελεσματικότητας των ελέγχων και να προσδιορίσει πως αυτές οι μετρήσεις θα χρησιμοποιηθούν στην παραγωγή συγκρίσιμων αποτελεσμάτων.
- Να εφαρμόσει προγράμματα κατάρτισης και ευαισθητοποίησης.
- Να διαχειρίζεται τη λειτουργία καθώς και τους πόρους του ISMS.
- Να εφαρμόσει διαδικασίες και ελέγχους ικανούς να επιτρέψουν τη γρήγορη ανίχνευση συμβάντων ασφαλείας και την αντιμετώπισή τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ

Πάγκαλου Γ., Μαυρίδη Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ. (2004). Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Κάτσικα Σ. (2001). Ασφάλεια Υπολογιστών (τόμος Α). Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα.

Ξένος, Μ. & Χριστοδουλάκης, Δ. (2002). Εισαγωγή στις βάσεις δεδομένων. Αθήνα: Εκδόσεις Παπασωτηρίου.

"ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements". International Organization for Standardization.

http://www.warandstrategy.gr/kyvernopolemos

https://el.wikipedia.org /wiki/ITIL

http://www.isaca.gr/index.php/en/standards/cobit.html

http://www.accountancygreece.gr

http://www.icte.uowm.gr/uploads/thesis/dipl_ergasia_am14.pdf (Διπλωματική Εργασία της κ. Λέρα Μαρίας, με θέμα: «ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ».)

http://www.tuvaustriahellas.gr

http://www.helmepacadets.gr/gr/shipping/the-role-of-shipping

https://securityreport.gr/magazine-archive/year-2016/item/2925-kyvernoasfaleia-kai-emporiki-naftilia