ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Πολυκριτήρια Αξιολόγηση Μέτρων Ασφάλειας σε Πληροφοριακά Συστήματα Εμπορικών Λιμένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πέτρος Α. Καρατζάς

Επιβλέπων : Ιωάννης Ψαρράς
Καθηγητής Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Πολυκριτήρια Αξιολόγηση Μέτρων Ασφάλειας σε Πληροφοριακά Συστήματα Εμπορικών Λιμένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πέτρος Α. Καρατζάς

Επιβλέπων : Ιωάννης Ψαρράς
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ……..

.....	.....	.....
Ιωάννης Ψαρράς	Δημήτριος Ασκούνης	Βασίλειος Ασημακόπουλος
Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2013

.....
Πέτρος Καρατζάς

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Οι εμπορικοί λιμένες αποτελούν κρίσιμες υποδομές πληροφορικής καθώς φιλοξενούν κρίσιμα πληροφοριακά συστήματα. Διαχειρίζονται μεγάλο αριθμό ευαίσθητων δεδομένων, κρίσιμων πληροφοριών και υπηρεσιών, ενώ καθημερινά εξυπηρετούν μεγάλο αριθμό χρηστών και αλληλεπιδρούν με άλλους φορείς. Οι παραπάνω υποδομές είναι συνεχώς εκτεθειμένες σε ένα μεγάλο αριθμό απειλών και αδυναμιών που μπορούν να βλάψουν την ορθή και αδιάκοπη λειτουργία ενός εμπορικού λιμένα και των οργανισμών του περιβάλλοντος του. Όπως λοιπόν γίνεται κατανοητό, η ανάλυση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος ενός εμπορικού λιμένα είναι σημαντική για την ομαλή λειτουργία και την επίτευξη των επιχειρησιακών στόχων, τόσο του ίδιου του οργανισμού, όσο και των συνεργαζόμενων με αυτόν φορέων.

Η παρούσα διπλωματική εργασία επικεντρώνεται στο στάδιο της θεραπείας κινδύνου, της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων, με στόχο την αξιολόγηση και επιλογή των κατάλληλων μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων.

Ωστόσο η σύγκριση και τελική επιλογή των μέτρων προστασίας δεν αποτελεί μονοδιάστατο πρόβλημα, αλλά ένα πολύπλοκο σύγχρονο πρόβλημα απόφασης που συνίσταται από πολλαπλά κριτήρια. Η ύπαρξη πολλαπλών κριτηρίων καθιστά τον τρόπο συλλογής, επεξεργασίας και αξιοποίησης της πληροφορίας αρκετά πιο σύνθετο και διαφορετικό, σε σχέση με εκείνον των μονοκριτήριων αναλύσεων, ωστόσο προσφέρει μεγαλύτερη ευελιξία και προοπτικές στον αποφασίζοντα διότι εξετάζονται περισσότερες διαστάσεις. Το εργαλείο που θα εξυπηρετήσει την επίτευξη του στόχου της παρούσας διπλωματικής είναι η πολυκριτήρια ανάλυση, η οποία αποτελεί ένα ευρέως χρησιμοποιούμενο και διαδεδομένο εργαλείο για την υποστήριξη αποφάσεων μέσα από τη συστηματική εξαγωγή τεκμηριωμένων επιλογών.

Συγκεκριμένα για τη σύγκριση και αξιολόγηση των μέτρων ασφάλειας προτείνεται η εφαρμογή μιας πολυκριτήριας προσέγγισης που στηρίζεται στη θεωρία του συναινετικού προγραμματισμού. Η αξιολόγηση των εναλλακτικών δράσεων στηρίζεται σε ένα σύστημα έντεκα κριτηρίων που είναι βασισμένο στους παρακάτω άξονες προτίμησης: α) εφικτότητα, β) αειφορία, γ) συντήρηση και δ) επιπτώσεις-αποτελεσματικότητα. Η εφαρμογή της προτεινόμενης μεθοδολογίας παρουσιάζεται μέσα από τη μελέτη μιας περίπτωσης όπου δίνεται βαρύτητα στα κριτήρια που αφορούν στο κόστος υλοποίησης ενός συνδυασμού μέτρων ασφάλειας και στο επίπεδο επικινδυνότητας.

Τέλος, οι εναλλακτικές δράσεις-μέτρα απεικονίζονται γραφικά, έτσι ώστε οι ορατές κατά Pareto βέλτιστες λύσεις να είναι κατανοητές και άμεσα εκμεταλλεύσιμες από τους ενδιαφερόμενους –αποφασίζοντες.

Λέξεις Κλειδιά: Πληροφοριακά συστήματα, Μέτρα ασφάλειας, Πολυκριτήρια ανάλυση, Λήψη αποφάσεων, Υποστήριξη αποφάσεων, Συναινετικός προγραμματισμός

Abstract

Commercial harbours constitute critical IT infrastructures as they accommodate crucial information systems. They manage large amounts of sensitive data and significant services and information, while serving and interacting with a great number of users and bodies daily. The above infrastructures are constantly exposed to a large number of threats and vulnerabilities that can harm the proper and continuous functioning of a commercial harbour and the bodies of its environment. Hence, the safety and protection of a commercial harbour's information system is important for its normal operation and the attainment of its business goals, not only regarding the harbour itself but also bodies cooperating with it.

This paper focuses on the risk treatment stage, of risk analysis and management process, aiming at the evaluation and selection of the appropriate security measures in commercial harbors' information systems.

However, the comparison and final choice of safety measures is not a one-dimensional problem, but a modern complex decision problem consisting of multiple criteria. The existence of multiple criteria makes the collection, processing and utilization of information far more complex and different than that of one-dimensional analyzes, however, offers more flexibility and perspectives to the decision-maker as examined more dimensions. The tool that will serve the objective of this paper is the multicriteria analysis, which is a widely used and popular tool for decision support through the systematic extraction of documented choices.

Specifically, for the overall evaluation and comparison of safety measures is proposed the implementation of a multicriteria approach based on the theory of compromise programming. The alternative operations are evaluated over a system of eleven criteria consisting of four points of view: (a) feasibility, (b) sustainability, (c) maintenance, and (d) impact – efficacy. The application of the suggested methodology is presented in a form of a case study where emphasis is placed on the criteria regarding the implementation cost of a combination of safety measures and the level of risk.

In the end, the alternative operations are illustrated graphically so as the visualized Pareto optimal solutions would be easily comprehensible and directly accessible to related stakeholders - decision makers.

Keywords: Information systems, Safety measures, Multicriteria analysis, Decision making, Decision Support, Compromise programming

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά το ακαδημαϊκό έτος 2012-2013 στον τομέα Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Αρχικά θα ήθελα να ευχαριστήσω τον καθηγητή κ. Ιωάννη Ψαρρά για την ανάθεση της διπλωματικής και την δυνατότητα που μου δόθηκε να ασχοληθώ με έναν τόσο ενδιαφέροντα τομέα, καθώς και τον καθηγητή κ. Ιωάννη Σίσκο για την πολύτιμη καθοδήγηση που μου παρείχε κατά την εκπόνηση της εργασίας.

Επίσης, ιδιαίτερες ευχαριστίες οφείλω στον υποψήφιο διδάκτορα Λευτέρη Σίσκο και τον κ. Θεόδωρο Ντούσκα, η βοήθεια και η υποστήριξη των οποίων ήταν σημαντική κατά την εκπόνηση της διπλωματικής.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την υποστήριξη που μου παρείχαν καθ' όλη τη διάρκεια των σπουδών μου.

Αθήνα, Δεκέμβριος 2013

Πέτρος Καρατζάς

Περιεχόμενα

Εικόνες – Πίνακες - Γραφήματα

1ο ΚΕΦΑΛΑΙΟ

Εισαγωγή

1 Εισαγωγή

1.1 Σκοπός-αντικείμενο διπλωματικής εργασίας

Τα σημερινά πληροφοριακά συστήματα των εμπορικών λιμένων διαχειρίζονται κρίσιμα και ευαίσθητα δεδομένα, προσφέρουν πληθώρα και διαφορετικής φύσης ηλεκτρονικές υπηρεσίες, αλληλεπιδρούν με πληροφοριακά συστήματα άλλων οργανισμών και εξυπηρετούν μεγάλο αριθμό χρηστών. Επομένως, για την ομαλή λειτουργία των εμπορικών λιμένων είναι επιβεβλημένη η διαχείριση της ασφάλειας των πληροφοριακών τους συστημάτων και κατά συνέπεια η εφαρμογή των ενδεδειγμένων μέτρων προστασίας που εξασφαλίζουν την αδιάκοπη και σωστή λειτουργία τους.

Στόχος της παρούσας διπλωματικής εργασίας είναι η παρουσίαση μιας μεθοδολογίας για την επιλογή μέτρων ασφαλείας σε πληροφοριακά συστήματα εμπορικών λιμένων. Η σύγκριση και αξιολόγηση των μέτρων ασφάλειας είναι ένα πολυδιάστατο πρόβλημα που συνίσταται από πολλαπλά κριτήρια. Για το λόγο αυτό, το εργαλείο που χρησιμοποιείται για την επίλυση του παραπάνω προβλήματος είναι η πολυκριτήρια ανάλυση, η οποία συμβάλει στην αξιοποίηση όλων των διαθέσιμων πληροφοριών ώστε να διευκολυνθεί το έργο του αποφασίζοντα και των υπόλοιπων εμπλεκόμενων στη διαδικασία της απόφασης.

1.2 Φάσεις υλοποίησης

Η διπλωματική εργασία εκπονήθηκε το διάστημα Δεκέμβριος 2012 – Αύγουστος 2013. Η υλοποίηση της πραγματοποιήθηκε σε πέντε φάσεις οι οποίες παρουσιάζονται παρακάτω:

Φάση 1^{η}: Ανάληψη διπλωματικής

Αρχικά έγινε μια πρώτη μελέτη της διδακτορικής διατριβής «Συνεργατική, πολυκριτηριακή διαχείριση ασφάλειας Πληροφοριακών Συστημάτων» του Θεόδωρου Ν. Ντούσκα. Το ενδιαφέρον εστιάστηκε στα κεφάλαια που αφορούσαν στην αντιμετώπιση της ανάλυσης και διαχείρισης της επικινδυνότητας ως πολυκριτήριο πρόβλημα και στην διαχείριση της ασφάλειας πληροφοριακών συστημάτων εμπορικών λιμένων. Τελικά αποφασίστηκε η μελέτη της παρούσας διπλωματικής να επικεντρωθεί στο κομμάτι που αφορά στα μέτρα ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων και συγκεκριμένα στην αντιμετώπιση του προβλήματος ως πολυκριτήριο.

Φάση 2η: Παρακολούθηση διαλέξεων του μαθήματος «Πολυκριτηριακά συστήματα υποστήριξης αποφάσεων» και μελέτη προτύπων διαχείρισης ασφάλειας πληροφοριακών συστημάτων

Το επόμενο στάδιο μετά την ανάληψη της διπλωματικής ήταν η παρακολούθηση του μαθήματος «Πολυκριτηριακά συστήματα υποστήριξης αποφάσεων» που γίνεται σε επίπεδο διδακτορικού από τους καθηγητές Ι. Σίσκο (ΠΑ.ΠΕΙ) και Ι. Ψαρρά (Ε.Μ.Π.). Η παρακολούθηση των διαλέξεων του μαθήματος είχε ως στόχο την γνωριμία με βασικές έννοιες της πολυκριτήριας ανάλυσης και τα υπάρχοντα μοντέλα αποφάσεων, εφόδια απαραίτητα για την επίλυση του προβλήματος της πολυκριτήριας επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων. Παράλληλα μελετήθηκαν βασικά πρότυπα διαχείρισης ασφάλειας πληροφοριακών συστημάτων.

Φάση 3η: Μοντελοποίηση προβλήματος

Στην τρίτη φάση μελετήθηκε η φύση του προβλήματος της επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων με στόχο την πλήρη κατανόηση του τρόπου που προκύπτει το σύνολο των εναλλακτικών δράσεων, την κατασκευή της συνεπούς οικογένειας κριτηρίων αξιολόγησης των δράσεων και την επιλογή της μεθοδολογίας πολυκριτήριας ανάλυσης που χρησιμοποιήθηκε για την επίλυση του παραπάνω προβλήματος.

Φάση 4η: Μελέτη περίπτωσης

Στη συγκεκριμένη φάση κατασκευάστηκε και μελετήθηκε μια περίπτωση επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων. Μέσα από την μελέτη του παραδείγματος περιγράφηκε η δομή ενός τέτοιου προβλήματος, πραγματοποιήθηκε η επίλυση του με εφαρμογή της προτεινόμενης μεθοδολογίας και έγινε παρουσίαση των τελικών αποτελεσμάτων αξιολόγησης των μέτρων.

Φάση 5η: Συμπεράσματα και προοπτικές.

Στην Πέμπτη και τελευταία φάση εκπόνησης της διπλωματικής εξήχθησαν τα συμπεράσματα από την πολυκριτήρια επιλογή μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων και εξετάστηκαν οι πιθανές προοπτικές επέκτασης του μοντέλου.

1.3 Δομή διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία αποτελείται συνολικά από οχτώ κεφάλαια τα οποία παρουσιάζονται παρακάτω:

- Το παρόν πρώτο κεφάλαιο αποτελεί την εισαγωγή της διπλωματικής εργασίας, όπου παρουσιάζονται το αντικείμενο και ο σκοπός της διπλωματικής, οι φάσεις που ακολουθήθηκαν κατά την εκπόνηση της και αναλύεται το περιεχόμενο των κεφαλαίων της.

- Στο δεύτερο κεφάλαιο της εργασίας παρατίθενται πληροφορίες και στοιχεία που αφορούν στους εμπορικούς λιμένες και συγκεκριμένα στα πληροφοριακά συστήματα που φιλοξενούν. Περιγράφεται δηλαδή η λειτουργία και οι εφαρμογές τους, η κρισιμότητα τους, η ανάγκη προστασίας των αγαθών τους, οι υπηρεσίες που παρέχουν, οι χρήστες που περιλαμβάνουν και οι συνεργαζόμενοι με τους εμπορικούς λιμένες φορείς.

- Στο επόμενο κεφάλαιο περιγράφεται αρχικά ο κύκλος ζωής της ασφάλειας των αγαθών ενός πληροφοριακού συστήματος, δηλαδή παρουσιάζεται ο κύκλος των διεργασιών που πρέπει να ακολουθηθούν για τη λήψη των απαραίτητων μέτρων προστασίας του πληροφοριακού συστήματος. Στην συνέχεια περιγράφονται οι στόχοι και οι κύριες οδηγίες που περιλαμβάνουν ορισμένα βασικά πρότυπα διαχείρισης ασφάλειας πληροφοριακών συστημάτων.

- Το τέταρτο κεφάλαιο αφορά στην ανάλυση και διαχείριση κινδύνου της ασφάλειας πληροφοριακών συστημάτων. Αρχικά παρουσιάζονται οι φάσεις που αποτελούν την εν λόγω διαδικασία, γίνεται αναλυτικότερη περιγραφή της Εκτίμησης Κινδύνου, που είναι η σημαντικότερη φάση της διαδικασίας, ενώ έμφαση δίνεται στο στάδιο της Θεραπείας Κινδύνου, που περιλαμβάνει την επιλογή των μέτρων ασφάλειας πληροφοριακών συστημάτων. Τέλος, παρατίθενται ορισμένες μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων μαζί με κάποια βασικά για την αξιολόγηση τους κριτήρια και γίνεται περιγραφή της συνεργατικής μεθοδολογίας STORM-RM, η οποία αποτέλεσε και αφορμή της συγκεκριμένης διπλωματικής.

- Στο κεφάλαιο που ακολουθεί παρουσιάζονται κύριες έννοιες και βασικά χαρακτηριστικά της πολυκριτήριας λήψης αποφάσεων και περιγράφεται αναλυτικά η διαδικασία μοντελοποίησης προβλημάτων απόφασης. Επιπλέον παρατίθενται ορισμένες κατηγοριοποιήσεις των μεθόδων της πολυκριτήριας λήψης αποφάσεων. Τέλος περιγράφεται η μέθοδος που επιλέχθηκε για την επίλυση του προβλήματος, η οποία είναι μια πολυκριτήρια προσέγγιση βασισμένη στον συναινετικό προγραμματισμό.

- Το έκτο κεφάλαιο είναι αφιερωμένο στην μοντελοποίηση του προβλήματος της επιλογής μέτρων ασφαλείας σε πληροφοριακά συστήματα εμπορικών λιμένων. Παρουσιάζεται η κατηγοριοποίηση των μέτρων και η διαδικασία ορισμού του συνόλου των δράσεων, ενώ στη συνέχεια γίνεται αναλυτική περιγραφή της συνεπούς οικογένειας κριτηρίων αξιολόγησης και επιλογής των μέτρων ασφάλειας.

- Στο έβδομο κεφάλαιο πραγματοποιείται η μελέτη μιας περίπτωσης επιλογής μέτρων ασφάλειας σε πληροφοριακό σύστημα εμπορικού λιμένα. Στην αρχή του κεφαλαίου γίνεται μια περιγραφή τους προβλήματος και της διαδικασίας σύμφωνα με την οποία ένα αγαθό προκύπτει υψηλού κινδύνου και χρήζει προστασίας. Στη συνέχεια επιλύεται το πρόβλημα με βάση τη μεθοδολογία του συναινετικού προγραμματισμού και γίνεται παρουσίαση των τελικών αποτελεσμάτων.

- Στο όγδοο και τελευταίο κεφάλαιο της διπλωματικής εργασίας παρουσιάζονται τα συμπεράσματα που εξήχθησαν από την παραπάνω μελέτη.

Επιπλέον παρατίθενται δύο παραρτήματα που περιλαμβάνουν α) τους πίνακες αντιστοίχισης αγαθών - απειλών - αδυναμιών – μέτρων ασφάλειας πληροφοριακών συστημάτων εμπορικών λιμένων και β) τα δεδομένα όλων των δυνατών συνδυασμών μέτρων ασφάλειας του παραδείγματος που μελετάται στο έβδομο κεφάλαιο.

2ο ΚΕΦΑΛΑΙΟ

Πληροφοριακά Συστήματα Εμπορικών Λιμένων

2 Πληροφοριακά Συστήματα Εμπορικών Λιμένων

2.1 Εισαγωγή

Οι εμπορικοί λιμένες είναι μεγάλης κλίμακας κρίσιμες υποδομές πληροφορικής καθώς διαθέτουν πληροφοριακά συστήματα που προσφέρουν κρίσιμες υπηρεσίες και φιλοξενούν ευαίσθητα δεδομένα. Η υποβάθμιση ή η διακοπή της λειτουργίας των πληροφοριακών τους συστημάτων μπορεί να έχει σοβαρές επιπτώσεις στην εθνική άμυνα, υγεία, ασφάλεια και οικονομία [1].

Εικόνα2. 1 Πληροφοριακό Σύστημα

Τα πληροφοριακά συστήματα των εμπορικών λιμένων χαρακτηρίζονται από των μεγάλο όγκο πληροφοριών που επεξεργάζονται, την πολυπλοκότητα και τα κατανεμημένα στοιχεία που διαθέτουν. Επιπλέον καλούνται να παρέχουν μια ποικιλία υπηρεσιών στους χρήστες που εξυπηρετούν, σε δημόσιους οργανισμούς και άλλες κρίσιμες υποδομές με τις οποίες αλληλεπιδρούν. Έτσι η υποβάθμιση, η διακοπή ή η φθορά των πληροφοριακών τους συστημάτων έχει σοβαρές συνέπειες όχι μόνο για την οικονομία και το γενικό πληθυσμό αλλά και για τις εξαρτώμενες υποδομές [2]. Δεδομένου λοιπόν, ότι τα πληροφοριακά συστήματα των εμπορικών λιμένων φιλοξενούν και διαχειρίζονται κρίσιμα και ευαίσθητα δεδομένα, η διαχείριση της ασφάλειας τους αποτελεί απαραίτητη διαδικασία για την αξιολόγηση και θεραπεία των κινδύνων στους οποίους εκτίθενται [3].

2.2 Κατηγοριοποίηση αγαθών των πληροφοριακών συστημάτων των εμπορικών λιμένων

Αρχικά τα πληροφοριακά συστήματα των εμπορικών λιμένων αποτελούνται όπως όλα τα πληροφοριακά συστήματα από τα εξής στρώματα [4][5]:

- **Υποδομές** (π.χ. κτίρια, πλατφόρμες, διακομιστές, ακίνητους/κινητούς τερματικούς σταθμούς, ναυτιλιακά συστήματα, βάσεις δεδομένων, πύλες, μαρίνες)

- **Τηλεπικοινωνιακά συστήματα** (π.χ. εξοπλισμός δικτύων, δορυφόροι, γεωγραφικά συστήματα πληροφοριών, διακομιστές, σταθμοί αναμετάδοσης)

- **Λογισμικό και συστήματα** (π.χ. δίκτυα επικοινωνιών, συστήματα αναγνώρισης, πλοήγησης, λογισμικό δρομολόγησης, συστήματα διαχείρισης επιχειρησιακών πόρων, εισιτηρίων)

- **Πληροφορία και ηλεκτρονικά δεδομένα** (π.χ. λιμενικά και ακτοπλοϊκά δεδομένα, εμπορικά δεδομένα)

- **Υπηρεσίες** (π.χ. τιμολόγηση, πλοήγηση, διαχείριση αποσκευών, φορτίων και σκαφών)

- **Άλλος εξοπλισμός** (π.χ. συστήματα συναγερμού πυρκαγιάς, κάμερες)

- **Χρήστες:**
  α) εσωτερικοί χρήστες (π.χ. διαχειριστές, προσωπικό)
  β) εξωτερικοί χρήστες (π.χ. λιμενικές αρχές, ναυτιλιακές εταιρίες, τελωνεία, ασφαλιστικές εταιρίες, εμπορικούς προμηθευτές)
  γ) οντότητες (πλοία, πλήρωμα, αποσκευές, φορτίο, οχήματα)

Το πληροφοριακό σύστημα ενός εμπορικού λιμένα είναι ασφαλές όταν όλα τα παραπάνω αγαθά των 7 στρωμάτων ικανοποιούν όλες τις διαστάσεις ασφάλειας, δηλαδή εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και έλεγχο πρόσβασης. Τα υφιστάμενα πρότυπα ασφάλειας στη ναυτιλία, οι μεθοδολογίες και τα εργαλεία εστιάζουν μόνο στη φυσική ασφάλεια των λιμένων, δηλαδή ικανοποιούν μόνο τις απαιτήσεις της διαθεσιμότητας και του ελέγχου πρόσβασης [7]. Η φυσική ασφάλεια θεωρείται υποτομέας του πεδίου της γνώσης της ασφάλειας πληροφοριών [8].

2.3 Ηλεκτρονικές υπηρεσίες πληροφοριακών συστημάτων εμπορικών λιμένων

Επιπλέον οι ηλεκτρονικές υπηρεσίες που παρέχονται από τα πληροφοριακά συστήματα των εμπορικών λιμένων μπορούν να ταξινομηθούν στις παρακάτω πέντε βασικές κατηγορίες:

- Τις υπηρεσίες διαχείρισης πλοίων, οι οποίες παρέχουν
  - Ηλεκτρονικές πληροφορίες στους πράκτορες για τα πλοία
  - Ηλεκτρονική επικοινωνία με λιμενικές αρχές και άλλους λιμένες
  - Ηλεκτρονικές διαδικασίες διαχείρισης
  - Υπηρεσίες πλοήγησης
  - Αυθεντικοποίηση πλοίων
  - Παρακολούθηση πλοίων μέσω γεωγραφικών συστημάτων

- Υπηρεσίες διαχείρισης φορτίου, οι οποίες προσφέρουν:
  - Ηλεκτρονική διαχείριση φορτίων
  - Ηλεκτρονικά έγγραφα στους πράκτορες και πληροφορίες για την κατάσταση των φορτίων
  - Αυθεντικοποίηση φορτίων
  - Παρακολούθηση φορτίων μέσω γεωγραφικών συστημάτων

- Επικοινωνία λιμένων:
  - Επικοινωνία λιμένων με άλλες οντότητες του περιβάλλοντος της ναυτιλίας

- Εσωτερικές υπηρεσίες εφοδιασμού οι οποίες παρέχουν της παρακάτω υπηρεσίες ηλεκτρονικά:
  - Διαχείριση εσωτερικών διαδικασιών
  - Προμήθειες
  - Τιμολόγηση
  - Πληρωμή
  - Κράτηση

- Υπηρεσίες διασύνδεσης με άλλα συστήματα:
  - Τελωνεία
  - Λιμενικές αρχές
  - Φορείς υγείας
  - Άλλες κρίσιμες υποδομές όπως αεροδρόμια, σιδηροδρομικοί σταθμοί κλπ.

2.4 Το περιβάλλον της ναυτιλίας

Το περιβάλλον της ναυτιλίας είναι αρκετά περίπλοκο και όπως αναφέρθηκε παραπάνω, οι λιμενικές υποδομές δεν μπορούν να θεωρηθούν ως μια απομονωμένη μονάδα, καθώς αλληλεπιδρούν με άλλους φορείς και προσφέρουν υπηρεσίες σε πολλαπλές κρίσιμες υποδομές. Οι εμπορικοί λιμένες είναι οι κεντρικές οντότητες στο περιβάλλον της ναυτιλίας καθώς είναι μεγάλης κλίμακας υποδομές και χαρακτηρίζονται από την πολλαπλότητα των εξαρτήσεων μεταξύ αυτών και των άλλων οντοτήτων του περιβάλλοντος της ναυτιλίας [6].

Έτσι λοιπόν το περιβάλλον της ναυτιλίας με κεντρική οντότητα τους εμπορικούς λιμένες περιλαμβάνει φορείς όπως οι εξής:

- Λιμάνια
- Πλοία (με επιβάτες, πλήρωμα, φορτίο)
- Λιμενικές αρχές
- Ναυτιλιακές εταιρίες
- Ασφαλιστικές εταιρίες
- Τελωνεία
- Τράπεζες
- Υπουργεία
- Ναυπηγεία
- Άλλες κρίσιμες υποδομές (αεροδρόμια, σιδηροδρόμους)
- Εμπορικούς προμηθευτές
- Βιομηχανία πλοίων
- Τηλεπικοινωνιακούς παρόχους κ.ά.

3ο ΚΕΦΑΛΑΙΟ

Κύκλος Ζωής και Πρότυπα Διαχείρισης Ασφάλειας

3 Κύκλος Ζωής και Πρότυπα Διαχείρισης Ασφάλειας

3.1 Εισαγωγή

Σύμφωνα με όσα αναφέρθηκαν στο προηγούμενο κεφάλαιο γίνεται αντιληπτό ότι τα πληροφοριακά συστήματα αποτελούν σημαντικό παράγοντα για την ορθή λειτουργία και την επίτευξη των επιχειρησιακών στόχων ενός εμπορικού λιμένα. Είναι λοιπόν εμφανής η ανάγκη για την ύπαρξη ασφάλειας ώστε να εξασφαλισθούν τα παραπάνω.

Η διαχείριση της ασφάλειας ενός πληροφοριακού συστήματος είναι μια αδιάκοπη διαδικασία εντοπισμού, εκτίμησης, ανάλυσης, αντιμετώπισης και παρακολούθησης των κινδύνων που αντιμετωπίζει ένας οργανισμός, με στόχο την προστασία του από απειλές που θα μπορούσαν να επηρεάσουν την ομαλή λειτουργία του.

Αρχικά, στο παρόν κεφάλαιο περιγράφεται ο κύκλος ζωής της ασφάλειας ενός πληροφοριακού συστήματος. Παρουσιάζεται δηλαδή η σειρά των διαδικασιών που πρέπει να ακολουθηθούν ώστε να ληφθούν τα απαραίτητα μέτρα ασφάλειας.

Τέλος, στην συνέχεια του κεφαλαίου παρουσιάζονται ορισμένα βασικά πρότυπα διαχείρισης ασφάλειας. Συγκεκριμένα περιγράφονται οι στόχοι και οι βασικές διαδικασίες που περιλαμβάνει το κάθε πρότυπο διαχείρισης ασφάλειας, καθώς και το είδος των οργανισμών στους οποίους απευθύνεται.

3.2 Κύκλος ζωής της ασφάλειας των αγαθών του πληροφοριακού συστήματος

Ο στόχος της ασφάλειας των αγαθών του πληροφοριακού συστήματος ενός οργανισμού είναι η προστασία των επιχειρηματικών λειτουργιών που υποστηρίζονται από το πληροφοριακό σύστημα του οργανισμού αυτού. Για να ληφθούν ωστόσο τα μέτρα ασφάλειας που είναι απαραίτητα για την προστασία του πληροφοριακού συστήματος θα πρέπει να ακολουθηθεί ένας κύκλος από συγκεκριμένες διαδικασίες, ο επονομαζόμενος « κύκλος ζωής της ασφάλειας » [9].

Οι διεργασίες του κύκλου ζωής της ασφάλειας παρουσιάζονται στο σχήμα που ακολουθεί και περιγράφονται στη συνέχεια της ενότητας.

Εικόνα 3. 1 Κύκλος ζωής της ασφάλειας [9]

1. **Διαχείριση της ασφάλειας.** Στο συγκεκριμένο στάδιο γίνεται ανάλυση των απαιτήσεων ασφάλειας του πληροφοριακού συστήματος του οργανισμού. Αναλύονται δηλαδή οι ανάγκες προστασίας των διαφόρων συστημάτων, εφαρμογών, υποδομών και δεδομένων του οργανισμού προς εξέταση. Ανάλογα με το βαθμό κρισιμότητας των επιχειρηματικών διαδικασιών που υποστηρίζει το κάθε αγαθό του πληροφοριακού συστήματος, εντοπίζονται τα πιο ευαίσθητα από άποψη ασφάλειας αγαθά. Στη συνέχεια καθορίζεται η πολιτική και οι κατευθυντήριες γραμμές που θα ακολουθήσει ο οργανισμός για την προστασία του πληροφοριακού συστήματος. Η πολιτική αυτή τίθεται σε εφαρμογή με τη λήψη και υλοποίηση των επιλεγμένων μέτρων προστασίας στα στάδια που έπονται.

2. **Σχεδιασμός και αρχιτεκτονική ασφαλείας.** Στη φάση αυτή γίνεται ο σχεδιασμός και ο καθορισμός των προδιαγραφών των λύσεων που είναι απαραίτητες για την τεχνική υλοποίηση των απαιτήσεων ασφάλειας του πληροφοριακού συστήματος. Επίσης γίνεται ο σχεδιασμός της τοπολογίας του δικτύου, καθορίζονται δηλαδή τα σημεία εισόδου-εξόδου, σχεδιάζεται ο έλεγχος πρόσβασης και γίνεται ο διαχωρισμός του δικτύου σε επιμέρους δίκτυα (ιδιωτικά, ευρείας ζώνης κλπ.).

Τελευταία διαδικασία του σταδίου αυτού είναι ο καθορισμός των προδιαγραφών του δικτυακού εξοπλισμού ασφάλειας.

3. **Υλοποίηση μέτρων ασφάλειας.** Το στάδιο αυτό του κύκλου ζωής περιλαμβάνει την εγκατάσταση και εφαρμογή των λύσεων-μέτρων ασφάλειας που έχουν επιλεγεί στο προηγούμενο στάδιο. Πρόκειται δηλαδή για την εγκατάσταση των απαιτούμενων εφαρμογών και εξοπλισμού, την κατάλληλη παραμετροποίηση των συστημάτων και του δικτύου, και γενικά την υλοποίηση των μέτρων ασφάλειας που έχουν παρουσιαστεί στην προηγούμενη φάση, με στόχο την επαρκή ασφάλεια του πληροφοριακού συστήματος.

4. **Παρακολούθηση της ασφάλειας.** Όπως δηλώνει και ο τίτλος, στη συγκεκριμένη φάση γίνεται παρακολούθηση των συστημάτων ασφάλειας που έχουν εγκατασταθεί, καθώς και των υπόλοιπων αγαθών του πληροφοριακού συστήματος, με σκοπό την επιβεβαίωση της ασφαλούς και ορθής λειτουργίας τους. Η υλοποίηση των μέτρων ασφάλειας μονάχα δεν επαρκεί για την ασφαλή λειτουργία του συστήματος, αλλά απαιτείται συνεχής παρακολούθηση της σωστής λειτουργίας και ενημέρωσης τους.

5. **Επιβεβαίωση και αναθεώρηση ασφάλειας.** Εκτός από τη συστηματική παρακολούθηση της ορθής λειτουργίας του πληροφοριακού συστήματος και των εγκατεστημένων μέτρων ασφάλειας, απαραίτητη διαδικασία είναι και η συνεχής επιβεβαίωση της ορθότητας της πολιτικής ασφάλειας και της επάρκειας των εφαρμοζόμενων μέτρων από τον οργανισμό. Κατά τη συγκεκριμένη λοιπόν διαδικασία γίνονται οι απαραίτητοι έλεγχοι, είτε εσωτερικοί είτε εξωτερικοί, για την εξασφάλιση της πληρότητας και της αποτελεσματικότητας των μέτρων που έχουν υλοποιηθεί. Έτσι επανεξετάζονται τα κρίσιμα αγαθά που χρήζουν προστασίας και ανανεώνεται, αν κριθεί απαραίτητο, η στρατηγική ασφάλειας που ακολουθεί ο οργανισμός [9].

3.3 Πρότυπα διαχείρισης ασφάλειας πληροφοριακών συστημάτων

3.3.1 ISO/IEC 27001:2005

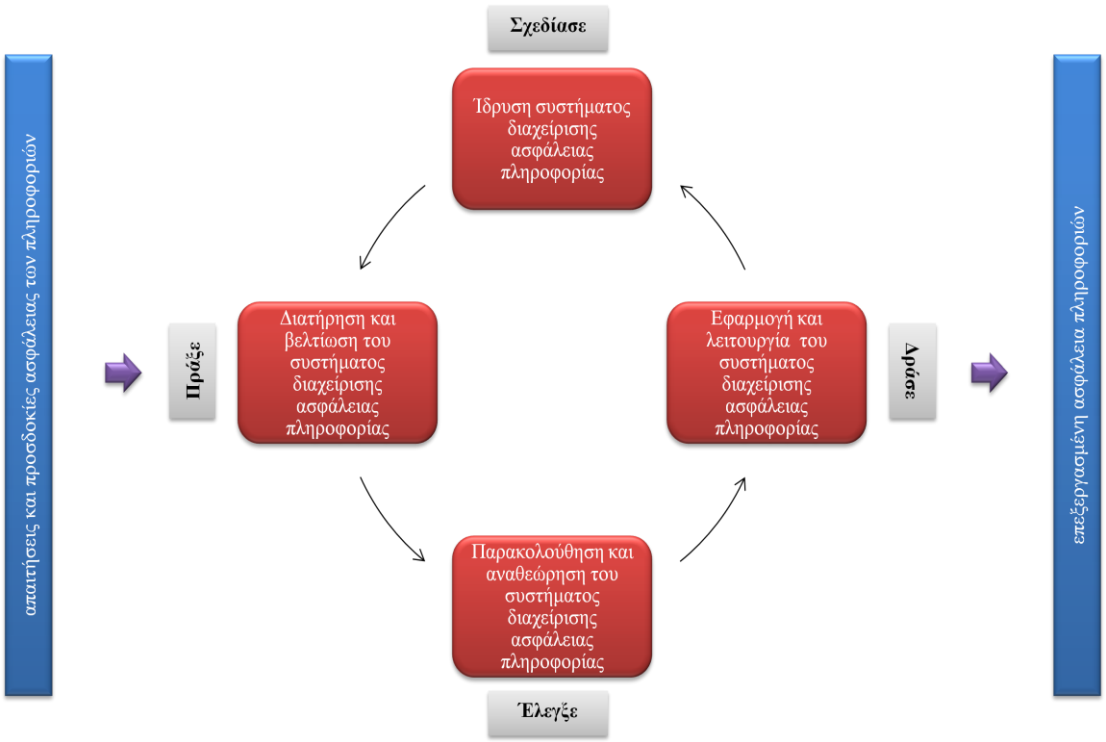
Το ISO/IEC 27001:2005 [10] είναι ένα διεθνές πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που κατασκευάστηκε με σκοπό να παρέχει ένα μοντέλο για την ίδρυση, την εφαρμογή, τη λειτουργία, την παρακολούθηση, την αναθεώρηση, τη διατήρηση και την βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS). Το σύστημα διαχείρισης ασφάλειας πληροφοριών είναι ένα σύνολο πολιτικών που έχουν να κάνουν με την διαχείριση και τον έλεγχο της ασφάλειας ενός πληροφοριακού συστήματος.

Αυτό το διεθνές πρότυπο καλύπτει όλα τα είδη των οργανισμών, όπως για παράδειγμα εμπορικές επιχειρήσεις και κυβερνητικές υπηρεσίες. Ωστόσο η εφαρμογή του θεωρείται ότι καλύπτει περισσότερο μεγάλης κλίμακας οργανισμούς. Επίσης καθορίζει τις απαιτήσεις για την εφαρμογή ελέγχων ασφάλειας προσαρμοσμένες τόσο στις ανάγκες ενός ολόκληρου οργανισμού όσο και τμήματος αυτού.

Η διαδικασία που παρουσιάζεται στο συγκεκριμένο πρότυπο σχετικά με την διαχείριση ασφάλειας ενός πληροφοριακού συστήματος βοηθάει τους χρήστες να επικεντρωθούν στην σημασία των παρακάτω διαδικασιών:

- Κατανόηση των απαιτήσεων ασφάλειας των πληροφοριών ενός οργανισμού και την ανάγκη ίδρυσης μιας πολίτικης για την ασφάλεια των πληροφοριών.
- Την πραγματοποίηση ελέγχων για την διαχείριση του κινδύνου της ασφάλειας των πληροφοριών.
- Παρακολούθηση της αποτελεσματικότητας του συστήματος διαχείρισης ασφάλειας πληροφοριών.
- Διαρκής βελτίωση βασισμένη στις αντικειμενικές μετρήσεις.

Το συγκεκριμένο πρότυπο ακολουθεί το μοντέλο "Σχεδίασε-Πράξε-Έλεγξε-Δράσε" ("Plan-Do-Check-Act" – PDCA model) όπως αυτό περιγράφεται στο παρακάτω σχήμα. Το μοντέλο αυτό δέχεται ως είσοδο τις απαιτήσεις και προσδοκίες ασφάλειας των πληροφοριών και δίνει ως έξοδο την επεξεργασμένη ασφάλεια πληροφοριών.



Εικόνα 3. 2 Μοντέλο "Σχεδίασε-Πράξε-Έλεγξε-Δράσε" του συστήματος διαχείρισης ασφάλειας πληροφοριών [10]

Επίσης, επισημαίνεται ότι το πρότυπο δίνει μεγάλη έμφαση στον κίνδυνο που διατρέχει η πληροφορία. Οι απαιτήσεις και οι διαδικασίες που περιγράφει έχουν ως επίκεντρο των εντοπισμό, την εκτίμηση και την αντιμετώπιση των κινδύνων που αντιμετωπίζει ο οργανισμός. Σύμφωνα με μία από τις απαιτούμενες διαδικασίες που περιγράφει το πρότυπο, ο οργανισμός είναι υποχρεωμένος να εφαρμόσει μια μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας, χωρίς ωστόσο να παρουσιάζεται μια συγκεκριμένη μέθοδος [10].

3.3.2 ISO/IEC 27002:2005

Το ISO/IEC 27002:2005 [11] είναι ένα εμπορικό πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που καθορίζει τις βασικές αρχές για την εφαρμογή, τη διατήρηση και τη βελτίωση της διαχείρισης ασφάλειας του πληροφοριακού συστήματος ενός οργανισμού. Το διεθνές αυτό πρότυπο μπορεί να χρησιμεύσει ως ένας πρακτικός οδηγός για την ανάπτυξη προτύπων και αποτελεσματικών πρακτικών διαχείρισης ασφάλειας σε έναν οργανισμό.

Το συγκεκριμένο πρότυπο περιλαμβάνει τις κατευθυντήριες αρχές του ISO / IEC 17799:2005 [14] και είναι σε θέση να καλύψει όλα τα είδη των οργανισμών όπως για παράδειγμα κυβερνητικούς οργανισμούς, μικρού, μεσαίου και μεγάλου μεγέθους επιχειρήσεις.

Επίσης το πρότυπο δεν παρουσιάζει κάποια μέθοδο για την ανάλυση και διαχείριση του κινδύνου, αλλά περιλαμβάνει μία σειρά από βασικούς τομείς ελέγχου. Οι βασικοί αυτοί τομείς είναι 11 (περιέχουν 39 βασικές κατηγορίες ασφαλείας και μία εισαγωγική κατηγορία που αποτελεί την εισαγωγή στην εκτίμηση και θεραπεία του κινδύνου) και καθορίζουν τις προϋποθέσεις που πρέπει να πληροί ο οργανισμός για να συμβαδίζει με το πρότυπο.

Οι βασικοί αυτοί τομείς που περιλαμβάνει το ISO/IEC 27002:2005 [11] είναι οι εξής παρακάτω:

i. Πολιτική Ασφάλειας
ii. Οργάνωση Ασφάλειας Πληροφοριακού Συστήματος
iii. Διαχείριση Κεφαλαίου
iv. Ασφάλεια Ανθρώπινου Δυναμικού
v. Φυσική και Περιβαλλοντική Ασφάλεια
vi. Διαχείριση Επικοινωνιών και Λειτουργιών
vii. Έλεγχος Πρόσβασης
viii. Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακού Συστήματος
ix. Διαχείριση Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων
x. Διαχείριση Επιχειρησιακής Συνέχειας
xi. Συμμόρφωση

3.3.3 ISO/IEC 27005:2008

Το ISO/IEC 27005:2008 [12] είναι ένα πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που παρέχει τις βασικές οδηγίες για τη διαχείριση κινδύνου όσον αφορά την ασφάλεια των πληροφοριών. Το διεθνές αυτό πρότυπο βασίζεται στις γενικές έννοιες που περιγράφονται στο ISO/IEC 27001:2005 [10] καθώς και στις αρχές και διαδικασίες που παρουσιάζονται στο ISO/IEC 27002:2005 [11].

Το συγκεκριμένο πρότυπο μπορεί να εφαρμοστεί σε όλους τους τύπους οργανισμών όπως για παράδειγμα εμπορικές επιχειρήσεις και κυβερνητικούς φορείς. Είναι ένα χρήσιμο εργαλείο για τους διαχειριστές και το προσωπικό που εμπλέκονται στην διαχείριση κινδύνου ασφάλειας των πληροφοριών.

Όλες οι δραστηριότητες της διαχείρισης κινδύνου στην ασφάλεια πληροφοριών περιγράφονται στις παρακάτω ενότητες που περιλαμβάνει το ISO/IEC 27005:2008 [12] και είναι οι εξής:

- Δημιουργία Γενικού Πλαισίου
- Εκτίμηση Κινδύνου
- Θεραπεία Κινδύνου
- Αποδοχή Κινδύνου
- Γνωστοποίηση Κινδύνου
- Παρακολούθηση Κινδύνου και Επανεξέταση

Επίσης το πρότυπο αυτό δεν παρέχει κάποια συγκεκριμένη μεθοδολογία για τη διαχείριση των κινδύνων ασφαλείας των πληροφοριών, καθώς η προσέγγιση της διαχείρισης του κινδύνου εναπόκειται σε κάθε οργανισμό ανάλογα με τη μορφή και τους στόχους του [12].

3.3.4 NIST SP 800-30

Το NIST SP 800-30 [13] αποτελεί ένα δωρεάν οδηγό που παρέχει τα βασικά στοιχεία για την ανάπτυξη ενός αποτελεσματικού προγράμματος διαχείρισης κινδύνων. Περιλαμβάνει όλες απαραίτητες διαδικασίες και βασικές πρακτικές που απαιτούνται για τον εντοπισμό και καταπολέμηση των κινδύνων που απειλούν τα πληροφοριακά συστήματα.

Το πρότυπο αυτό παρέχει μια κοινή βάση σε όλο το προσωπικό ενός οργανισμού, εξειδικευμένο ή μη, που εμπλέκεται με την διαχείριση κινδύνου πληροφοριακών συστημάτων με απώτερο σκοπό την βελτίωση της ασφάλειας, τη σωστή πληροφόρηση και την τεκμηρίωση αποτελεσμάτων της διαχείριση κινδύνου των πληροφοριακών συστημάτων.

Ο μεθοδολογία που παρουσιάζεται για τη διαχείριση κινδύνου σύμφωνα με το NIST SP 800-30 [13] χωρίζεται σε τρεις διαδικασίες:

I. Η πρώτη διαδικασία, η **Ανάλυση Επικινδυνότητας**, αφορά των εντοπισμό των απειλών και κινδύνων που διατρέχει το πληροφοριακό σύστημα, καθώς και τον προσδιορισμό των μέτρων που τις αντιμετωπίζουν. Σύμφωνα με το NIST 800-30, ο κίνδυνος είναι μια συνάρτηση της πιθανότητας μιας δεδομένης απειλής, η οποία συντελείται από συγκεκριμένες αδυναμίες, και των επιπτώσεων της εν λόγω απειλής στην ομαλή λειτουργία του πληροφοριακού συστήματος. Η ανάλυση επικινδυνότητας αποτελείται από εννέα βήματα:

- Βήμα 1 – Χαρακτηρισμός Συστήματος
- Βήμα 2 – Προσδιορισμός Απειλών
- Βήμα 3 – Προσδιορισμός Αδυναμιών
- Βήμα 4 – Ανάλυση Μέτρων Ασφάλειας
- Βήμα 5 – Προσδιορισμός Πιθανότητας
- Βήμα 6 – Ανάλυση Επιπτώσεων
- Βήμα 7 – Προσδιορισμός Κινδύνου
- Βήμα 8 – Προτάσεις Μέτρων Ασφάλειας
- Βήμα 9 – Τεκμηρίωση Αποτελεσμάτων

II. Η δεύτερη διαδικασία είναι η **Μείωση Κινδύνου** και αφορά την αξιολόγηση και εφαρμογή των κατάλληλων μέτρων που προσδιορίστηκαν από την προηγούμενη διαδικασία (Ανάλυση Επικινδυνότητας) με σκοπό τη μείωση του κινδύνου.

Η συγκεκριμένη διαδικασία χωρίζεται σε έξι ενότητες οι οποίες αφορούν

- Τις επιλογές που υπάρχουν για την μείωση του κινδύνου (αποδοχή, αποφυγή, μεταφορά κλπ.)
- Την στρατηγική μείωσης του κινδύνου
- Μια προσέγγιση για την εφαρμογή μέτρων
- Τις κατηγορίες μέτρων
- Την ανάλυση κόστους-οφέλους της εφαρμογής των συνιστώμενων μέτρων
- Τον εναπομένοντα κίνδυνο

III. Η τρίτη και τελευταία διαδικασία είναι η **Αξιολόγηση και Εκτίμηση.** Η ενότητα αυτή δίνει έμφαση στην ανάγκη για αξιολόγηση και εκτίμηση του κινδύνου και στις συνιστώσες που θα κατευθύνουν σε ένα πετυχημένο πλάνο ανάλυσης και διαχείρισης κινδύνου.

Επίσης σημειώνεται ότι το NIST 800-30 [13] αποσκοπεί στο να βοηθήσει κυρίως μεγάλης κλίμακας οργανισμούς, όπως κυβερνητικούς οργανισμούς, για την αποτελεσματικότερη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων τους.

4ο ΚΕΦΑΛΑΙΟ

Ανάλυση και Διαχείριση Επικινδυνότητας

4 Ανάλυση και Διαχείριση Επικινδυνότητας

Στο τελευταίο μέρος του προηγούμενου κεφαλαίου παρουσιάστηκαν οι στόχοι και οι βασικές οδηγίες ορισμένων προτύπων διαχείρισης ασφάλειας πληροφοριακών συστημάτων. Το παρόν κεφάλαιο αφορά στις φάσεις που αποτελούν την διαδικασία της ανάλυσης και διαχείρισης κινδύνου της ασφάλειας πληροφοριακών συστημάτων καθώς και τις μεθοδολογίες που τις εξυπηρετούν.

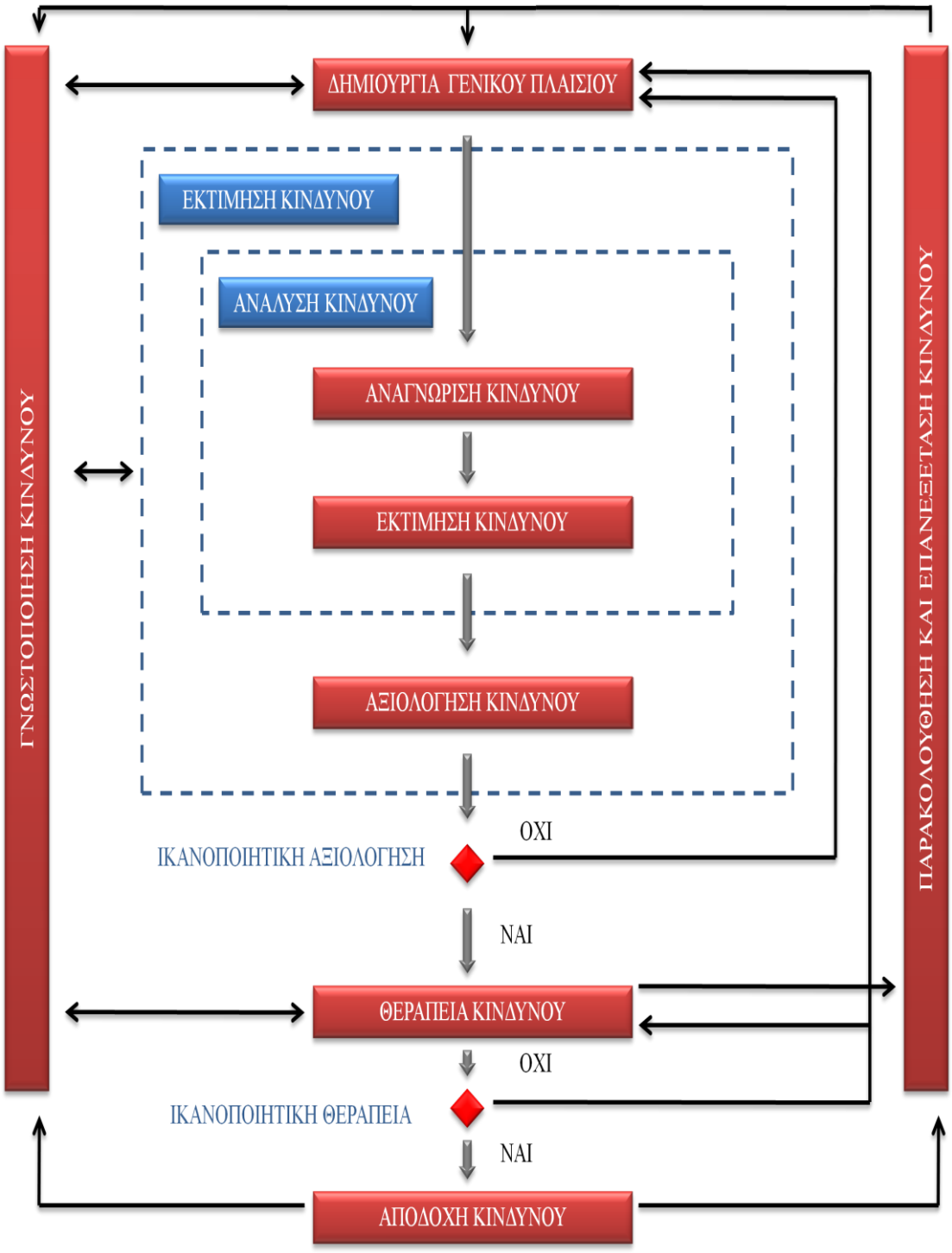
Συγκεκριμένα στην αρχή του κεφαλαίου παρουσιάζονται συνοπτικά οι δράσεις-φάσεις που αποτελούν την εν λόγω διαδικασία, ενώ στις δυο ενότητες που ακολουθούν γίνεται αναλυτικότερη περιγραφή της Εκτίμησης Κινδύνου, που είναι η σημαντικότερη φάση της διαδικασίας, και της Θεραπείας Κινδύνου, που μας απασχολεί ιδιαίτερα διότι περιλαμβάνει την επιλογή των κατάλληλων μέτρων προστασίας.

Τέλος, παρατίθενται εν συντομία ορισμένες μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων μαζί με κάποια βασικά για την αξιολόγηση τους κριτήρια και γίνεται μια περιγραφή της συνεργατικής μεθοδολογίας STORM-RM, η οποία αποτέλεσε και αφορμή της συγκεκριμένης διπλωματικής.

4.1 Γενικά για τη διαδικασία διαχείρισης κινδύνου της ασφάλειας πληροφοριακών συστημάτων

Σύμφωνα με το ISO/IEC 27005:2008 [12], όπως φαίνεται και από το σχήμα που ακολουθεί, η διαδικασία της διαχείρισης του κινδύνου της ασφάλειας των πληροφοριακών συστημάτων αποτελείται από τις εξής δράσεις: τη Δημιουργία Γενικού Πλαισίου, την Εκτίμηση Κινδύνου, τη Θεραπεία Κινδύνου, την Αποδοχή Κινδύνου, τη Γνωστοποίηση Κινδύνου και την Παρακολούθηση Κινδύνου και Επανεξέταση.

Η διαδικασία ξεκινάει με την Δημιουργία Γενικού Πλαισίου κατά την οποία καθορίζονται α) τα βασικά κριτήρια για την διαχείριση κινδύνου του πληροφοριακού συστήματος, β) το πεδίο εφαρμογής και τα όρια και γ) η θέσπιση του κατάλληλου οργανισμού για την λειτουργία της διαχείρισης του κινδύνου της ασφάλειας των πληροφοριών. Ο κύκλος εργασιών καταλήγει στην Αποδοχή Κινδύνου, όπου γίνεται επίσημη καταγραφή της απόφασης να γίνουν αποδεκτοί οι κίνδυνοι και των ευθυνών της απόφασης αυτής.



Εικόνα 4. 1 Διαδικασία διαχείρισης κινδύνου της ασφάλειας πληροφοριακών συστημάτων [12]

Επιπλέον καθ' όλη τη διάρκεια της διαδικασίας οι πληροφορίες για τον κίνδυνο διακινούνται ανάμεσα στον αποφασίζοντα και τα ενδιαφερόμενα μέλη (Γνωστοποίηση Κινδύνου), ενώ παρακολουθούνται συνεχώς όλες οι εργασίες ώστε να αξιολογούνται και να βελτιώνονται εάν αυτό κριθεί απαραίτητο(Παρακολούθηση Κινδύνου και Επανεξέταση).

Ωστόσο η σημαντικότερη διαδικασία που εμπεριέχεται στα πρότυπα αυτά και θα περιγραφεί αναλυτικότερα στη συνέχεια του κεφαλαίου είναι η Εκτίμηση του Κινδύνου. Επίσης, θα δοθεί έμφαση και στη Θεραπεία του Κινδύνου, καθώς η συγκεκριμένη φάση επικεντρώνεται στην επιλογή των μέτρων για την αντιμετώπιση των κινδύνων του πληροφοριακού συστήματος.

Η περιγραφή της εκτίμησης-αξιολόγησης και της θεραπείας του κινδύνου στις επόμενες ενότητες θα γίνει σύμφωνα με τις οδηγίες που παρουσιάζονται: α) στο ISO/IEC 27005:2008 [12], το οποίο είναι ένα πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που παρέχει τις βασικές οδηγίες για τη διαχείριση κινδύνου όσον αφορά την ασφάλεια των πληροφοριών και β) στον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) [15].

Να σημειωθεί εδώ ότι οι διαδικασίες της Ανάλυσης και Διαχείρισης Επικινδυνότητας που παρουσιάζονται στη συνέχεια με βάση τους δυο παραπάνω οδηγούς είναι οι ίδιες, απλά μπορεί να υπάρχουν κάποιες διαφοροποιήσεις στην κατηγοριοποίηση τους και στο στάδιο που τοποθετούνται κάποιες διεργασίες.

4.2 Εκτίμηση κινδύνου ασφάλειας πληροφοριακών συστημάτων

Κάθε οργανισμός βρίσκεται συνεχώς εκτεθειμένος σε μια σειρά από καινούριες ή μεταβαλλόμενες απειλές και αδυναμίες οι οποίες μπορεί να επηρεάσουν την ομαλή λειτουργία του και την επίτευξη των στόχων του. Η αναγνώριση, η εκτίμηση και η ανάλυση αυτών των απειλών και αδυναμιών είναι ο μόνος τρόπος για να γίνει κατανοητή και να μετρηθεί η επίπτωση της σχετικής επικινδυνότητας, ώστε στη συνέχεια να παρθούν οι κατάλληλες αποφάσεις για τους ελέγχους και τα μέτρα που τις αντιμετωπίζουν [16].

Ο κίνδυνος είναι ο συνδυασμός της πιθανότητας εμφάνισης ενός ανεπιθύμητου γεγονότος και των επιπτώσεων που θα επακολουθούσαν από την εμφάνιση του. Οι κίνδυνοι πρέπει να εντοπίζονται και να εκτιμώνται, τόσο ποιοτικά όσο και ποσοτικά, ανάλογα με τα κριτήρια αξιολόγησης επικινδυνότητας και τους στόχους που έχει θέσει ο οργανισμός, έτσι ώστε να δίνεται η δυνατότητα ιεράρχησης τους στους διαχειριστές του πληροφοριακού συστήματος.

Η εκτίμηση της επικινδυνότητας προσδιορίζει την αξία των αγαθών του πληροφοριακού συστήματος, εντοπίζει τις υπάρχουσες αδυναμίες και απειλές, προσδιορίζει τους υπάρχοντες ελέγχους και την επίδραση τους στους κινδύνους που εντοπίστηκαν, καθορίζει τις πιθανές επιπτώσεις και τέλος ιεραρχεί τους κινδύνους με βάση τα κριτήρια αξιολόγησης. Η διαδικασία της εκτίμησης του κινδύνου αποτελείται από τις ακόλουθες φάσεις:

- Την Ανάλυση Κινδύνου, η οποία επιμερίζεται στις εξής δραστηριότητες
    - Αναγνώριση Κινδύνου
    - Εκτίμηση Κινδύνου

- Την Αξιολόγηση Κινδύνου.

Επίσης η εκτίμηση της επικινδυνότητας μπορεί να γίνει σε δύο επαναλήψεις, αρχικά με ένα υψηλό επίπεδο αξιολόγησης όπου εντοπίζονται οι ισχυροί κίνδυνοι που χρήζουν περαιτέρω εκτίμησης και στη συνέχεια με μία εκτίμηση εις βάθος για την εξέταση των υψηλών κινδύνων που προσδιορίστηκαν στην πρώτη επανάληψη. Αξίζει ακόμα να σημειωθεί ότι εναπόκειται στον κάθε οργανισμό να επιλέξει την δική του προσέγγιση για την εκτίμηση του κινδύνου ανάλογα με τους στόχους του και το σκοπό της αξιολόγησης που έχει θέσει [12].

4.2.1 Ανάλυση κινδύνου

4.2.1.1 Αναγνώριση κινδύνου

Η πρώτη διαδικασία της ανάλυσης της επικινδυνότητας είναι η **Αναγνώριση της Επικινδυνότητας**. Αρχικά σε αυτή τη φάση εντοπίζονται τα αγαθά του πληροφοριακού συστήματος, οι απειλές και οι αδυναμίες. Η διαδικασία αυτή πρέπει να είναι πλήρης και συστηματική καθώς δεν πρέπει να παραληφθεί κάποιος κίνδυνος, ανεξάρτητα από το αν έχει ήδη εντοπιστεί από τον οργανισμό και είναι ελεγχόμενος. Επιπλέον προσδιορίζονται οι επιπτώσεις καθώς και οι υπάρχοντες έλεγχοι που μετριάζουν ή εξαλείφουν αυτούς τους κινδύνους.

Η καλή ποιότητα των πληροφοριών και η εμπεριστατωμένη γνώση του οργανισμού, καθώς και του εσωτερικού και εξωτερικού περιβάλλοντος του, είναι πολύ σημαντικά στοιχεία για τον προσδιορισμό των κινδύνων. Επιπλέον, οι μέθοδοι και τα εργαλεία που χρησιμοποιούνται για τον εντοπισμό των κινδύνων και της εμφάνισής τους περιλαμβάνουν λίστες ελέγχου, κρίσεις που βασίζονται στην εμπειρία και καταγεγραμμένα περιστατικά, διαγράμματα ροής, ανάλυση συστημάτων και ανάλυση σεναρίων [16].

Στην συνέχεια της ενότητας περιγράφονται οι δραστηριότητες της αναγνώρισης επικινδυνότητας που προαναφέρθηκαν:

Αναγνώριση Αγαθών: Τα αγαθά έχουν αξία και αποτελούν περιουσιακό στοιχείο για των οργανισμό και ως εκ τούτου πρέπει να προστατευτούν. Αγαθά για ένα πληροφοριακό σύστημα δεν αποτελούν μόνο το υλικό και το λογισμικό, αλλά και οι εγκαταστάσεις και οι υποδομές, τα δεδομένα, ο δικτυακός εξοπλισμός κλπ. Η αναγνώριση των αγαθών θα πρέπει να γίνεται σε τέτοιο επίπεδο ώστε να συλλέγονται όλες οι πληροφορίες που είναι απαραίτητες για την αξιολόγηση του κινδύνου.

Αναγνώριση Απειλών: Μια απειλή μπορεί να βλάψει τα αγαθά του πληροφοριακού συστήματος και μπορεί να είναι φυσικής ή ανθρώπινης προέλευσης, τυχαία ή σκόπιμη. Στο στάδιο αυτό εντοπίζονται οι πιθανές απειλές και οι πηγές τους, ενώ πρέπει να προσδιορίζονται αρχικά κατά γενικές κατηγορίες και είδος, και στη συνέχεια ως μεμονωμένες σε κάθε γενική κατηγορία.

Προσδιορισμός Αδυναμιών: Στη συγκεκριμένη φάση εντοπίζονται οι αδυναμίες τις οποίες μπορεί να εκμεταλλευτούν οι υπάρχουσες απειλές και να προκαλέσουν βλάβη στα αγαθά του πληροφοριακού συστήματος. Οι αδυναμίες μπορούν να προσδιοριστούν στους τομείς της οργάνωσης, των διαδικασιών και διεργασιών, του προσωπικού, του φυσικού περιβάλλοντος, της διαμόρφωσης του πληροφοριακού συστήματος, του υλικού, του λογισμικού, του δικτυακού εξοπλισμού και των εξαρτήσεων από εξωτερικούς φορείς.

Προσδιορισμός των Υφιστάμενων Ελέγχων-Μέτρων: Κατά το συγκεκριμένο στάδιο παράγεται μια λίστα από όλους τους υφιστάμενους και προγραμματισμένους ελέγχους, την εφαρμογή τους και την κατάσταση χρήσης τους. Η φάση αυτή είναι απαραίτητη ώστε να αποφευχθεί περιττή εργασία ή κόστος(π.χ. επανάληψη ελέγχου). Στον εντοπισμό αυτών των ελέγχων μπορεί να βοηθήσουν η επανεξέταση εγγράφων που περιέχουν πληροφορίες για τα μέτρα, η επικοινωνία με τους αρμόδιους της ασφάλειας του πληροφοριακού συστήματος, η διεξαγωγή μια έρευνας για το αν τα εφαρμοσμένα μέτρα λειτουργούν αποτελεσματικά και η σύγκριση με τη λίστα των αντίστοιχων υφιστάμενων μέτρων, και η επανεξέταση των αποτελεσμάτων των εσωτερικών ελέγχων.

Προσδιορισμός Επιπτώσεων: Η διαδικασία αυτή περιλαμβάνει τον εντοπισμό των επιπτώσεων ή της ζημιάς για τον οργανισμό από την εμφάνιση μιας απειλής ή μιας αδυναμίας. Προσδιορίζονται δηλαδή οι συνέπειες της απώλειας της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας για ένα αγαθό του πληροφοριακού συστήματος. Οι επιπτώσεις στην επιχειρησιακή λειτουργία του οργανισμού προσδιορίζονται με βάση την έρευνα και το χρόνο επισκευής, τον χαμένο χρόνο και τη χαμένη εργασία, το κόστος ευκαιρίας, την υγεία και την ασφάλεια, το οικονομικό κόστος αποκατάστασης της ζημιάς και τη δυσφήμηση του οργανισμού [12].

4.2.1.2 Εκτίμηση κινδύνου

Η δεύτερη διαδικασία της ανάλυσης της επικινδυνότητας είναι η **Εκτίμηση της Επικινδυνότητας.** Η εκτίμηση της επικινδυνότητας περιλαμβάνει τις εξής διεργασίες

- Αξιολόγηση των επιπτώσεων
- Αξιολόγηση της πιθανότητας εμφάνισης των επιπτώσεων
- Εκτίμηση του επιπέδου της επικινδυνότητας

Η εκτίμηση του κινδύνου μπορεί να είναι ποιοτική, ημι-ποσοτική ή ποσοτική ή και συνδυασμός των παραπάνω. Σε κάθε περίπτωση, ο τύπος της εκτίμησης που θα εκτελεστεί πρέπει να είναι σύμφωνος με τα βασικά κριτήρια για την διαχείριση κινδύνου του πληροφοριακού συστήματος που αναπτύχθηκαν στον προσδιορισμό του γενικού πλαισίου διαχείρισης επικινδυνότητας. Στην ποιοτική εκτίμηση, η σημασία και η πιθανότητα εμφάνισης των επιπτώσεων περιγράφονται λεπτομερώς. Οι κλίμακες που χρησιμοποιούνται μπορούν να προσαρμόζονται ανάλογα με τις περιστάσεις και διαφορετικές περιγραφές μπορούν να χρησιμοποιηθούν για διαφορετικούς κινδύνους. Στην ημι-ποσοτική εκτίμηση ο στόχος είναι να δοθούν κάποιες τιμές στις κλίμακες που χρησιμοποιούνται για την ποιοτική αξιολόγηση. Οι τιμές αυτές είναι συνήθως ενδεικτικές και όχι πραγματικές, πράγμα που είναι απαραίτητο για την ποσοτική προσέγγιση. Τέλος, στην ποσοτική εκτίμηση, αποδίδονται αριθμητικές τιμές στις επιπτώσεις και την πιθανότητα εμφάνισης τους. Η

ποιότητα της εκτίμησης εξαρτάται από την ακρίβεια των αποδιδόμενων τιμών και την ακρίβεια των στατιστικών μοντέλων [16].

Οι πληροφορίες που χρησιμοποιούνται για την εκτίμηση των συνεπειών των κινδύνων και την πιθανότητα εμφάνισης τους προέρχονται από προηγούμενη εμπειρία ή δεδομένα, διεθνή πρότυπα και οδηγούς, έρευνες και αναλύσεις της αγοράς, πειράματα, οικονομικά, τεχνικά και άλλα μοντέλα καθώς και από συμβουλές εξειδικευμένων ατόμων.

Επίσης το επίπεδο του κινδύνου μπορεί να εκτιμηθεί με τη χρήση στατιστικών αναλύσεων και υπολογισμών που συνδυάζουν την επίπτωση και την πιθανότητα εμφάνισης του περιστατικού. Οι τύποι και οι μέθοδοι για τη σύνθεσή του πρέπει να είναι σύμφωνοι με τα κριτήρια που ορίζονται κατά την δημιουργία του πλαισίου διαχείρισης κινδύνων.

4.2.2 Αξιολόγηση κινδύνου

Η Αξιολόγηση Κινδύνου αποτελεί την τελευταία διεργασία της Εκτίμησης Κινδύνου της ασφάλειας πληροφοριακών συστημάτων. Κατά τη συγκεκριμένη φάση, οι κίνδυνοι των οποίων το επίπεδο έχει αξιολογηθεί στο προηγούμενο στάδιο συγκρίνονται με τα κριτήρια αξιολόγησης και αποδοχής των κινδύνων. Τα κριτήρια αυτά και η συλλογιστική των αποφάσεων έχουν οριστεί κατά τη θέσπιση του γενικού πλαισίου και πρέπει να λαμβάνουν υπόψη τους επιχειρησιακούς στόχους του οργανισμού, τις απόψεις των εμπλεκόμενων ατόμων και τους σκοπούς της διαδικασίας διαχείρισης του κινδύνου.

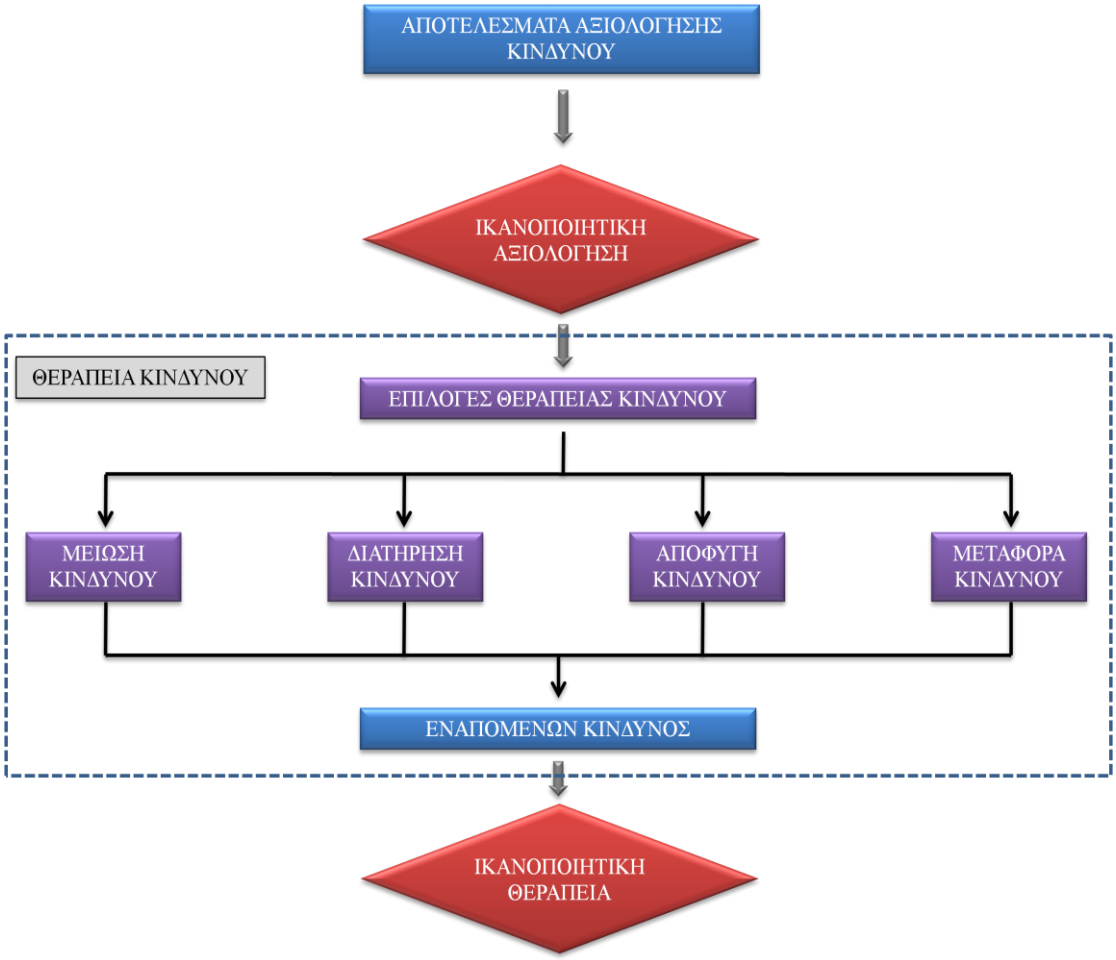
Επιπλέον, πέρα από το αποδεκτό επίπεδο επικινδυνότητας, οι αποφάσεις που παίρνονται κατά την αξιολόγηση του κινδύνου λαμβάνονται με βάση τις συνέπειες από την εμφάνιση του περιστατικού, την πιθανότητα εμφάνισης του, την αναγνώριση και ανάλυση των κινδύνων στα προηγούμενα στάδια, καθώς την συνολική επίπτωση από την ταυτόχρονη εμφάνιση πολλών περιστατικών κινδύνου.

Έτσι στο τέλος της διαδικασίας παράγεται ένα σύνολο κινδύνων οι οποίοι προκρίνονται σύμφωνα με τα κριτήρια αξιολόγησης και χρήζουν θεραπείας με βάση τις προτεραιότητες της αντιμετώπισης των κινδύνων [12][16].

4.3 Θεραπεία κινδύνου ασφάλειας πληροφοριακών συστημάτων

4.3.1 Γενική περιγραφή της διαδικασίας

Η διαδικασία της Θεραπείας Κινδύνου είναι η φάση που έπεται της Αξιολόγησης του Κινδύνου και αφορά άμεσα το έργο της διπλωματικής αφού κατά το συγκεκριμένο στάδιο επιλέγονται οι έλεγχοι για τη μείωση, την αποφυγή, τη διατήρηση ή την αποφυγή των κινδύνων και ορίζεται το σχέδιο αντιμετώπισης τους.



Εικόνα 4. 2 Διαδικασία θεραπείας κινδύνου ασφάλειας πληροφοριακών συστημάτων [12]

Οι επιλογές της Θεραπείας του Κινδύνου θα πρέπει να εκλέγονται με βάση τα αποτελέσματα της Εκτίμησης Κινδύνου, το αναμενόμενο κόστος από την εφαρμογή των συγκεκριμένων επιλογών και τα προσδοκώμενα οφέλη από την υλοποίηση τους. Όταν με χαμηλό κόστος μπορούμε να πετύχουμε σημαντική μείωση του κινδύνου

τότε τα επιλεγόμενα μέτρα πρέπει να υλοποιηθούν. Γενικότερα οι αρνητικές επιπτώσεις του κινδύνου θα πρέπει να πέσουν σε επίπεδα των οποίων η προσέγγιση είναι εφικτή για τον οργανισμό [12].

Όσον αφορά τις τέσσερις επιλογές που έχει ο οργανισμός για την αντιμετώπιση του κινδύνου (τη μείωση, την αποφυγή, τη διατήρηση ή την αποφυγή), η μία δεν αναιρεί την άλλη, αλλά μπορούμε να έχουμε και συνδυασμό αυτών. Για παράδειγμα ο οργανισμός μπορεί να επιλέξει μια στρατηγική μείωσης των επιπτώσεων και της πιθανότητας εμφάνισης του κινδύνου και μεταφορά ή διατήρηση του εναπομένοντος κινδύνου.

Επιπροσθέτως, θα πρέπει όπως αναφέρθηκε παραπάνω, να καθοριστεί και ένα πλάνο το οποίο θα ορίζει με σαφήνεια τις προτεραιότητες, καταδεικνύοντας έτσι το ποιες μεμονωμένες θεραπείες κινδύνων πρέπει να εφαρμοστούν και το χρονοδιάγραμμα υλοποίησης τους. Οι προτεραιότητες αυτές μπορούν να προκύψουν με βάση διάφορες μεθόδους, όπως είναι η ταξινόμηση των κινδύνων και ανάλυση κόστους-οφέλους.

Τελικά, αφότου καθοριστεί το πλάνο αντιμετώπισης των κινδύνων πρέπει να προσδιοριστεί ο εναπομένων κίνδυνος. Σε περίπτωση που ο εναπομένων κίνδυνος δεν ανταποκρίνεται στα κριτήρια και τα επίπεδα αποδοχής κινδύνου, τότε ίσως να είναι απαραίτητη μια επανάληψη της φάσης της Θεραπείας Κινδύνου πριν η διαδικασία προχωρήσει στο στάδιο όπως Αποδοχής του Κινδύνου [12].

4.3.2 Επιλογές Θεραπείας Κινδύνου

Σύμφωνα με όσα αναφέρθησαν στην προηγούμενη ενότητα οι επιλογές που υπάρχουν για την αντιμετώπιση του κινδύνου ασφάλειας πληροφοριακών συστημάτων είναι τέσσερις, και συγκεκριμένα η μείωση του κινδύνου, η αποφυγή, διατήρηση και η μεταφορά του [12].

Η πρώτη επιλογή, η **μείωση του κινδύνου**, αφορά την επιλογή των κατάλληλων μέτρων με σκοπό την μείωση του επιπέδου του κινδύνου σε επιθυμητά επίπεδα έτσι ώστε ο εναπομένων κίνδυνος να μπορεί να αξιολογηθεί ως αποδεκτός. Τα είδη προστασίας που μπορούμε να αποκομίσουμε από την εφαρμογή των μέτρων είναι η διόρθωση, η εξάλειψη, η αποτροπή, η πρόληψη, η μείωση των επιπτώσεων, ο εντοπισμός, η παρακολούθηση και η ευαισθητοποίηση.

Επιπλέον, εάν επιλεχθεί η μείωση του κινδύνου και η υλοποίηση μέτρων, θα πρέπει να ληφθούν υπόψη ορισμένοι περιορισμοί όπως οι εξής: χρονικοί και οικονομικοί περιορισμοί, τεχνικοί, επιχειρησιακοί, ηθικοί και νομικοί περιορισμοί, πολιτιστικοί και περιβαλλοντικοί, ατομικοί-προσωπικοί, και περιορισμοί για ενσωμάτωση νέων αλλά και ήδη υπαρχόντων μέτρων.

Επόμενη επιλογή αποτελεί η **αποφυγή του κινδύνου**. Σε περίπτωση που το επίπεδο του αναγνωρισμένου κινδύνου είναι πολύ υψηλό ή το κόστος εφαρμογής μιας επιλεγμένης θεραπείας κριθεί ότι δεν είναι αντιπροσωπευτικό των οφελών της, τότε μπορεί να παρθεί απόφαση για ολοκληρωτική αποφυγή του κίνδυνου. Αυτό μπορεί να πραγματοποιηθεί μέσα από την απόσυρση μιας δραστηριότητας που συνδέεται με τον κίνδυνο αυτό(ή όπως συνόλου δραστηριοτήτων) ή την αλλαγή των συνθηκών υπό τις οποίες λειτουργεί.

Σε ότι αφορά την επόμενη επιλογή, η **διατήρηση κινδύνου** επιλέγεται όταν το επίπεδο επικινδυνότητας πληροί τις προϋποθέσεις και τα κριτήρια της αποδοχής κινδύνου. Όπως γίνεται κατανοητό, στην προκειμένη περίπτωση δεν υπάρχει ανάγκη για την υλοποίηση κάποιον μέτρων και έτσι ο κίνδυνος μπορεί να διατηρηθεί.

Την τελευταία επιλογή όπως φάσης όπως Θεραπείας Κινδύνου αποτελεί η **μεταφορά κινδύνου**. Ο κίνδυνος μεταφέρεται σε έναν εξωτερικό φορέα ο οποίος μπορεί να τον διαχειριστεί αποτελεσματικά. Βέβαια, η μεταφορά μπορεί να δημιουργήσει νέους κινδύνους και άρα την ανάγκη για νέα μέτρα. Επίσης μπορεί να είναι δυνατή η μεταφορά της ευθύνης για τη διαχείριση του κινδύνου, ωστόσο δεν είναι κανονικά δυνατή η μεταφορά της ευθύνης των επιπτώσεων [12][17].

4.4 Μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας

Για την αποτίμηση των κινδύνων ασφαλείας καθώς και για την καταπολέμηση των απειλών και των αδυναμιών που αντιμετωπίζουν τα πληροφοριακά συστήματα, είναι απαραίτητη η εκτέλεση μιας μεθοδολογίας ανάλυσης και διαχείρισης επικινδυνότητας. Οι βασικές απαιτήσεις που πρέπει να έχουν οι μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας καθορίζονται από το πρότυπο ISO 27005:2008 [12].

Τέτοιες μεθοδολογίες είναι για παράδειγμα η Cramm [20][21], η Ebios [22], η Magerit [24][25] και άλλες. Πολλές από αυτές τις μεθοδολογίες διαθέτουν και κάποια εργαλεία που αυτοματοποιούν τις διαδικασίες ανάλυσης και διαχείρισης του κινδύνου και έτσι εξυπηρετούν τον οργανισμό στην δημιουργία μιας στρατηγικής ασφαλείας για την προστασία του πληροφοριακού του συστήματος.

Στον πίνακα που ακολουθεί παρατίθενται ορισμένες μεθοδολογίες και κάποια από τα βασικά κριτήρια με τα οποία γίνεται η αξιολόγηση τους, όπως είναι η συνεργατικότητα, το κόστος και η συμβατότητα με πρότυπα διαχείρισης ασφαλείας, όπως εκείνα που αναφέρθηκαν στο τρίτο κεφάλαιο [19][23][26][27].

Πίνακας 4. 1 Μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας

	Κόστος	**Εργαλείο**	**Κόστος Εργαλείου**	**Συνεργατικότητα**	**Γλώσσες**	**Συμβατότητα με Πρότυπα**	**Απαιτούμενο Επίπεδο Δεξιοτήτων**	**Απευθυνόμενοι οργανισμοί**
Cramm	Εμπορικό	Ναι	Εμπορικό	Όχι	Αγγλικά, Γερμανικά, Τσέχικα	Ναι	Υψηλό	Κυβερνητικοί φορείς, Μεγάλες επιχειρήσεις
Ebios	Δωρεάν	Ναι	Δωρεάν	Όχι	Αγγλικά, Γαλλικά, Γερμανικά, Ισπανικά	Ναι	Κανονικό	Κυβερνητικοί φορείς, Μεγάλες επιχειρήσεις, Μικρομεσαίες Επιχειρήσεις
Magerit	Δωρεάν	Ναι	Εμπορικό	Όχι	Αγγλικά, Ιταλικά, Ισπανικά	Ναι	Υψηλό	Κυβερνητικοί φορείς, Μεγάλες επιχειρήσεις, Μικρομεσαίες Επιχειρήσεις
Mehari	Εμπορικό	Ναι	Εμπορικό	Όχι	Πολύγλωσσο	Ναι	Κανονικό	Κυβερνητικοί φορείς, Μεσαίες προς μεγάλες επιχειρήσεις, Μη κερδοσκοπικοί οργανισμοί
Octave	Δωρεάν	Ναι	Εμπορικό	Ναι	Αγγλικά	Όχι	Κανονικό	Μικρομεσαίες Επιχειρήσεις

4.5 Συνεργατική μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας STORM-RM

Η STORM-RM (Secure Tool for Risk Management – Risk management Methodology) [29] είναι μια συνεργατική μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας, η οποία εμπλέκει όλες τις ομάδες χρηστών (μέλη διοίκησης, ομάδα ασφάλειας, διαχειριστές και τελικοί χρήστες του πληροφοριακού συστήματος) του υπό εξέταση οργανισμού σε όλη τη διαδικασία της ανάλυσης και διαχείρισης επικινδυνότητας.

Συγκεκριμένα η μεθοδολογία STORM-RM αντιμετωπίζει την ανάλυση και διαχείριση επικινδυνότητας ως ένα πολυκριτηριακό πρόβλημα όπου εμπλέκονται πολλοί χρήστες βασιζόμενοι στο γνωστικό τους επίπεδο και την εμπειρία τους. Στους υπολογισμούς της προτεινόμενης μεθοδολογίας, χρησιμοποιείται η πολυκριτηριακή μεθοδολογία Analytical Hierarchy Process (AHP). Πιο αναλυτικά, χρησιμοποιούνται διαφορετικά βάρη συμμετοχής για τις ομάδες χρηστών που λαμβάνουν μέρος στην διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας και με αυτόν τον τρόπο οδηγούμαστε σε πιο αντικειμενικά αποτελέσματα.

4.5.1 Πεδίο εφαρμογής και στόχοι της STORM-RM

Το πεδίο εφαρμογής της μεθοδολογίας STORM-RM περιλαμβάνει πληροφοριακά συστήματα τα οποία υποστηρίζουν κρίσιμες η-υπηρεσίες των υπό εξέταση οργανισμών και τις επιχειρησιακές λειτουργίες τους. Επίσης το πεδίο εφαρμογής της μεθοδολογίας περιέχει τον προσδιορισμό των κρίσιμων η-υπηρεσιών, την ανάλυση επικινδυνότητας και τον προσδιορισμό των βασικότερων κινδύνων, καθώς και τις διαδικασίες της διαχείρισης επικινδυνότητας και του προσδιορισμού των κατάλληλων μέτρων ασφάλειας [28].

Στόχος της STORM-RM είναι η κάλυψη των βασικών αναγκών ασφάλειας και η υποστήριξη των φάσεων της ανάλυσης επικινδυνότητας που αναφέρονται παρακάτω:

- Συμβατότητα με τις απαιτήσεις των διεθνών προτύπων ασφάλειας πληροφοριακών συστημάτων (ISO 27001:2005, ISO 27005:2008).
- Υποστήριξη της συμμετοχής όλων των χρηστών του πληροφοριακού συστήματος του υπό εξέταση οργανισμού στην ανάλυση επικινδυνότητας.
- Συμβατότητα με τη φύση των κρίσιμων υποδομών και τις απαιτήσεις ασφάλειας τους.
- Συμβατότητα με τη σχετική νομοθεσία.

4.5.2 Απαιτήσεις και χαρακτηριστικά STORM-RM

4.5.2.1 Απαιτήσεις της μεθοδολογίας

Η συνεργατική μεθοδολογία STORM-RM καλύπτει ορισμένες απαιτήσεις οι οποίες παρουσιάζονται παρακάτω [29]:

- **Φιλικότητα.** Απευθύνεται σε όλους τους χρήστες του υπό μελέτη πληροφοριακού συστήματος, ακόμα και σε εκείνους που δεν έχουν τις απαιτούμενες γνώσεις και εμπειρία σε θέματα ασφάλειας.
- **Προσαρμοστικότητα.** Υπάρχει η δυνατότητα εφαρμογής σε διαφορετικής φύσης και μεγέθους οργανισμούς.
- **Εύκολα Υλοποιήσιμη.** Είναι αλγοριθμική μεθοδολογία και επομένως μπορεί να υλοποιηθεί με τη χρήση γνωστών γλωσσών προγραμματισμού ως αυτοματοποιημένο εργαλείο ανάλυσης και διαχείρισης επικινδυνότητας.
- **Συμβατότητα με τα Πρότυπα Ασφάλειας.** Η μεθοδολογία καλύπτει όλες τις απαιτήσεις και τις βασικές οδηγίες που περιλαμβάνουν τα πρότυπα ασφάλειας πληροφοριακών συστημάτων.
- **Επεκτασιμότητα.** Υπάρχει η δυνατότητα επέκτασης της μεθοδολογίας ώστε να ανταποκρίνεται στην πραγματική εικόνα των οργανισμών που εξετάζονται.

4.5.2.2 Χαρακτηριστικά της μεθοδολογίας

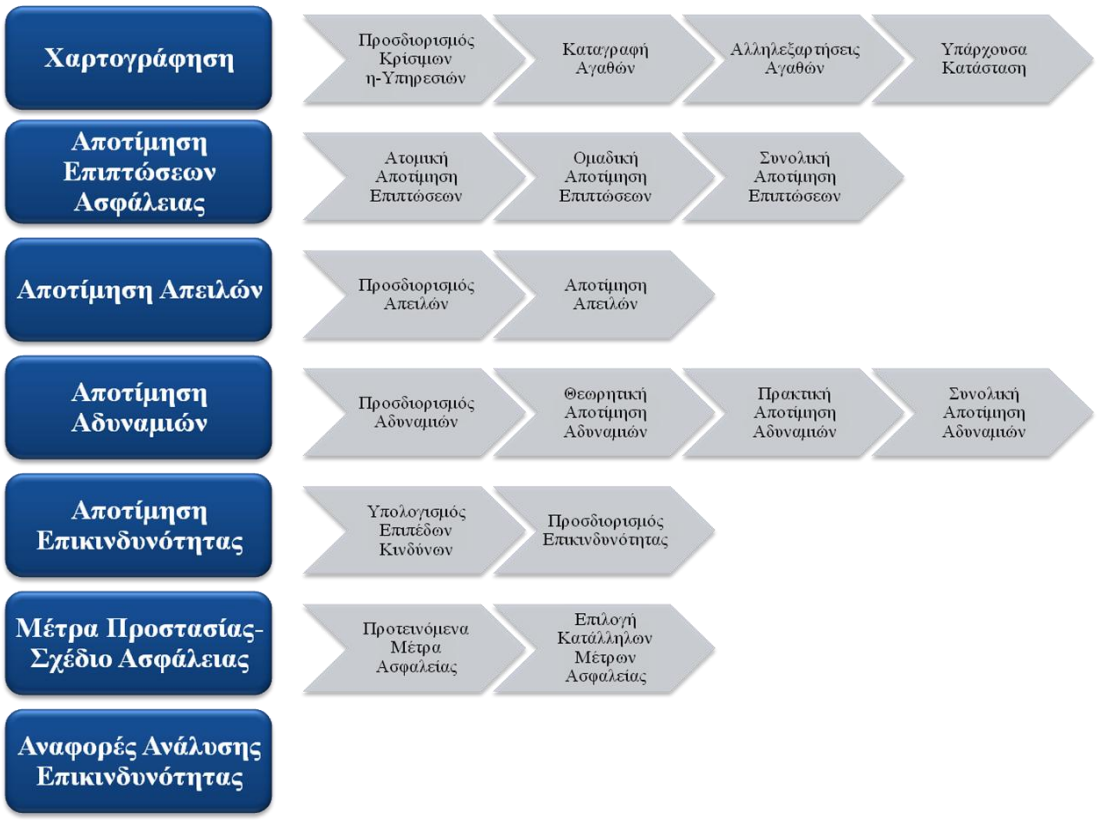
Στην συγκεκριμένη ενότητα παρουσιάζονται τα χαρακτηριστικά της συνεργατικής μεθοδολογίας STORM-RM και είναι τα εξής:

- **Συνεργατικότητα.** Η συγκεκριμένη μεθοδολογία αντιμετωπίζει το πρόβλημα της ανάλυσης και διαχείρισης επικινδυνότητας ως ένα συνεργατικό πρόβλημα, όπου συμμετέχουν πολλές διαφορετικές ομάδες χρηστών του πληροφοριακού συστήματος.
- **Προσανατολισμένη προς τους χρήστες του υπό εξέταση πληροφοριακού συστήματος.** Στόχος της μεθοδολογίας είναι η καθοδήγηση από τους ίδιους τους χρήστες του πληροφοριακού συστήματος.
- **Ελάττωση πολυπλοκότητας.** Οι χρήστες συμμετέχουν μόνο στα στάδια της μεθοδολογίας που μπορούν να κατανοήσουν και η συμμετοχή τους είναι πιο ωφέλιμη, ενώ απαιτείται από τους χρήστες η κατανόηση μόνο των στόχων και των τελικών αποτελεσμάτων και όχι όλης της συλλογιστικής.
- **Ανθεκτικότητα σε σφάλματα.** Η STORM-RM μέσα από την συμμετοχή στη διαδικασία πολλών διαφορετικών ομάδων χρηστών μπορεί να διορθώσει λανθασμένα δεδομένα εισόδου.

- **Αλγοριθμική.** Είναι αλγοριθμική μεθοδολογία και επομένως, όπως αναφέρθηκε και παραπάνω, μπορεί να υλοποιηθεί με τη χρήση γνωστών γλωσσών προγραμματισμού ως αυτοματοποιημένο εργαλείο ανάλυσης και διαχείρισης επικινδυνότητας.
- **Επεκτασιμότητα και προσαρμοστικότητα.** Η λογική με την οποία η μεθοδολογία λαμβάνει υπόψη τις γνώμες των διαφορετικών χρηστών μπορεί να παραμετροποιηθεί ανάλογα με τις απαιτήσεις του υπό εξέταση οργανισμού. Επίσης μπορεί να εφαρμοστεί σε διαφορετικής φύσης και μεγέθους οργανισμούς [28].

4.5.3 Φάσεις της μεθοδολογίας STORM-RM

Στην εικόνα που ακολουθεί παρουσιάζονται οι 7 βασικές φάσεις από τις οποίες αποτελείται η μεθοδολογία καθώς τα επιμέρους στάδια από τα οποία συντελείται η κάθε μία [29].



Εικόνα 4. 3 Φάσεις μεθοδολογίας STORM-RM [29]

5ο ΚΕΦΑΛΑΙΟ

Πολυκριτήρια Λήψη Αποφάσεων

5 Πολυκριτήρια Λήψη Αποφάσεων

5.1 Εισαγωγή

Η διαπίστωση ότι η επίλυση πολύπλοκων και σημαντικών προβλημάτων λήψης αποφάσεων δεν μπορεί να πραγματοποιείται μέσω μίας μονόπλευρης και μονοδιάστατης ανάλυσης οδήγησε στην ανάπτυξη και διάδοση της πολυκριτήριας ανάλυσης αποφάσεων (Multicriteria Decision Aid - MCDA, ή Multicriteria Decision Making - MCDM).

Η διαδικασία λήψης μιας απόφασης είναι η διαδικασία εκείνη που αποσκοπεί στην επιλογή μιας δράσης ανάμεσα από ένα σύνολο εναλλακτικών επιλογών. Η λήψη απόφασης γίνεται από τον αποφασίζοντα (Decision Maker), ο οποίος συγκρίνει και αξιολογεί τις εναλλακτικές δράσεις ώστε να επιλεχθεί τελικά η καταλληλότερη λύση για το αντίστοιχο πρόβλημα.

Η Πολυκριτήρια Λήψη Αποφάσεων (Multiple Criteria Decision Making - MCDM) είναι ο κλάδος της Επιχειρησιακής Έρευνας που ασχολείται με την επίλυση προβλημάτων, λαμβάνοντας υπόψη περισσότερα από ένα κριτήρια απόφασης.

Ωστόσο, κατά την προσπάθεια εξέτασης όλων των παραμέτρων ενός προβλήματος και των κριτηρίων που επηρεάζουν τη λήψη της κατάλληλης απόφασης, δημιουργείται το πρόβλημα σύνθεσης τον παραγόντων για την ορθή λήψη αποφάσεων. Η πολυκριτήρια ανάλυση αποφάσεων έχει ως βασικό αντικείμενο την αντιμετώπιση του προβλήματος αυτού.

Κύριο χαρακτηριστικό και σημαντική διαφορά της πολυκριτήριας ανάλυσης από άλλες εναλλακτικές προσεγγίσεις είναι ότι η αναγκαία σύνθεση πραγματοποιείται λαμβάνοντας υπόψη την πολιτική λήψης των αποφάσεων και το σύστημα προτιμήσεων και αξιών, το οποίο χρησιμοποιείται συνειδητά ή ασυνείδητα από τον αποφασίζοντα. Έτσι, η πολυκριτήρια ανάλυση αποφάσεων ενσωματώνει τον αποφασίζοντα και τις προτιμήσεις του στη διαδικασία ανάπτυξης των υποδειγμάτων, χωρίς να του προσδίδει απλά έναν παθητικό ρόλο και να περιορίζει τη συμμετοχή του στην παρακολούθηση και εφαρμογή των αποτελεσμάτων μαθηματικών μοντέλων.

Στις ενότητες που ακολουθούν παρουσιάζονται αναλυτικά οι βασικές έννοιες και τα στάδια μοντελοποίησης της πολυκριτήριας λήψης αποφάσεων καθώς και διάφορες κατηγοριοποιήσεις των αντίστοιχων μεθοδολογιών. Τέλος παρουσιάζεται η μέθοδος που επιλέχθηκε για την επίλυση του προβλήματος, η οποία είναι μια πολυκριτήρια προσέγγιση βασισμένη στον συναινετικό προγραμματισμό.

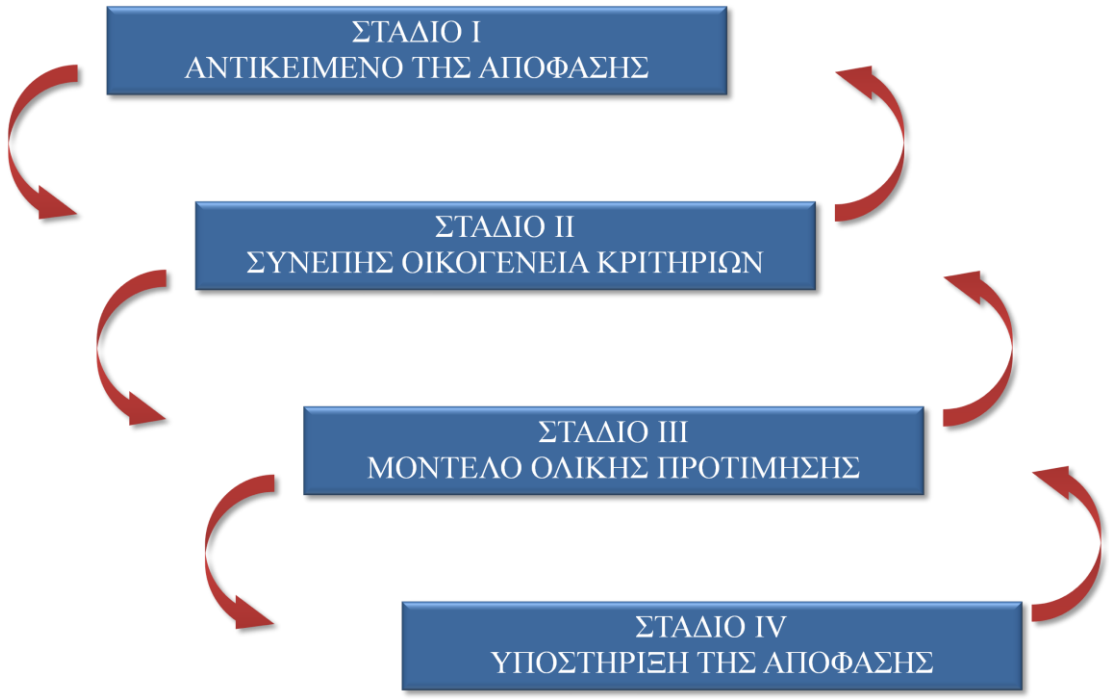
5.2 Διαδικασία μοντελοποίησης προβλημάτων απόφασης

Η διαδικασία της μοντελοποίησης προβλημάτων απόφασης αφορά περισσότερο στην παρέμβαση του αναλυτή ή μελετητή του προβλήματος στην διαδικασία της απόφασης. Ο ρόλος του αναλυτή διακρίνεται από εκείνον του αποφασίζοντος, από το γεγονός ότι η δραστηριότητα του αναλυτή στηρίζεται σε μοντέλα περισσότερο ή λιγότερο μαθηματικοποιημένα.

Ο Bernard Roy(1985), ένας εκ των θεμελιωτών της σύγχρονης ιστορίας της πολυκριτήριας ανάλυσης, από τα μέσα της δεκαετίας του 1970 προτείνει ένα γενικό μεθοδολογικό πλαίσιο μοντελοποίησης προκειμένου να αναλύσει και να οριοθετήσει τις δραστηριότητες του αναλυτή [32].

Το γενικό αυτό μεθοδολογικό πλαίσιο αποτελείται από 4 στάδια όπως φαίνεται συνοπτικά στο παρακάτω σχήμα. Τα στάδια λήψης αποφάσεων που προτείνει ο Roy δεν είναι αναγκαίο να υλοποιούνται διαδοχικά, αλλά ο αναλυτής μπορεί να ανατρέξει σε οποιοδήποτε στάδιο αν διαπιστώσει ότι υπάρχει κάποιο σφάλμα ή ότι η πληροφόρηση είναι ελλιπής.

Το παρακάτω σχήμα αποτελεί τη βάση για τη λήψη κάθε πολυκριτήριας απόφασης, και χαρακτηρίζει τη λογική όλων των μεθοδολογιών του χώρου, αντιμετωπίζοντας από τα απλά ως τα πιο σύνθετα προβλήματα του μάνατζμεντ.



Εικόνα 5. 1 Διαδικασία μοντελοποίησης προβλημάτων απόφασης [32]

5.2.1 Στάδιο Ι: Αντικείμενο της απόφασης

Το αρχικό στάδιο του μεθοδολογικού πλαισίου της πολυκριτήριας ανάλυσης αποφάσεων αφορά στον προσδιορισμό του προβλήματος που απαιτεί τη λήψη μιας απόφασης. Το στάδιο αυτό αποτελείται από δύο βασικές ενέργειες, τον αυστηρό ορισμό του συνόλου Α των δράσεων και τον καθορισμό μιας προβληματικής.

Την πρώτη εργασία αποτελεί ο **αυστηρός ορισμός του συνόλου Α των εναλλακτικών δράσεων**, δηλαδή ο καθορισμός των εναλλακτικών δραστηριοτήτων που αποτελούν τη λύση του προβλήματος προς εξέταση. Το σύνολο Α των δράσεων μπορεί να είναι συνεχές ή διακριτό.

Η ενέργεια που έπεται του προσδιορισμού του συνόλου Α των δράσεων είναι ο **καθορισμός της προβληματικής**. Στη φάση αυτή καθορίζεται ο τρόπος με τον οποίο θα εξεταστούν οι εναλλακτικές δράσεις. Οι προβληματικές αναφοράς μπορούν να διακριθούν σε τέσσερις κατηγορίες όπως φαίνεται παρακάτω:

1. **Προβληματική α: επιλογή** μίας και μόνο δράσης από το σύνολο Α.
2. **Προβληματική β: ταξινόμηση** των δράσεων σε ομογενείς προκαθορισμένες κατηγορίες, οι οποίες είναι διατεταγμένες ως προς τις προτιμήσεις του αποφασίζοντος.
3. **Προβληματική γ: κατάταξη** των δράσεων του συνόλου Α από την καλύτερη έως τη χειρότερη.
4. **Προβληματική δ: περιγραφή** των δράσεων και των συνεπειών τους στη γλώσσα των εμπλεκόμενων στη διαδικασία της απόφασης.

Η επιλογή μίας μόνο προβληματικής δεν παραμένει αναγκαστικά σταθερή καθ' όλη τη διάρκεια της διαδικασίας απόφασης, αλλά μπορεί να χρησιμοποιηθεί και συνδυασμός προβληματικών ανάλογα με την πολυπλοκότητα και τις απαιτήσεις του προβλήματος [33].

5.2.2 Στάδιο ΙΙ: Συνεπής οικογένεια κριτηρίων

Στο δεύτερο στάδιο της διαδικασίας προσδιορίζονται οι παράγοντες που επιδρούν στην λήψη της απόφασης. Στα πλαίσια της πολυκριτήριας ανάλυσης αποφάσεων κάθε παράγοντας που επιδρά στη λήψη της απόφασης θεωρείται ότι έχει τη μορφή ενός κριτηρίου. Κάθε δράση από το σύνολο Α εκπέμπει ένα *νέφος στοιχειωδών επιπτώσεων* (Roy 1985) [32].

5.2.2.1 Μοντελοποίηση κριτηρίων

Ο ρόλος του αναλυτή συνίσταται στη διασαφήνιση των επιπτώσεων των δράσεων του συνόλου Α και στη συνέχεια στον εντοπισμό και μοντελοποίηση των κριτηρίων βάση των οποίων θα ληφθεί η απόφαση. Αποτέλεσμα της διαδικασίας αυτής είναι η κατασκευή ενός συστήματος κριτηρίων που αποκαλείται **«συνεπής οικογένεια κριτηρίων»**. Για το συγκεκριμένο στάδιο ο Bernard Roy (1985) προτείνει μια διαδικασία που περιγράφει τις δραστηριότητες του αναλυτή του προβλήματος, η οποία παρουσιάζεται στο παρακάτω σχήμα [32].

Εικόνα 5. 2 Διαδικασία κατασκευής συνεπούς οικογένειας κριτηρίων [32]

Μετά τον αυστηρό ορισμό του συνόλου των δράσεων ο αναλυτής καταγράφει όλες τις στοιχειώδεις επιπτώσεις των δράσεων την μια μετά την άλλη, ενώ πολλές από τις οποίες μπορεί να είναι κοινές**.** *Στοιχειώδης επίπτωση* μιας δράσης a ονομάζεται κάθε ιδιότητα ή χαρακτηριστικό της δράσης a η οποία είναι α) επαρκώς καθορισμένη ως προς το περιεχόμενο της ώστε να μπορούν οι εμπλεκόμενοι να κατανοήσουν τη σημασία της και β) επιτρέπει την περιγραφή κάποιου συγκεκριμένου αποτελέσματος που έπεται της επιλογής της δράσης a.

Στην συνέχεια ο αναλυτής κατηγοριοποιεί τις επιπτώσεις καθορίζοντας έτσι τους *άξονες προτίμησης*, το σύνολο δηλαδή των στοιχειωδών επιπτώσεων που

αναφέρονται στον ίδιο στόχο μέσω των οποίων θα αξιολογηθούν και θα συγκριθούν οι δράσεις.

Επόμενο βήμα της διαδικασίας είναι η επιλογή κλιμάκων προτίμησης, η οποία δίνει υπόσταση στις διαστάσεις στο πλαίσιο κάθε άξονα προτίμησης. Τέλος, τα κριτήρια κατασκευάζονται είτε με ταύτιση τους με διαστάσεις, είτε με διάσπαση διαστάσεων, είτε με σύμπτυξη διαστάσεων. Σε κάθε περίπτωση πάντως ένα κριτήριο ορίζεται μέσω μιας κλίμακας προτίμησης.

Κλίμακα προτίμησης είναι ένα σύνολο καταστάσεων ή στοιχείων, τα οποία ονομάζονται βαθμίδες της κλίμακας και ορίζουν μια διάταξη ως προς τις προτιμήσεις ενός εμπλεκόμενου στη διαδικασία λήψης της απόφασης. Η κλίμακα προτίμησης μπορεί να είναι είτε *ποσοτική/μετρική***,** είτε *διάταξης*. Επίσης, *διάσταση* αποκαλείται μια στοιχειώδης επίπτωση τέτοια ώστε το σύνολο των καταστάσεων που αυτή υπαγορεύει να ορίζει μια κλίμακα προτίμησης [33].

5.2.2.2 Αυστηρός ορισμός κριτηρίου

Στη μαθηματική γλώσσα ένα κριτήριο μοντελοποιείται από μια πραγματική συνάρτηση:

$$g: A \rightarrow R \,/\, a \rightarrow g\,(a) \qquad (5.1)$$

όπου g (a) είναι η *τιμή ή αξιολόγηση* της δράσης a $\mathcal{E}$ A πάνω στο κριτήριο g. Η συνάρτηση αυτή πρέπει να πληροί την ιδιότητα της συνέπειας ή μονοτονίας. Αν δηλαδή a και b είναι δύο δράσεις του συνόλου A ισχύει ότι

$$g(a) > g(b) \Leftrightarrow aSb \qquad (5.2)$$

όπου aSb σημαίνει ότι η δράση a υπερέχει της b. Η *σχέση υπεροχής S* είναι σύνθετη και εμπεριέχει χωρίς σαφή διάκριση τις *σχέσεις της αδιαφορίας*, της *ασθενούς προτίμησης* και της *ισχυρής προτίμησης* [33].

5.2.2.3 Συνεπής οικογένεια κριτηρίων

Ένα σύστημα αξιολόγησης των εναλλακτικών δράσεων του προβλήματος μοντελοποιείται μέσω μιας **συνεπούς οικογένειας κριτηρίων** F= $(g_1, g_2, \ldots, g_n)$ η οποία περιλαμβάνει n κριτήρια τα οποία πρέπει να πληρούν τις παρακάτω προϋποθέσεις:

1) Συνέπεια ή μονοτονία. Αν για ένα ζεύγος δράσεων (a,b) ισχύει: $g_i(a) = g_i(b)$, για κάθε $i \neq j$ και $g_j(a) > g_j(b)$, τότε η δράση a υπερέχει της b.

2) Επάρκεια. Αν για ένα ζεύγος δράσεων (a,b) ισχύει: $g_i(a) = g_i(b)$ για κάθε i= 1, 2,…, n τότε η δράση a είναι αδιάφορη της b, δηλαδή δεν απουσιάζει κανένα κριτήριο από το σύνολο των n κριτηρίων

3) Μη πλεονασμός. Η διαγραφή ενός κριτηρίου g_i από το σύνολο των κριτηρίων είναι ικανή να αναιρέσει μια από τις προηγούμενες δύο συνθήκες για κάποια ζεύγη δράσεων.

Τέλος με $g(a) = (g_1(a), g_2(a), \ldots, g_n(a))$ συμβολίζουμε το διάνυσμα των τιμών της δράσης a $\mathcal{E}$ A πάνω στα n κριτήρια, το ποίο ονομάζουμε **πολυκριτήρια αξιολόγηση** της δράσης a [33].

5.2.2.4 Τύποι κριτηρίων

- **Κριτήρια ποσοτικά ή μετρικά.** Πρόκειται για κριτήρια των οποίων η κλίμακα προτίμησης είναι μια κλίμακα μέτρου. Ένα ποσοτικό κριτήριο επιτρέπει τη σύγκριση διαστημάτων στο εσωτερικό της κλίμακας. Αν ο αποφασίζων έχει ορίσει κατώφλια αδιαφορίας και προτίμησης για την κλίμακα τιμών ενός κριτηρίου τότε το κριτήριο αυτό μπορεί να είναι ένα *ημικριτήριο, προκριτήριο* ή *ψευδοκριτήριο*.

- **Κριτήρια ποιοτικά ή διάταξης.** Πρόκειται για κριτήρια των οποίων η κλίμακα προτίμησης είναι μια κλίμακα διάταξης. Ένα κριτήριο διάταξης ορίζει μόνο μια προδιάταξη (διάταξη με ισοδυναμίες πάνω στο σύνολο των δράσεων). Σε μερικές ωστόσο περιπτώσεις μπορεί να συνοδεύεται και από ένα κατώφλι προτίμησης.

- **Κριτήρια πιθανοτικά.** Πρόκειται για κριτήρια στα οποία η αξιολόγηση μιας δράσης είναι κατά πιθανότητα γνωστή πάνω στην κλίμακα του κριτηρίου. Αν $[g_*, g^*]$ είναι η κλίμακα του κριτηρίου g τότε η τιμή της δράσης a ορίζεται μέσω μιας πυκνότητας πιθανότητας δ^a για την οποία ισχύει ότι

$$\sum_j \delta^a(g^j) = 1 \text{ , όταν είναι διακριτή η κλίμακα} \qquad (5.3)$$

$$\int_{G_*}^{g^*} \delta^a(g)\mathrm{d}g = 1 \text{ , όταν είναι συνεχής η κλίμακα} \qquad (5.4)$$

- **Κριτήρια ασαφή.** Πρόκειται για κριτήρια στα οποία η αξιολόγηση μιας δράσης είναι ένα διάστημα της κλίμακας του κριτηρίου, όπου έχει οριστεί μια *συνάρτηση δυνατότητας* που δείχνει πόσο δυνατή είναι μια τιμή του κριτηρίου.

5.2.3 Στάδιο ΙΙΙ: Μοντέλο ολικής προτίμησης

Στα δύο προηγούμενα στάδια της ανάλυσης καταλήξαμε στον καθορισμό του αντικειμένου της απόφασης και την κατασκευή της συνεπούς οικογένειας κριτηρίων. Το παρόν στάδιο αφορά τον κανόνα σύνθεσης των μοντέλων μερικής προτίμησης, δηλαδή των κριτηρίων [33].

Ο ρόλος του αναλυτή είναι να καθορίσει μια μέθοδο πολυκριτήριας σύνθεσης με βάση την οποία θα γίνει η σύγκριση των εναλλακτικών δράσεων του συνόλου Α, λαμβάνοντας υπόψη τις τιμές των δράσεων αυτών πάνω στα κριτήρια της συνεπούς οικογένειας κριτηρίων.

Το μοντέλο ολικής προτίμησης μπορεί να χρησιμοποιηθεί ως βάση για:

1. Τον προσδιορισμό μιας συνολικής αξιολόγησης κάθε εναλλακτικής
2. Την πραγματοποίηση διμερών συγκρίσεων μεταξύ των εναλλακτικών.
3. Τη διερεύνηση του συνόλου των εναλλακτικών λύσεων, όταν αυτό είναι συνεχές.

Η ανάπτυξη του μοντέλου ολικής προτίμησης μπορεί να πραγματοποιηθεί με δύο τρόπους:

1. Αλληλεπιδραστικά μέσω της συνεργασίας του αναλυτή με τον αποφασίζοντα. Στην προσέγγιση αυτή ο αποφασίζων καθορίζει ένα σύνολο παραμέτρων σχετικών με την πολιτική λήψης των αποφάσεων που ακολουθεί (για παράδειγμα, τα βάρη των κριτηρίων).
2. Αναλύοντας τις αποφάσεις που λαμβάνει ο αποφασίζων έτσι ώστε να αναπτυχθεί το κατάλληλο μοντέλο ολικής προτίμησης που είναι συμβατό με την πολιτική λήψης των αποφάσεων που ακολουθεί ο αποφασίζων. Η προσέγγιση αυτή έχει αρκετές ομοιότητες με τη μεθοδολογία της παλινδρόμησης η οποία είναι ιδιαίτερα διαδεδομένη στο χώρο της στατιστικής.

5.2.4 Στάδιο IV: Υποστήριξη της απόφασης

Το τελευταίο στάδιο του μεθοδολογικού πλαισίου της πολυκριτήριας ανάλυσης αποφάσεων είναι η υποστήριξη της απόφασης. Η λύση που δίνει ένα μοντέλο μπορεί να μην είναι άμεσα κατανοητή και εκμεταλλεύσιμη από τον αποφασίζοντα, γι' αυτό στο συγκεκριμένο στάδιο πραγματοποιούνται όλες οι ενέργειες που θα βοηθήσουν τον αποφασίζοντα να κατανοήσει τα αποτελέσματα και τη διαδικασία με την οποία εξήχθησαν.

Συγκεκριμένα στο στάδιο αυτό ο αναλυτής συγκεντρώνει και οργανώνει τα στοιχεία της απάντησης σε συγκεκριμένα ερωτήματα που έχουν θέσει ή ενδέχεται να θέσουν οι συμμετέχοντες στην διαδικασία της απόφασης και κυριότερα ο αποφασίζων. Οι τεχνικές που εξυπηρετούν την αρτιότερη υποστήριξη των διάφορων επιλογών εξαρτώνται από το μοντέλο ολικής προτίμησης που έχει επιλεγεί στο προηγούμενο στάδιο(Σίκσος 2008) [33].

5.3 Κατηγοριοποίηση μεθόδων πολυκριτήριας λήψης αποφάσεων

Ο χώρος της πολυκριτήριας ανάλυσης αποφάσεων περιλαμβάνει ένα ευρύ φάσμα μεθοδολογιών για την πολυκριτήρια λήψη αποφάσεων μεταξύ των οποίων υπάρχουν σημαντικές διαφοροποιήσεις στη μορφή των μεθόδων που αναπτύσσονται καθώς και στη διαδικασία που χρησιμοποιείται για την ανάπτυξη τους.

Για την πολυκριτήρια λήψη αποφάσεων έχουν αναπτυχθεί διάφορες μεθοδολογικές προσεγγίσεις, οι οποίες μπορούν να χωριστούν σε διάφορες κατηγορίες όπως παρουσιάζεται παρακάτω.

Ο Σίσκος (2008) χωρίζει τα μοντέλα σύνθεσης πολλαπλών κριτηρίων σε δύο κατηγορίες [33]:

- **Αντισταθμιστικά μοντέλα:** Πρόκειται για μοντέλα στα οποία η υποβάθμιση ενός κριτηρίου μπορεί να αποζημιωθεί από τη βελτίωση της τιμής ενός άλλου κριτηρίου.
- **Μη αντισταθμιστικά μοντέλα:** Πρόκειται για μοντέλα στα οποία η αντιστάθμιση ενός κριτηρίου από ένα άλλο δεν είναι επιτρεπτή.

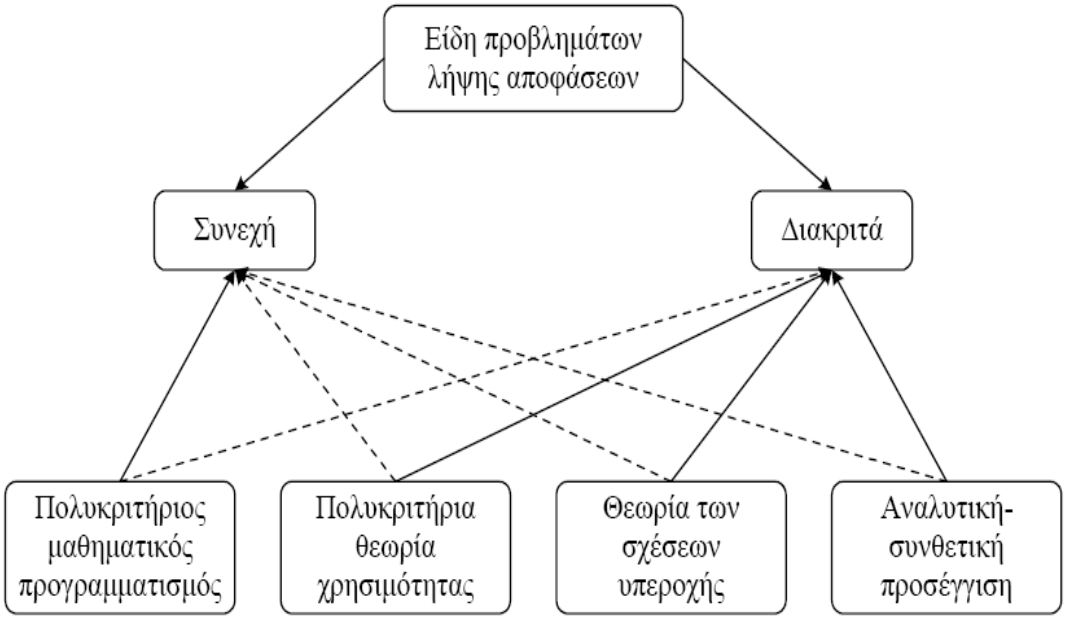
Επίσης, ο ίδιος (Σίσκος 2008), από θεωρητικής πλευράς, ταξινομεί τις κυριότερες κατηγορίες πολυκριτήριων μεθόδων ως εξής [33]:

- **Συναρτησιακές Μέθοδοι:** Η σύνθεση των κριτηρίων επιτυγχάνεται μέσω μιας ή περισσοτέρων συναρτήσεων αξίας χρησιμότητας.
- **Σχεσιακές Μέθοδοι:** Η σύνθεση των κριτηρίων επιτυγχάνεται μέσω μιας ή περισσοτέρων συναρτήσεων υπεροχής.
- **Αναλυτικές Μέθοδοι:** Το μοντέλο σύνθεσης των κριτηρίων συμπεραίνεται έμμεσα από δεδομένα ολικής προτίμησης του αποφασίζοντος.

Μια ακόμα εναλλακτική κατηγοριοποίηση των πολυκριτήριων μεθόδων προτάθηκε από τους Pardalos et al. (1995), ανάλογα με τη μορφή του μοντέλου ολικής προτίμησης που χρησιμοποιούν, αλλά και τη διαδικασία ανάπτυξης του μοντέλου. Βάση της θεώρησης αυτής προτάθηκε η ταξινόμηση που ακολουθεί [31]:

- Πολυκριτήριος μαθηματικός προγραμματισμός
- Πολυκριτήρια θεωρία χρησιμότητας
- Θεωρία των σχέσεων υπεροχής
- Αναλυτική-συνθετική προσέγγιση

Στο ακόλουθο σχήμα οι συνεχείς γραμμές συμβολίζουν την άμεση συμβολή του κάθε μεθοδολογικού ρεύματος της πολυκριτήριας ανάλυσης στην αντιμετώπιση του υποδεικνυόμενου είδους προβλημάτων λήψης αποφάσεων, ενώ οι διακεκομμένες γραμμές συμβολίζουν την έμμεση συμβολή.



Εικόνα 5. 3 Συμβολή των θεωρητικών ρευμάτων της πολυκριτήριας ανάλυσης στην επίλυση συνεχών και διακριτών προβλημάτων λήψης αποφάσεων

Όπως φαίνεται από το παραπάνω σχήμα η πολυκριτήρια θεωρία χρησιμότητας, η θεωρία των σχέσεων υπεροχής και η αναλυτική-συνθετική προσέγγιση, προσανατολίζονται προς την αντιμετώπιση διακριτών προβλημάτων λήψης αποφάσεων, ενώ ο πολυκριτήριος μαθηματικός προγραμματισμός προς την αντιμετώπιση συνεχών. Ωστόσο οι τρείς τελευταίες κατηγορίες μπορούν να χρησιμοποιηθούν και ως εργαλεία για την αντιμετώπιση συνεχών προβλημάτων, συμβάλλοντας στην αποτύπωση του συστήματος αξιών και προτιμήσεων του αποφασίζοντος σε ένα μαθηματικό υπόδειγμα. Αντίστοιχα, και ο πολυκριτήριος μαθηματικός προγραμματισμός μπορεί να συμβάλλει στην αντιμετώπιση διακριτών προβλημάτων [30].

5.4 Πολυκριτήρια προσέγγιση του προβλήματος βασισμένη στον συναινετικό προγραμματισμό

Η μεθοδολογία που επιλέχθηκε για την επίλυση του προβλήματος της επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων είναι μια πολυκριτήρια προσέγγιση βασισμένη στον συναινετικό προγραμματισμό. Στην συνέχεια της ενότητας παρατίθενται όλοι οι ορισμοί και οι βασικές έννοιες που είναι απαραίτητες για την κατανόηση και εφαρμογή της συγκεκριμένης μεθοδολογίας [34].

Ο πολυκριτήριος ή αλλιώς πολυστοχικός γραμμικός προγραμματισμός αποτελεί γενίκευση αλλά ταυτόχρονα αναπόσπαστο μέρος του γραμμικού προγραμματισμού και χαρακτηρίζεται από την ύπαρξη πολλαπλών αντικειμενικών συναρτήσεων υπό μεγιστοποίηση(ελαχιστοποίηση).

Η γενική μορφή ενός πολυκριτήριου προγράμματος μεγιστοποίησης ή ελαχιστοποίησης είναι η παρακάτω:

Να μεγιστοποιηθούν οι n αντικειμενικές συναρτήσεις:

$$g_1(x) = c_{11}x_1 + c_{12}x_2 + \cdots + c_{1l}x_l$$

$$g_2(x) = c_{21}x_1 + c_{22}x_2 + \cdots + c_{2l}x_l$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$g_n(x) = c_{n1}x_1 + c_{n2}x_2 + \cdots + c_{nl}x_l \qquad (5.5)$$

υπό τους περιορισμούς

$x \in A = \{ x \in R^l / Ax \leq b, x \geq 0 \}$

όπου A είναι η επιτρεπτή περιοχή των λύσεων η οποία οριοθετείται από σύστημα γραμμικών ανισοεξισώσεων και A,x και b είναι αντίστοιχα μήτρες διαστάσεων $m \times l$, $l \times 1$ και $m \times 1$.

Μια βασική έννοια και αναπαράσταση του ανταγωνισμού μεταξύ των πολλαπλών αντικειμενικών συναρτήσεων είναι ο **πίνακας πληρωμών ή κερδών**. Συνίσταται στη βελτιστοποίηση καθεμίας χωριστά αντικειμενικής συνάρτησης $g_i(x)$, i=1,2,…., n και την αντικατάσταση της εκάστοτε βέλτιστης λύσης στις υπόλοιπες αντικειμενικές συναρτήσεις.

Τα στοιχεία των ενεργειών αυτών, μεταφέρονται σε έναν πίνακα, ο οποίος περιέχει σε κάθε γραμμή τη βελτιστοποίηση που πραγματοποιείται, τις τιμές της βέλτιστης λύσης πάνω σε όλες τις αντικειμενικές συναρτήσεις και τις τιμές των μεταβλητών απόφασης, εφόσον το πλήθος τους είναι μικρό, αλλιώς παραλείπονται. Ο πίνακας πληρωμών παρέχει πολύ χρήσιμα στοιχεία, τόσο για την ποιότητα των λύσεων στις οποίες οδηγούν οι αντικειμενικές συναρτήσεις, όσο και για το ανταγωνιστικό καθεστώς που υπάρχει ανάμεσα τους [34].

Πίνακας 5. 1 Πίνακας πληρωμών [34]

Τύπος λύσης	g_1 g_2 ... g_i ... g_n	**Αντιστοιχούσα λύση**
$[\max] g_1(x)$	g_{1*} g_{12} ... g_{1i} ... g_{in}	x_1^1 x_2^1 ... x_l^1
$[\max] g_2(x)$	g_{21} g_{2*} ... g_{2i} ... g_{2n}	x_1^2 x_2^2 ... x_l^2
...	...	...
$[\max] g_i(x)$	g_{i1} g_{i2} ... g_{i*} ... g_{in}	x_1^i x_2^i ... x_l^i
...	...	...
$[\max] g_n(x)$	g_{n1} g_{n2} ... g_{ni} ... g_{n*}	x_1^n x_2^n ... x_l^n

Μετά τη μεγιστοποίηση της αντικειμενικής συνάρτησης $g_i(x)$, ονομάζουμε x^i την επιτευχθείσα λύση και έχουμε:

$$g_i^* = \max_{x \in A} g_i(x) \quad (5.6)$$

$$g_{ij} = g_j(x^i), j \neq i \quad (5.7)$$

Δύο ακόμα βασικές έννοιες του πολυκριτήριου γραμμικού προγραμματισμού είναι οι εξής:

- **Κυριαρχία**: μια δυνατή λύση x λέγεται ότι κυριαρχεί μιας άλλης y (x Δ y) αν και μόνο αν ισχύει ότι :

  $x \Delta y \Leftrightarrow g_i(x) \geq g_i(y)\ \forall\ i$ και για έναν τουλάχιστον δείκτη i^* :

  $g_{i^*}(x) > g_{i^*}(y)$

- **Αποτελεσματικότητα**: μια δυνατή λύση x $\mathcal{E}$ A λέγεται αποτελεσματική για την οικογένεια κριτηρίων $(g_1, g_2, \ldots, g_n)$ αν και μόνο αν δεν υπάρχει δυνατή λύση y $\mathcal{E}$ A η οποία κυριαρχεί της x.

Για να είναι μια δυνατή λύση x $\mathcal{E}$ A αποτελεσματική, αρκεί να υπάρχουν πραγματικοί θετικοί τελεστές $\lambda_1, \lambda_2, \ldots, n$ ώστε η x να μεγιστοποιεί τη σύνθετη αντικειμενική συνάρτηση $\sum_{i=1}^{n} \lambda_i g_i(x)$ πάνω στο σύνολο A.

Η πολυκριτήρια ανάλυση που βασίζεται στον **συναινετικό προγραμματισμό**, είναι μια μεθοδολογία λήψης αποφάσεων, όπου για την επίλυση ενός προβλήματος στηρίζεται στην απόσταση των δυνατών λύσεων από μία ιδεώδη λύση, με σκοπό να βρεθεί η συναινετική λύση [34].

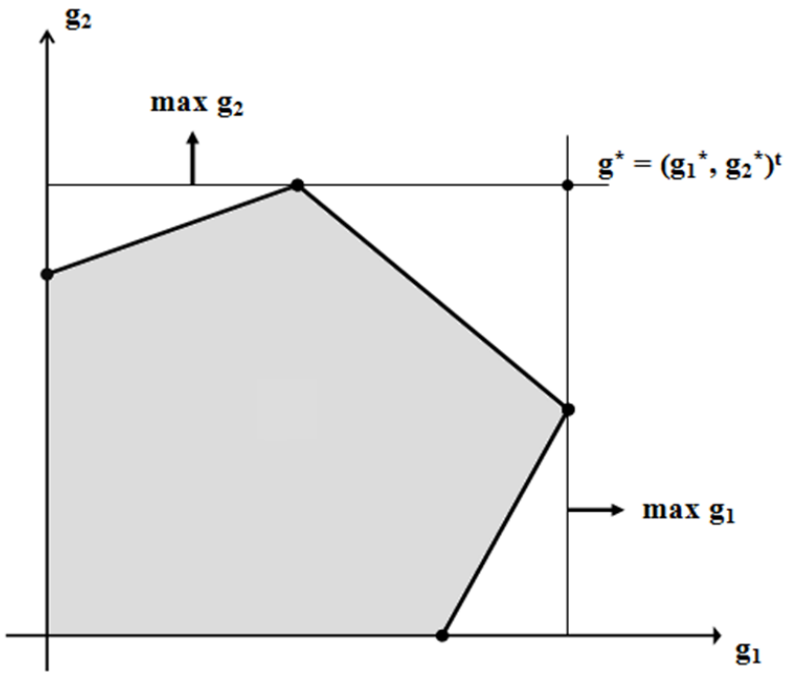
Ιδεώδης λύση ονομάζεται το διάνυσμα των τιμών των μεταβλητών απόφασης που μεγιστοποιεί όλα τα κριτήρια ταυτόχρονα, έχει δηλαδή συντεταγμένες στο χώρο των κριτηρίων:

$$g^* = (g_1^*, g_2^*, \ldots, g_n^*)^t \tag{5.8}$$

Φυσικά δεν πρόκειται για δυνατή λύση, αφού το σημείο g^* βρίσκεται έξω από το επιτρεπτό σύνολο τιμών των g_i.

Στο σχήμα που ακολουθεί παρουσιάζεται ο χώρος των κριτηρίων και η ιδεώδης λύση. Ο γραμμοσκιασμένος χώρος του σχήματος είναι η απεικόνιση του συνόλου A των δυνατών λύσεων.

Συναινετική λύση (compromise solution) αποκαλούμε μια δυνατή λύση όταν βρίσκεται σε ελάχιστη απόσταση από το ιδεώδες σημείο g^*.



Εικόνα 5. 1 Χώρος κριτηρίων και ιδεώδης λύση [34]

Ο ορισμός φυσικά προϋποθέτει την ύπαρξη κάποιας απόστασης μεταξύ των σημείων του χώρου A και της ιδεώδους λύσης. Η απόσταση που χρησιμοποιείται συνήθως είναι η εξής.

$$F_P(x) = \left[\sum_{i=1}^{n} p_i \left(\frac{g_i^* - g_i(x)}{g_i^*}\right)^P\right]^{\frac{1}{P}} \quad (5.9)$$

όπου P είναι φυσικός αριθμός που επιλέγεται από τον αναλυτή του προβλήματος και $p_1, p_2, \dots, p_n$ είναι συντελεστές βαρύτητας των κριτηρίων με άθροισμα την μονάδα

$$\sum_i p_i = 1 \quad (5.10)$$

Η απόσταση $F_P(x)$ αποτελεί υπερκριτήριο βελτιστοποίησης κατά την έννοια:

$$x^* = \min_{x\, \varepsilon\, A} F_P(x) \quad (5.11)$$

Η διαδικασία επίλυσης του παραπάνω μαθηματικού προβλήματος (5.11) ονομάστηκε από τον Zeleny(1982) **συναινετικός προγραμματισμός** (compromise programming). Ωστόσο το πρόβλημα είναι πιο σύνθετο καθώς για τιμές της παραμέτρου $P \neq 1, \infty$ το παραπάνω πρόβλημα (1) είναι πρόβλημα μη γραμμικού προγραμματισμού.

Το πρόβλημα αυτό ανάγεται σε γραμμικού προγραμματισμού για P = 1 και P = ∞. Ειδικότερα στην δεύτερη περίπτωση η απόσταση $F_P(x)$ καταλήγει στην **απόσταση Tchebycheff**:

$$F_\infty(x) = \lim_{P\to\infty} F_P(x) = \max_{i=1,2,\dots,n}\left[p_i\left(\frac{g_i^* - g_i(x)}{g_i^*}\right)\right] \qquad (5.12)$$

Τέλος για να προσδιοριστεί η δυνατή λύση που ελαχιστοποιεί την απόσταση F_∞ , αρκεί να λύσουμε το ακόλουθο πρόβλημα γραμμικού προγραμματισμού που είναι ισοδύναμο του προβλήματος $\min F_\infty(x)$, $x \in A$:

$[\min]z = \lambda$

υ.π.

$\lambda \geq [g_i^* - g_i(x)]\frac{p_i}{g_i^*} \quad \forall\, i = 1,2, \dots, n$

$x \in A\ ,\ \lambda \geq 0$ (5.13)

6ο ΚΕΦΑΛΑΙΟ

Μοντελοποίηση Προβλήματος Επιλογής Μέτρων Ασφαλείας σε Πληροφοριακά Συστήματα Εμπορικών Λιμένων

6 Μοντελοποίηση Προβλήματος Επιλογής Μέτρων Ασφαλείας σε Πληροφοριακά Συστήματα Εμπορικών Λιμένων

Στο παρόν κεφάλαιο μοντελοποιείται το πρόβλημα της επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων, σύμφωνα με τα στάδια μοντελοποίησης της πολυκριτήριας λήψης αποφάσεων που περιγράφηκαν στο προηγούμενο κεφάλαιο.

Αρχικά παρουσιάζεται η κατηγοριοποίηση των μέτρων και η διαδικασία ορισμού του συνόλου των δράσεων. Στη συνέχεια γίνεται αναλυτική περιγραφή της συνεπούς οικογένειας κριτηρίων της επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων.

6.1 Κατηγοριοποίηση μέτρων και διαδικασία ορισμού συνόλου δράσεων μέτρων ασφάλειας πληροφοριακών συστημάτων εμπορικών λιμένων

6.1.1 Κατηγοριοποίηση μέτρων ασφάλειας

Κατά την διαδικασία της εκτίμησης του κινδύνου, όπως περιγράφηκε σε προηγούμενο κεφάλαιο, προσδιορίζονται τα κρίσιμα αγαθά του πληροφοριακού συστήματος ενός οργανισμού (εμπορικού λιμένα στην περίπτωση μας), εντοπίζονται οι απειλές με τις οποίες μπορεί να έρθουν αντιμέτωπα τα αγαθά αυτά, οι αδυναμίες τις οποίες μπορούν να εκμεταλλευτούν αυτές οι απειλές και προσδιορίζονται ακόμα τα αντίστοιχα μέτρα που τις αντιμετωπίζουν.

Τα αγαθά του πληροφοριακού συστήματος ενός εμπορικού λιμένα αποτελούν περιουσιακό στοιχείο για τον οργανισμό και η προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας τους είναι απαραίτητη για να εύρυθμη και αδιάλειπτη λειτουργία του. Η ταξινόμηση τους μπορεί να γίνει σε διάφορες κατηγορίες, ωστόσο μια προτεινόμενη κατηγοριοποίηση είναι η παρακάτω:

- Φυσικά Αγαθά
- Αγαθά Υλικού (Hardware)
- Αγαθά Λογισμικού (Software)
- Εξοπλισμός Δικτύου και
- Αγαθά Δεδομένων (Data)

Για κάθε κατηγορία αγαθών προσδιορίζονται οι απειλές που μπορεί να βλάψουν το πληροφοριακό σύστημα. Οι απειλές μπορούν αρχικά να προσδιοριστούν κατά γενικές

κατηγορίες και είδος και ύστερα μεμονωμένα σε κάθε κατηγορία. Οι απειλές μπορεί να είναι φυσικές (πχ. σεισμός, πλημμύρα), τεχνολογικές (πχ. δυσλειτουργία υλικού εξοπλισμού), περιβαλλοντολογικές (πχ. μόλυνση, ρύπανση), ανθρώπινες (πχ. προσβολή από ιό, εσφαλμένα δικαιώματα πρόσβασης) , τυχαίες ή σκόπιμες (πχ. εμπρησμός, τρομοκρατική ενέργεια) και αλλοίωσης δεδομένων (πχ. κακόβουλη καταστροφή δεδομένων). Ύστερα για κάθε κατηγορία αγαθού αντιστοιχίζονται οι ομάδες πιθανών απειλών.

Επιπλέον, για κάθε κατηγορία αγαθών και για όλες τις απειλές προσδιορίζονται και αντιστοιχούνται οι αδυναμίες ασφάλειας του πληροφοριακού συστήματος που σχετίζονται με την κάθε απειλή. Κάθε απειλή δηλαδή συντελείται από ένα σύνολο αδυναμιών.

Τέλος, προσδιορίζονται τα μέτρα αντιμετώπισης των απειλών που σχετίζονται με τα συγκεκριμένα αγαθά. Οι αδυναμίες είναι εκείνες που υποδεικνύουν τις λύσεις-μέτρα που τις αντιμετωπίζουν. Τα μέτρα προστασίας ουσιαστικά εντοπίζονται με βάση τις αδυναμίες, αφού κάθε μέτρο αποτελεί την θεραπεία της αντίστοιχης αδυναμίας.

Στο ΠΑΡΑΡΤΗΜΑ Α παρουσιάζεται η παραπάνω προτεινόμενη κατηγοριοποίηση με την αντιστοίχιση Απειλών, Αδυναμιών και Μέτρων Προστασίας. Να σημειωθεί εδώ ότι τέτοιοι πίνακες ανανεώνονται και ενημερώνονται συνεχώς ανάλογα με τα καινούρια δεδομένα (εμφάνιση νέων απειλών, αδυναμιών κλπ.).

6.1.2 Διαδικασία ορισμού συνόλου εναλλακτικών δράσεων

Το πρόβλημα που καλούμαστε να αντιμετωπίσουμε είναι η επιλογή των κατάλληλων μέτρων ασφάλειας για την αντιμετώπιση των κινδύνων που εμφανίζονται στα πληροφοριακά συστήματα των εμπορικών λιμένων. Στην παρούσα ενότητα περιγράφεται η διαδικασία με την οποία προκύπτει το τελικό σύνολο των εναλλακτικών δράσεων, δηλαδή η λίστα με τα μέτρα τα οποία πρέπει να αξιολογήσουμε και να συγκρίνουμε.

Για όλα τα κρίσιμα αγαθά του πληροφοριακού συστήματος προσδιορίζονται αρχικά οι παρακάτω τρεις συνιστώσες

- Επίπεδο Επίπτωσης: ο βαθμός της οικονομικής επίπτωσης από την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας του αγαθού
- Επίπεδο Απειλής: η συχνότητα εμφάνισης της απειλής
- Επίπεδο Αδυναμίας: η πιθανότητα για κάθε αδυναμία να συμβεί το χειρότερο σενάριο

Με βάση τους παραπάνω παράγοντες υπολογίζεται το επίπεδο επικινδυνότητας για κάθε απειλή. Έτσι λοιπόν, σε περίπτωση που το επίπεδο αυτό είναι υψηλό για κάποια

απειλή, σημαίνει ότι η απειλή πρέπει να αντιμετωπιστεί και εμείς καλούμαστε να αποφασίσουμε για τα μέτρα προστασίας που θα ληφθούν.

Έστω λοιπόν ότι για κάποιο αγαθό προκύπτει ότι το επίπεδο του κινδύνου είναι υψηλό. Για παράδειγμα, ας υποθέσουμε πως για κάποιο αγαθό δεδομένων η απειλή ‘’κακόβουλη καταστροφή δεδομένων’’ έχει υψηλό βαθμό κινδύνου.

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Κακόβουλη καταστροφή δεδομένων	Δυσαρεστημένοι υπάλληλοι	Ικανοποίηση υπαλλήλων
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκής επικοινωνία της διεύθυνσης με το προσωπικό	Διατήρηση επικοινωνίας μεταξύ διεύθυνσης και προσωπικού
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ανεπαρκείς μηχανισμοί αυθεντικοποίησης	Εγκατάσταση μηχανισμού πιστοποίησης κωδικών και χρηστών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκείς έλεγχοι προσωπικού	Έλεγχος δραστηριότητας προσωπικού

Εικόνα 6. 2 Παράδειγμα αντιστοίχισης Απειλής-Αδυναμίας-Μέτρου

Όπως αναφέραμε στην προηγούμενη ενότητα και φαίνεται και από τον παραπάνω πίνακα, η κάθε απειλή συνίσταται από ένα σύνολο αδυναμιών, ενώ με τη σειρά τους τα μέτρα ασφαλείας προκύπτουν με βάση τις αδυναμίες αυτές καθώς είναι οι λύσεις που τις θεραπεύουν.

Οι δράσεις που αντιμετωπίζουν διαφορετικές αδυναμίες είναι ανεξάρτητες μεταξύ τους αφού κάθε δράση αντιμετωπίζει μία αδυναμία, αναφερόμενοι πάντα στην ίδια απειλή. Άρα είναι αθροιστικές και επομένως μπορούμε να επιλέξουμε παραπάνω από μια δράσεις με στόχο να θεραπεύσουμε παραπάνω από μια αδυναμίες και έτσι να μειώσουμε περεταίρω το επίπεδο αδυναμίας. Αξίζει επιπλέον να αναφέρουμε πως ένα μέτρο που θεραπεύει μια αδυναμία για μια συγκεκριμένη απειλή ενός αγαθού υπάρχει περίπτωση να θεραπεύει την ίδια αδυναμία και για άλλα αγαθά.

Ακόμα, αθροιστικές δράσεις μπορούν να προκύψουν από τον επιμερισμό του πεδίου εφαρμογής ενός μέτρου. Για παράδειγμα, ένα μέτρο που αφορά στην κρυπτογράφηση φορητών συσκευών, επιμερίζεται στην κρυπτογράφηση κινητών τηλεφώνων και φορητών υπολογιστών, δημιουργώντας έτσι δύο αθροιστικές δράσεις. Να σημειωθεί εδώ, ότι αν επιλεχθεί μονάχα μία από τις δύο αθροιστικές αυτές δράσεις δεν αντιμετωπίζεται συνολικά η αδυναμία αλλά ένα ποσοστό της, ανάλογα με την κρισιμότητα του πεδίου.

Επίσης, κάποια από τα μέτρα μπορούν να επιμεριστούν σε επιπλέον εναλλακτικές δράσεις, καθεμία από τις οποίες αντιμετωπίζει εξίσου την αδυναμία. Για παράδειγμα το μέτρο ‘’εγκατάσταση μηχανισμών ταυτοποίησης χρηστών’’ δημιουργεί επιπρόσθετες εναλλακτικές λύσεις καθώς υπάρχουν διαφορετικοί τρόποι-εργαλεία με τους οποίους μπορεί να γίνει η ταυτοποίηση. Έτσι πέρα από τις αθροιστικές δράσεις το τελικό σύνολο των λύσεων περιλαμβάνει και εναλλακτικές δράσεις.

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, το σύνολο των δράσεων που αφορά τα μέτρα ασφαλείας, που θεραπεύουν μια απειλή την οποία αντιμετωπίζει κάποιο αγαθό του πληροφοριακού συστήματος ενός εμπορικού λιμένα, προκύπτει από όλους τους δυνατούς συνδυασμούς των αθροιστικών και επιμέρους εναλλακτικών δράσεων που προσδιορίζονται με τον τρόπο που περιγράφηκε παραπάνω.

6.2 Συνεπής οικογένεια κριτηρίων επιλογής μέτρων προστασίας

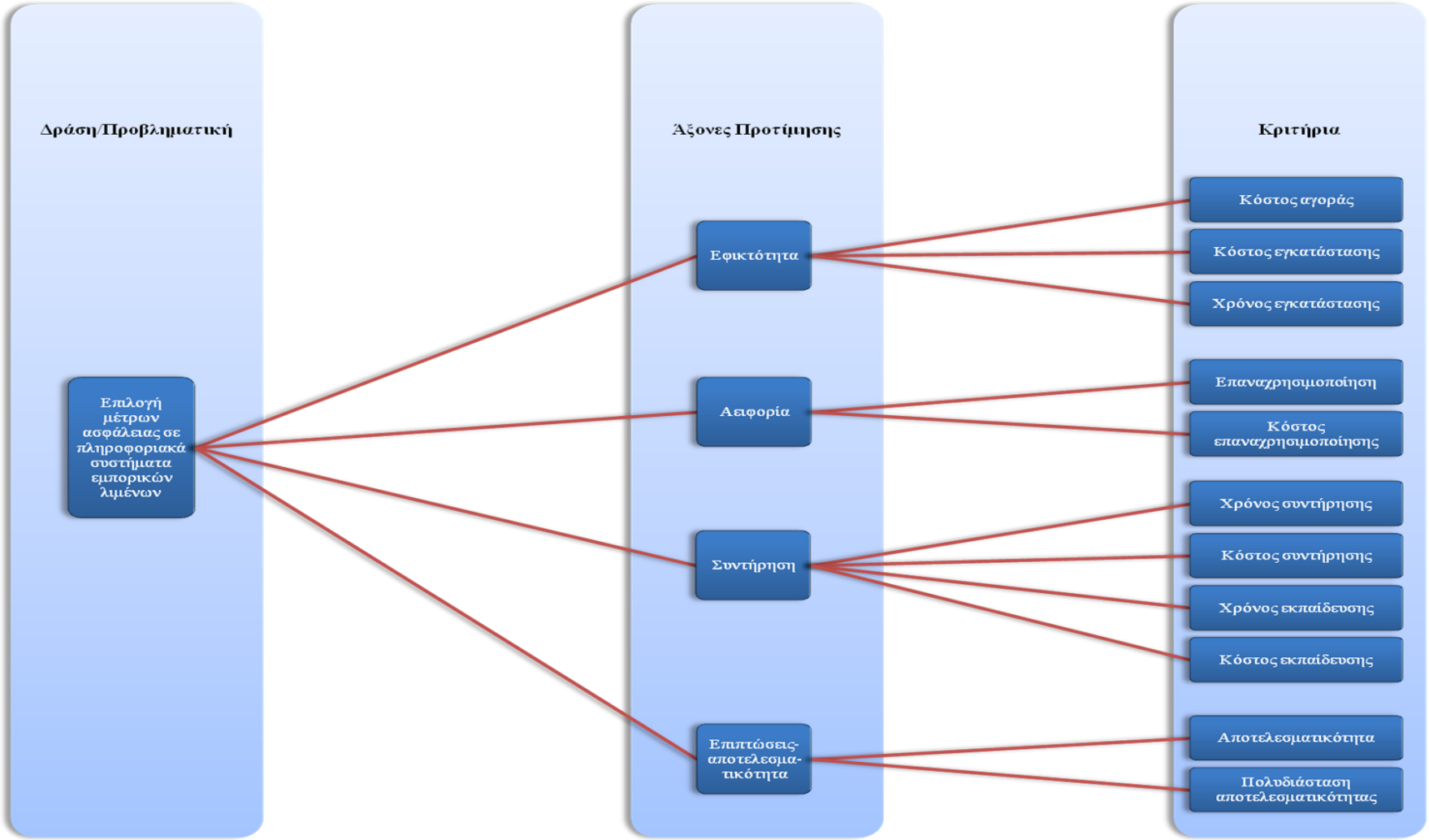
Οι εμπορικοί λιμένες φιλοξενούν κρίσιμα πληροφοριακά συστήματα η ομαλή λειτουργία των οποίων επηρεάζει την ορθή λειτουργία και την επίτευξη των επιχειρησιακών στόχων, τόσο των ίδιων των λιμένων, όσο και των συνεργαζόμενων με αυτούς φορείς. Στόχος του προβλήματος είναι η επιλογή των κατάλληλων μέτρων που θα προστατεύσουν το πληροφοριακό σύστημα ενός εμπορικού λιμένα από ενδεχόμενες απειλές και θα εξασφαλίσουν την ομαλή και αδιάκοπη λειτουργία του.

Η επιλογή των μέτρων ασφάλειας για τα πληροφοριακά συστήματα εμπορικών λιμένων δεν είναι ένα μονοδιάστατο πρόβλημα, αλλά εξαρτάται από αρκετούς παράγοντες και μπορεί να αντιμετωπιστεί ως πολυκριτήριο πρόβλημα. Έτσι λοιπόν η σύγκριση και αξιολόγηση των μέτρων ασφαλείας βασίζεται σε περισσότερα από ένα κριτήρια επιλογής τα οποία περιγράφονται παρακάτω.

Αρχικά η επιλογή των κριτηρίων βασίζεται σε τέσσερις άξονες προτίμησης οι οποίοι με τη σειρά τους οδηγούν στα κριτήρια επιλογής των μέτρων ασφάλειας. Οι τέσσερις αυτοί άξονες, όπως φαίνεται και από το σχήμα που ακολουθεί, είναι οι εξής:

- **Εφικτότητα:** εκφράζει το κατά πόσον είναι δυνατή η εφαρμογή ενός μέτρου ανάλογα με το κόστος υλοποίησης του (αγορά και εγκατάσταση) και το χρόνο που απαιτείται για την εγκατάσταση του.
- **Αειφορία:** εκφράζει το κατά πόσο θα μπορούμε να επωφελούμαστε μελλοντικά από την εφαρμογή ενός μέτρου και αποτελείται από τη δυνατότητα και το κόστος επαναχρησιμοποίησης.
- **Συντήρηση:** εκφράζει τη διατήρηση ενός μέτρου σε καλή κατάσταση μέσα από συνεχείς ελέγχους και αποτελείται από το κόστος και το χρόνο συντήρησης του μέτρου καθώς και από το κόστος και το χρόνο εκπαίδευσης.
- **Επιπτώσεις- Αποτελεσματικότητα:** εκφράζει το βαθμό στον οποίο κάποιο μέτρο αντιμετωπίζει τις απειλές και αποτελείται από την αποτελεσματικότητα και την πολυδιάσταση αποτελεσματικότητας.

Στο παρακάτω σχήμα παρουσιάζεται η συνεπής οικογένεια κριτηρίων επιλογής των μέτρων ασφάλειας, η οποία αποτελείται από τέσσερις άξονες προτίμησης και έντεκα κριτήρια.



Εικόνα 6. 3 Συνεπής οικογένεια κριτηρίων επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων

Τα κριτήρια επιλογής των μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων είναι τα εξής:

- **Κόστος Αγοράς:** πρόκειται για το χρηματικό ποσό που πρέπει να καταβάλει ο οργανισμός για την απόκτηση του μέτρου ασφάλειας. Το κόστος αγοράς μπορεί να ποικίλει ακόμα και όταν μιλάμε για το ίδιο μέτρο-προϊόν, καθώς όταν πρόκειται για προϊόντα της αγοράς η τιμή τους εξαρτάται από την προσφορά του κατασκευαστή. Επιπλέον όταν το μέτρο είναι κάποια διαδικασία που γίνεται στο εσωτερικό του οργανισμού το κόστος αγοράς είναι μηδενικό.

- **Κόστος Εγκατάστασης:** πρόκειται για το χρηματικό ποσό που πρέπει να καταβάλει ο οργανισμός για την εγκατάσταση του μέτρου, ώστε να μπορεί να τεθεί σε εφαρμογή. Αφορά κυρίως τεχνικά μέτρα(πχ. εγκατάσταση εξοπλισμού, λογισμικού κλπ.), όπου απαιτείται η απασχόληση εξειδικευμένου προσωπικού εκτός του οργανισμού. Ωστόσο, μπορεί το κόστος να είναι μηδενικό σε περίπτωση που ο οργανισμός διαθέτει ήδη καταρτισμένο προσωπικό που μπορεί να πραγματοποιήσει την εγκατάσταση. Επιπλέον, όταν αναφερόμαστε σε προϊόντα της αγοράς συμβαίνει συχνά το κόστος εγκατάστασης να συμπεριλαμβάνεται στην τιμή αγοράς του προϊόντος

- **Χρόνος Εγκατάστασης:** πρόκειται για το χρονικό διάστημα που απαιτείται για την εγκατάσταση του μέτρου, ώστε να μπορεί πλέον να τεθεί σε εφαρμογή. Αφορά τόσο τεχνικά μέτρα όσο και διαδικασίες, αφού και τα δύο μπορεί να χρειάζονται κάποιο χρόνο εγκατάστασης και ρύθμισης εωσότου να τεθούν σε λειτουργία. Ο χρόνος εγκατάστασης ποικίλει ανάλογα με την δυσκολία της εγκατάστασης και την πολυπλοκότητα των ρυθμίσεων λειτουργίας(set up).

- **Επαναχρησιμοποίηση:** πρόκειται για τη δυνατότητα χρησιμοποίησης ενός μέτρου περισσότερες από μία φορές. Υπάρχουν μέτρα που είτε μπορούν να εφαρμοστούν μονάχα μια φορά, οπότε απαιτείται η εκ νέου απόκτηση-εφαρμογή τους μελλοντικά για αντιμετώπιση της ίδιας απειλής, είτε μπορούν να εφαρμοστούν για περισσότερες φορές. Η δεύτερη επιλογή συμπεριλαμβάνει και τα μέτρα που είναι μόνιμα, δηλαδή εκείνα που εγκαθίστανται μια φορά και μπορεί να γίνει χρήση τους ανά πάσα στιγμή (πχ. εγκατάσταση συστήματος παρακολούθησης εργασιών).

- **Κόστος Επαναχρησιμοποίησης:** προφανώς αφορά μέτρα για τα οποία υπάρχει η δυνατότητα να εφαρμοστούν περισσότερες από μια φορές μετά την απόκτηση τους. Πρόκειται για το χρηματικό ποσό που καταβάλλεται από τον οργανισμό για την κάθε φορά που ένα μέτρο εφαρμόζεται, εκτός φυσικά της πρώτης φοράς που αποκτάται και τίθεται σε λειτουργία.

- **Χρόνος Συντήρησης:** πρόκειται για το χρόνο που απαιτείται τη διατήρηση ενός μέτρου σε καλή κατάσταση μέσα από συνεχείς ελέγχους. Μπορεί να αφορά τόσο μέτρα-διαδικασίες, όπως για παράδειγμα η ανανέωση(συντήρηση) των πληροφοριών-δεδομένων σε ένα μέτρο που αφορά την παραμετροποίηση των ρυθμίσεων στο δίκτυο(διαδικασία), όσο και τεχνικά μέτρα, όπως για παράδειγμα η συντήρηση ενός εξοπλιστικού συστήματος στο δίκτυο του πληροφοριακού συστήματος.

- **Κόστος Συντήρησης:** πρόκειται για το χρηματικό ποσό που πρέπει να καταβάλει ο οργανισμός για τη διατήρηση της κατοχής ενός μέτρου, αλλά και τη συντήρηση του σε καλή κατάσταση μέσα από συνεχείς ελέγχους. Για παράδειγμα, πέρα από την αγορά ενός προγράμματος προστασίας(firewall), είναι αναγκαία και η συχνή ανανέωση της άδειας χρήσης του.

- **Χρόνος Εκπαίδευσης:** πρόκειται για το χρονικό διάστημα που απαιτείται για την μετάδοση της αναγκαίας τεχνογνωσίας και την κατάρτιση του προσωπικού που εμπλέκεται στο πληροφοριακό σύστημα του οργανισμού, ώστε να αποκτήσει την απαραίτητη γνώση για την εφαρμογή και λειτουργία των μέτρων ασφάλειας.

- **Κόστος Εκπαίδευσης:** πρόκειται για το χρηματικό ποσό που πρέπει να καταβάλει ο οργανισμός για την κατάρτιση και εκπαίδευση των ατόμων που εμπλέκονται στο πληροφοριακό σύστημα του οργανισμού, ώστε να αποκτήσουν την αναγκαία τεχνογνωσία για την εφαρμογή και λειτουργία των μέτρων ασφάλειας που πρόκειται να υλοποιηθούν.

- **Αποτελεσματικότητα:** όπως αναφέρθηκε σε προηγούμενη ενότητα κάθε απειλή συντελείται από ένα σύνολο αδυναμιών, οι οποίες υποδεικνύουν και τα αντίστοιχα μέτρα που τις αντιμετωπίζουν. Κάθε αδυναμία έχει ένα βάρος, το οποίο είναι σταθερό και εκφράζει τη σημαντικότητα της και το ποσοστό συνεισφοράς της στην απειλή. Επομένως, συμπεραίνουμε ότι τα μέτρα που αντιμετωπίζουν αδυναμίες με μεγαλύτερο βάρος, μειώνουν κατά μεγαλύτερο ποσοστό τη συνολική αδυναμία και συνεπώς είναι πιο αποτελεσματικά. Άρα, η αποτελεσματικότητα εκφράζει το κατά πόσο ένα μέτρο μειώνει τη συνολική αδυναμία της απειλής και κατά συνέπεια το επίπεδο του κινδύνου.

- **Πολυδιάσταση αποτελεσματικότητας:** σύμφωνα με όσα αναφέρθηκαν σε προηγούμενη ενότητα, κάθε μέτρο ασφάλειας θεραπεύει την αντίστοιχη αδυναμία που εμφανίζει κάποιο αγαθό, το οποίο αντιμετωπίζει μια απειλή. Ωστόσο η υλοποίηση του μέτρου μπορεί να χρησιμεύσει και για τη θεραπεία της ίδιας απειλής που εμφανίζει κάποιο άλλο αγαθό του πληροφοριακού συστήματος του εμπορικού λιμένα. Το κριτήριο αυτό λοιπόν, εκφράζει την δυνατότητα κάποιου μέτρου να αντιμετωπίζει την ίδια αδυναμία για περισσότερα από ένα αγαθά.

7ο ΚΕΦΑΛΑΙΟ

Μελέτη Περίπτωσης Επιλογής Μέτρων Ασφάλειας Πληροφοριακού Συστήματος Εμπορικού Λιμένα

7 Μελέτη Περίπτωσης Επιλογής Μέτρων Ασφάλειας Πληροφοριακού Συστήματος Εμπορικού Λιμένα

Στόχος του κεφαλαίου αυτού είναι η μελέτη μιας περίπτωσης επιλογής μέτρων ασφάλειας σε πληροφοριακό σύστημα εμπορικού λιμένα για την καλύτερη κατανόηση της μορφής ενός τέτοιου προβλήματος και την εφαρμογή της πολυκριτήριας προσέγγισης βασισμένης στον συναινετικό προγραμματισμό, που περιγράφηκε στο προηγούμενο κεφάλαιο.

Στην αρχή του παρόντος κεφαλαίου γίνεται μια περιγραφή τους προβλήματος και της διαδικασίας σύμφωνα με την οποία ένα αγαθό προκύπτει υψηλού κινδύνου και χρήζει προστασίας. Η διαδικασία και τα αποτελέσματα της αξιολόγησης έχουν εξαχθεί από το εργαλείο STORM [29] [28].

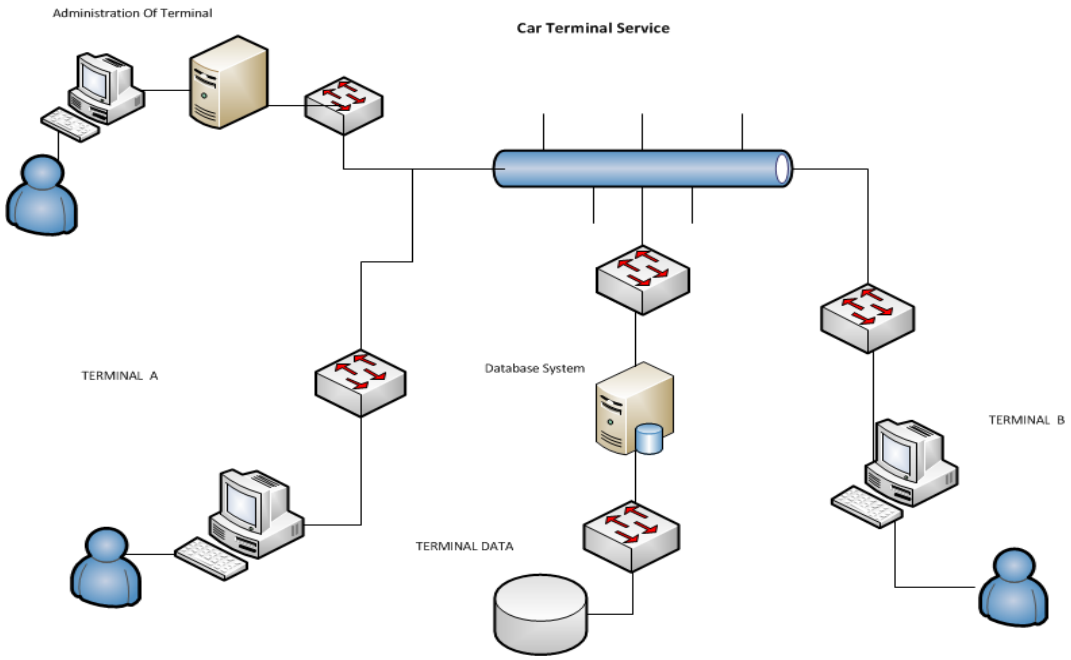
Τέλος, με βάση τη μεθοδολογία του συναινετικού προγραμματισμού, γίνεται επίλυση του προβλήματος αυτού και παρουσίαση των τελικών αποτελεσμάτων, ώστε πλέον ο αποφασίζων να έχει πλήρη εικόνα του προβλήματος και να είναι σε θέση να αποφασίσει για τα μέτρα που θα υλοποιηθούν.

7.1 Παρουσίαση προβλήματος

Για την εξυπηρέτηση της μελέτης εξετάζεται ένα τμήμα του δικτύου του πληροφοριακού συστήματος ενός εμπορικού λιμένα ‘Χ’ (Λ.Χ.). Συγκεκριμένα το τμήμα αυτό του πληροφοριακού συστήματος αποτελείται από το δίκτυο της υπηρεσίας ’Car Terminal’ του εμπορικού λιμένα. Η συγκεκριμένη υπηρεσία αφορά στο σταθμό διακίνησης αυτοκινήτων του εμπορικού λιμένα Χ.

Εικόνα 7. 1 Σταθμός διακίνησης αυτοκινήτων εμπορικού λιμένα

Το δίκτυο του πληροφοριακού συστήματος της υπηρεσίας Car Terminal φαίνεται στην εικόνα που ακολουθεί και αποτελείται από εξής τμήματα: Σύστημα διαχείρισης βάσης, Σύστημα διαχείρισης σταθμών, Σταθμός αποβίβασης Α και Σταθμός αποβίβασης Β.



Εικόνα 7. 2 Δίκτυο πληροφοριακού συστήματος υπηρεσίας Car Terminal

Στη συνέχεια της ενότητας αυτής περιγράφεται η διαδικασία με την οποία προκύπτουν τα αποτελέσματα της αξιολόγησης της επικινδυνότητας των αγαθών του δικτύου της εικόνας 7.2, ώστε να εξαχθούν εκείνα που είναι υψηλού κινδύνου και χρήζουν προστασίας.

Στο σημείο αυτό να σημειωθεί ότι η εκτίμηση και αξιολόγηση των παραγόντων που ακολουθούν(επίπτωσης, απειλής, αδυναμίας και κινδύνου) πραγματοποιείται για όλες τις κατηγορίες αγαθών του παραπάνω δικτύου (φυσικά αγαθά, υλικό, λογισμικό, δεδομένα), αλλά στο συγκεκριμένο παράδειγμα θα παρουσιαστούν μόνο τα αποτελέσματα για τα αγαθά δεδομένων. Το αγαθό δεδομένων που εμπλέκεται στο παραπάνω δίκτυο είναι οι ‘πληροφορίες αυτοκινήτων’.

Αξιολόγηση επίπτωσης

Η πρώτη αξιολόγηση αφορά στην οικονομική επίπτωση που θα έχει στον εμπορικό λιμένα η απώλεια της διαθεσιμότητας , της εμπιστευτικότητας και της ακεραιότητας του αγαθού ‘πληροφορίες αυτοκινήτων’. Στους επόμενους πίνακες παρατίθενται η κλίμακα επιπέδων επίπτωσης και τα αποτελέσματα της αξιολόγησης της επίπτωσης για το αγαθό.

Πίνακας 7. 1 Κλίμακα επιπέδων επίπτωσης

Επίπεδο Επίπτωσης	Βαθμός Επίπτωσης	Περιγραφή
Πολύ Χαμηλό (ΠΧ)	1	Ασήμαντη Επίπτωση - Οικονομική Απώλεια έως 10.000 €
Χαμηλό (Χ)	2	Χαμηλή Επίπτωση - Οικονομική Απώλεια έως 100.000 €
Μέτριο (Μ)	3	Μέτρια Επίπτωση - Οικονομική Απώλεια έως 1.000.000 €
Υψηλό (Υ)	4	Σημαντική Επίπτωση - Οικονομική Απώλεια έως 10.000.000 €
Πολύ Υψηλό (ΠΥ)	5	Καταστροφική Επίπτωση - Οικονομική Απώλεια > 10.000.000 €

Πίνακας 7. 2 Αξιολόγηση επίπτωσης του αγαθού 'Πληροφορίες Αυτοκινήτων'

	Μέγιστος Βαθμός		Διαθεσιμότητα		Εμπιστευτικότητα		Ακεραιότητα		
Αγαθό	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Υπηρεσία
Πληροφορίες αυτοκινήτων	5	ΠΥ	5	ΠΥ	5	ΠΥ	5	ΠΥ	Car Terminal

Αξιολόγηση απειλής

Το επόμενο στάδιο αξιολόγησης αφορά στην συχνότητα εμφάνισης της απειλής. Στους ακόλουθους πίνακες παρουσιάζονται το επίπεδο και ο βαθμός απειλής, καθώς και τα αποτελέσματα αξιολόγησης της απειλής για το υπό εξέταση αγαθό του εμπορικού λιμένα Χ.

Πίνακας 7. 3 Κλίμακα επιπέδων απειλής

Επίπεδο Απειλής	Βαθμός Απειλής	Περιγραφή
Πολύ Χαμηλό (ΠΧ)	0.01	Το πολύ μία φορά τα 10 χρόνια
Χαμηλό (Χ)	0.034	Μία φορά κάθε 3 χρόνια
Μέτριο (Μ)	0.1	Μία φορά τον χρόνο
Υψηλό (Υ)	0.33	Μία φορά κάθε 4 μήνες
Πολύ Υψηλό (ΠΥ)	1	Μία φορά τον μήνα

Η αξιολόγηση απειλής για το αγαθό του εμπορικού λιμένα Χ, όπως φαίνεται από τον πίνακα 7.4, πραγματοποιείται για όλες τις δυνατές απειλές που αντιμετωπίζει το αγαθό δεδομένων 'πληροφορίες αυτοκινήτων'.

Πίνακας 7. 4 Αξιολόγηση απειλής του αγαθού 'Πληροφορίες Αυτοκινήτων'

Αγαθό	Απειλή	Βαθμός απειλής	Επίπεδο απειλής	Λιμάνι
Πληροφορίες αυτοκινήτων	Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	0.1	M	Λ.Χ.
Πληροφορίες αυτοκινήτων	Κοινωνική Μηχανική	0.034	X	Λ.Χ.
Πληροφορίες αυτοκινήτων	Μη νομική συμμόρφωση	0.034	X	Λ.Χ.

Αξιολόγηση Αδυναμίας

Τη τρίτη φάση της αξιολόγησης αποτελεί η αξιολόγηση της αδυναμίας. Σύμφωνα με τον πίνακα που ακολουθεί η κατηγοριοποίηση των επιπέδων αδυναμίας γίνεται σύμφωνα με την πιθανότητα να συμβεί το χειρότερο σενάριο.

Πίνακας 7. 5 Κλίμακα επιπέδων αδυναμίας

Επίπεδο αδυναμίας	Βαθμός αδυναμίας	Σκορ αδυναμίας	Περιγραφή
Χαμηλό (X)	0.33	33	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι < 33%
Μέτριο (M)	0.66	66	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι μεταξύ 33% - 66%
Υψηλό (Y)	1	100	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι > 66%

Τα αποτελέσματα του εργαλείου STORM για την αξιολόγηση της αδυναμίας του αγαθού δεδομένων είναι τα παρακάτω

Πίνακας 7. 6 Αξιολόγηση αδυναμίας του αγαθού 'Πληροφορίες Αυτοκινήτων'

Αγαθό	Απειλή	Τελικό Σκορ Αδυναμίας	Τελικό επίπεδο αδυναμίας	Λιμάνι
Πληροφορίες αυτοκινήτων	Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	86,4	Y	Λ.Χ.
Πληροφορίες αυτοκινήτων	Κοινωνική Μηχανική	88,1	Y	Λ.Χ.
Πληροφορίες αυτοκινήτων	Μη νομική συμμόρφωση	66,375	Y	Λ.Χ.

Στον πίνακα 7.7 παρουσιάζεται αναλυτικά ο τρόπος εξήχθησαν τα αποτελέσματα αξιολόγησης της αδυναμίας μονάχα για την απειλή 'μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές', καθώς στην συνέχεια του παραδείγματος θα μελετήσουμε και θα εφαρμόσουμε το επιλεγμένο μοντέλο απόφασης μόνο για την συγκεκριμένη απειλή.

Πίνακας 7. 7 Αναλυτική αξιολόγηση αδυναμίας της απειλής 'Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές' του αγαθού 'Πληροφορίες Αυτοκινήτων'

Απειλές	Αδυναμίες	Βάρος	Ερωτηματολόγιο	Μέτρο Ασφάλειας	ΑΠΑΝΤΗΣΕΙΣ	
Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	Οι χρήστες έχουν δικαιώματα χρήσης εξωτερικών μέσων αποθήκευσης π.χ. cd - usb κτλ.	10	Έχει ληφθεί μέριμνα ώστε οι απλοί χρήστες να μην μπορούν να χρησιμοποιούν εξωτερικά μέσα αποθήκευσης στον υπολογιστή τους, π.χ. usb;	Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση εξωτερικού μέσου αποθήκευσης (π.χ. κάρτα μνήμης - usb κτλ).	0,66	6,60
	Ελλιπής κρυπτογράφηση φορητών συσκευών	17,5	Τα ευαίσθητα δεδομένα που βρίσκονται σε φορητές συσκευές είναι κρυπτογραφημένα;	Τα κρίσιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	1	17,50
	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLP)	17,5	Υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs);	Θα πρέπει να υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων	1	17,50
	Έλλειψη διαβάθμισης (classification) των πόρων	30	Υπάρχει μεθοδολογία διαβάθμισης των πόρων του οργανισμού;	Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού	0,66	19,80
	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	25	Γίνεται κρυπτογράφηση των ευαίσθητων δεδομένων με αναγνωρισμένες μεθόδους κρυπτογράφησης; (π.χ. AES)	Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	1	25,00
				Τελικό Σκορ Αδυναμίας		**86,40**
				Τελικός βαθμός Αδυναμίας		**1,00**

Το τελικό σκορ αδυναμίας για κάθε απειλή προκύπτει ως άθροισμα των σκορ των αδυναμιών που συνιστούν την συγκεκριμένη απειλή (ΠΑΡΑΡΤΗΜΑ Α αντιστοίχηση αγαθών-απειλών-αδυναμιών-μέτρων). Το σκορ για κάθε αδυναμία προκύπτει από το γινόμενο του βάρους της αδυναμίας επί το βαθμό αδυναμίας, όπως τον έχει δώσει ο χρήστης. Κάθε αδυναμία ανάλογα με την κρισιμότητα της έχει ένα συγκεκριμένο βάρος το οποίο είναι σταθερό. Στον προηγούμενο πίνακα βλέπουμε πώς προκύπτουν αναλυτικά τα παραπάνω αποτελέσματα. Στον κλάδο 'ΑΠΑΝΤΗΣΕΙΣ' η πρώτη στήλη περιλαμβάνει τις απαντήσεις του χρήστη για τον βαθμό αδυναμίας, ενώ η δεύτερη στήλη το γινόμενο του βαθμού αδυναμίας επί το βάρος της αδυναμίας. Η συγκεκριμένη αντιστοίχιση απειλών-αδυναμιών-μέτρων έχει εξαχθεί από τους αντίστοιχους πίνακες του εργαλείου STORM [29].

Αξιολόγηση Κινδύνου

Η τελευταία αξιολόγηση που πραγματοποιείται είναι αυτή του κινδύνου, η οποία είναι βασισμένη στα αποτελέσματα που εξήχθησαν από τις προηγούμενες ενότητες. Η κατηγοριοποίηση των διαφόρων επιπέδων επικινδυνότητας γίνεται σύμφωνα με τους παρακάτω πίνακες.

Πίνακας 7. 8 Κλίμακα επιπέδων επικινδυνότητας

Επίπεδο Επικινδυνότητας	Βαθμός Επικινδυνότητας	Περιγραφή
Πολύ Χαμηλή (ΠΧ)	**1**	**R < 1.000**
Χαμηλή (Χ)	**2**	**1.000 ≤ R < 10.000**
Μέτρια (Μ)	**3**	**10.000 ≤ R < 150.000**
Υψηλή (Υ)	**4**	**150.000 ≤ R < 5.000.000**
Πολύ Υψηλή (ΠΥ)	**5**	**αν R ≥ 5.000.000**

Πίνακας 7. 9 Κίνδυνος R

	ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ	ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Μ	Μ	Μ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ
		0,01	0,01	0,01	0,034	0,034	0,034	0,1	0,1	0,1	0,33	0,33	0,33	1	1	1
	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ
		0,33	0,66	1	0,33	0,66	1	0,33	0,66	1	0,33	0,66	1	0,33	0,66	1
ΕΠΙΠΤΩΣΗ	ΠΧ	10.000	33	66	100	112	224	340	330	660	1.000	1.089	2.178	3.300	3.300	6.600	10.000
	Χ	100.000	330	660	1.000	1.122	2.244	3.400	3.300	6.600	10.000	10.890	21.780	33.000	33.000	66.000	100.000
	Μ	1.000.000	3.300	6.600	10.000	11.220	22.440	34.000	33.000	66.000	100.000	108.900	217.800	330.000	330.000	660.000	1.000.000
	Υ	10.000.000	33.000	66.000	100.000	112.200	224.400	340.000	330.000	660.000	1.000.000	1.089.000	2.178.000	3.300.000	3.300.000	6.600.000	10.000.000
	ΠΥ	²100.000.000	330.000	660.000	1.000.000	1.122.000	2.244.000	3.400.000	3.300.000	6.600.000	10.000.000	10.890.000	21.780.000	33.000.000	33.000.000	66.000.000	100.000.000

Πίνακας 7. 10 Αξιολόγηση επικινδυνότητας

ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ		ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Μ	Μ	Μ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ
ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ		Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ
ΕΠΙΠΤΩΣΗ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Χ	Χ	Χ	Μ
	Χ	ΠΧ	ΠΧ	Χ	Χ	Χ	Χ	Χ	Χ	Μ	Μ	Μ	Μ	Μ	Μ	Μ
	Μ	Χ	Χ	Μ	Μ	Μ	Μ	Μ	Μ	Μ	Μ	Υ	Υ	Υ	Υ	Υ
	Υ	Μ	Μ	Μ	Μ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	ΠΥ	ΠΥ
	ΠΥ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ

Σύμφωνα λοιπόν με τους παραπάνω πίνακες και την ανάλυση που πραγματοποιήθηκε στις προηγούμενες ενότητες (αξιολόγηση επίπτωσης, απειλής και αδυναμίας), προκύπτουν τα αποτελέσματα της αξιολόγησης της επικινδυνότητας τα οποία παρουσιάζονται στη συνέχεια(πίνακας 7.12). Το σκορ επικινδυνότητας προκύπτει ως γινόμενο της οικονομικής επίπτωσης, του τελικού βαθμού αδυναμίας και του τελικού βαθμού απειλής.

R = οικονομική επίπτωση × τελικός βαθμός αδυναμίας × τελικός βαθμός απειλής

Τα τελικά αποτελέσματα όλων των σταδίων αξιολόγησης για όλες τις δυνατές απειλές του αγαθού δεδομένων ‘πληροφορίες αυτοκινήτων’ παρουσιάζονται συνοπτικά στους πίνακες 7.11 και 7.12.

Πίνακας 7. 11 Συνοπτική παρουσίαση αξιολόγησης επίπτωσης, απειλής και αδυναμίας του αγαθού 'Πληροφορίες Αυτοκινήτων'

	Μέγιστος Βαθμός		Διαθεσιμότητα		Εμπιστευτικότητα		Ακεραιότητα						
Αγαθό	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Απειλή	Υπηρεσία	Επίπεδο Απειλής	Επίπεδο Αδυναμίας	Επίπεδο Επίπτωσης
Πληροφορίες αυτοκινήτων	VH	5	VH	10000000	VH	10000000	VH	10000000	Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	Car Terminal	M	Y	100000000
Πληροφορίες αυτοκινήτων	H	5	H	3400000	H	3400000	H	3400000	Κοινωνική Μηχανική	Car Terminal	X	Y	100000000
Πληροφορίες αυτοκινήτων	H	5	H	3400000	H	3400000	H	3400000	Μη νομική συμμόρφωση	Car Terminal	X	Y	100000000

Πίνακας 7. 12 Αξιολόγηση επικινδυνότητας του αγαθού 'Πληροφορίες Αυτοκινήτων'

ΑΓΑΘΟ	ΑΠΕΙΛΗ	Σκορ Επικινδυνότητας	Επίπεδο κινδύνου	Τελικός Βαθμός Απειλής	Τελικό Επίπεδο Απειλής	Τελικό Σκορ Αδυναμίας	Τελικός Βαθμός Αδυναμίας	Τελικό Επίπεδο Αδυναμίας	Οικονομική Επίπτωση	Βαθμός Επίπτωσης	Επίπεδο Επίπτωσης
Πληροφορίες αυτοκινήτων	Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	10.000.000 €	VERY HIGH	0,10	M	86,40	1	Y	100.000.000 €	5	ΠΥ
Πληροφορίες αυτοκινήτων	Κοινωνική Μηχανική	3.400.000 €	HIGH	0,034	X	88,10	1	Y	100.000.000 €	5	ΠΥ
Πληροφορίες αυτοκινήτων	Μη νομική συμμόρφωση	3.400.000 €	HIGH	0,034	X	66,38	1	Y	100.000.000 €	5	ΠΥ

7.2 Επίλυση προβλήματος με εφαρμογή του προτεινόμενου μοντέλου αποφάσεων

Με βάση τα αποτελέσματα της αξιολόγησης των αγαθών του δικτύου του πληροφοριακού συστήματος της υπηρεσίας Car Terminal του υπό εξέταση εμπορικού λιμένα Χ, το επίπεδο επικινδυνότητας για την απειλή 'Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές' του αγαθού δεδομένων 'Πληροφορίες Αυτοκινήτων' προέκυψε *πολύ υψηλό.* Επομένως, το πολυκριτηριακό πρόβλημα που καλούμαστε να αντιμετωπίσουμε είναι η επιλογή μέτρων προστασίας για την απειλή 'μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές' που αφορά το συγκεκριμένο αγαθό δεδομένων.

Σύμφωνα λοιπόν με την αντιστοίχηση απειλών-αδυναμιών μέτρων του πίνακα 7.7 της προηγούμενης ενότητας, η λίστα των μέτρων την οποία θα πρέπει να εξετάσουμε είναι η εξής:

Πίνακας 7. 13 Μέτρα ασφαλείας προς εξέταση

Απειλή	Αδυναμίες	WEIGHT	Μέτρα Ασφάλειας
Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	Οι χρήστες έχουν δικαιώματα χρήσης εξωτερικών μέσων αποθήκευσης	10	Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση εξωτερικού μέσου αποθήκευσης
	Ελλιπής κρυπτογράφηση φορητών συσκευών	17,5	Τα κρίσιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης
	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων	17,5	Θα πρέπει να υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων
	Έλλειψη διαβάθμισης των πόρων	30	Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού
	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	25	Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης

Ωστόσο, σύμφωνα με όσα αναφέρθηκαν για το ορισμό του συνόλου των δράσεων στην ενότητα 6.1.2, από την παραπάνω λίστα μέτρων μπορεί να προκύψουν επιπρόσθετες εναλλακτικές και αθροιστικές δράσεις. Στην συγκεκριμένη περίπτωση που μελετάμε προκύπτουν οι εξής επιμερισμοί:

- Το μέτρο που αφορά στην κρυπτογράφηση δεδομένων που βρίσκονται σε φορητές συσκευές διασπάται σε κρυπτογράφηση κινητών τηλεφώνων και φορητών ηλεκτρονικών συσκευών. Οι δράσεις αυτές είναι αθροιστικές εφόσον καθεμία αντιμετωπίζει μονάχα κατά ένα ποσοστό την αδυναμία, ενώ και οι δύο μαζί την αντιμετωπίζουν συνολικά
- Ακόμα το μέτρο που αφορά στην κρυπτογράφηση ευαίσθητων δεδομένων με αναγνωρισμένες μεθόδους κρυπτογράφησης αρχικά επιμερίζεται σε δύο αθροιστικές δράσεις(web based application και desktop). Στην συνέχεια η πρώτη δράση επιμερίζεται σε τρείς εναλλακτικές και η δεύτερη σε δύο. Οι εναλλακτικές δράσεις αντιμετωπίζουν εξίσου την αδυναμία και επιλέγεται μονάχα μία από αυτές.

Στον πίνακα που ακολουθεί έχουν καταγραφεί οι τιμές των κριτηρίων επιλογής των μέτρων που αναλύθηκαν στο προηγούμενο κεφάλαιο. Οι τιμές αυτές είναι προσεγγιστικές και εξήχθησαν με βάση τα τρέχοντα δεδομένα της ισχύουσας κατάστασης και της αγοράς. Ωστόσο, τα δεδομένα αυτά μπορούν να αναπροσαρμόζονται χωρίς να δημιουργείται βλάβη στην εφαρμογή της προτεινόμενης μεθοδολογίας που θα περιγραφεί στην συνέχεια.

Να σημειωθεί στο σημείο αυτό ότι για την συμπλήρωση των πινάκων 7.14 και 7.15 έγιναν οι εξής υποθέσεις-θεωρήσεις:

- Ο τομέας του υπό εξέταση δικτύου του πληροφοριακού συστήματος αποτελείται από 30 άτομα συνολικά, εκ των οποίων τα 5 είναι μέλη της διοίκησης και τα υπόλοιπα 25 απλό προσωπικό.
- Ο οργανισμός(εμπορικός λιμένας Χ) διαθέτει υπάλληλο που ασχολείται με τις ρυθμίσεις του δικτύου του πληροφοριακού συστήματος.
- Θεωρήθηκε ότι το πλάνο προστασίας του πληροφοριακού συστήματος του οργανισμού είναι 5ετές, ώστε να υπολογιστούν τα ανάλογα κόστη(πίνακας 7.15).
- Στις περιπτώσεις που οι τιμές των κριτηρίων ήταν διαστήματα χρησιμοποιήθηκε η μέση τιμή(πίνακας 7.15).

Με βάση λοιπόν τα παραπάνω στοιχεία, προκύπτει ο πίνακας 7.14 με τη λίστα όλων των μέτρων ασφάλειας και των τιμών τους για τη συνεπή οικογένεια κριτηρίων, ο οποίος φαίνεται παρακάτω.

Πίνακας 7. 14 Επιμερισμός μέτρων ασφάλειας και καταγραφή των τιμών τους για τη συνεπή οικογένεια κριτηρίων

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ			Κριτήρια										
			Κόστος αγοράς	Κόστος εγκατάστασης	Χρόνος εγκατάστασης	Δυνατότητα επαναχρησιμοποίησης	Κόστος επαναχρησιμοποίησης	Χρόνος συντήρησης	Κόστος συντήρησης	Χρόνος εκπαίδευσης	Κόστος εκπαίδευσης	Αποτελεσματικότητα	Πολυδιάσταση αποτελεσματικότητας
Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση εξωτερικού μέσου αποθήκευσης (π.χ. κάρτα μνήμης - usb κτλ).	Διαδικασία - set up στο δίκτυο, στο active directory		μηδενικό	μηδενικό	1 ημέρα	είναι μόνιμο σε όλους τους χρήστες	μηδενικό	1 ημέρα σε περίπτωση που προστεθούν χρήστες	μηδενικό	μηδενικό, το πιθανότερο είναι να διαθέτει ο οργανισμός υπάλληλο που να γνωρίζει τη διαδικασία	μηδενικό	10	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
Τα κρίσιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	70% κρυπτογράφηση laptop		1500 € / τεμ.	μηδενικό	Μηδενικό, το προϊόν αγοράζεται κρυπτογραφημένο	Η κρυπτογράφηση αφορά μόνο τη συγκεκριμένη αδυναμία. Είναι μόνιμο.	μηδενικό	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη. Δεν αφορά το κριτήριο η ανανέωση εξοπλισμού	μηδενικό	μηδενικό	μηδενικό	17,5 * 70%	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
	30% κρυπτογράφηση κινητών		500 € / τεμ.	μηδενικό	Μηδενικό, το προϊόν αγοράζεται κρυπτογραφημένο	Η κρυπτογράφηση αφορά μόνο τη συγκεκριμένη αδυναμία. Είναι μόνιμο.	μηδενικό	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη. Δεν αφορά το κριτήριο η ανανέωση εξοπλισμού	μηδενικό	μηδενικό	μηδενικό	17,5 * 30%	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
Θα πρέπει να υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων	Προϊόν -> DLP		100.000 €	μηδενικό	set up λειτουργίας 1 μήνας	μόνιμο	μηδενικό, μηχάνημα που τοποθετείται στο δίκτυο και είναι μόνιμο	1-6 μήνες, ανάλογα με την πολιτική και τις ρυθμίσεις	10000-20000 € ανανέωση άδειας	1-6 μήνες η εκπαίδευση εδώ αφορά την εκμάθηση χρήσης του μηχανισμού από τους αρμόδιους	Δεν έχει. Περιλαμβάνεται στο πακέτο της τιμής αγοράς	17,5	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού	Διαδικασία : Πληροφορία κρίσιμη, δημόσια, ιδιωτική		μηδενικό	μηδενικό	1 μήνα μέχρι 1 χρόνο, ανάλογα με τον όγκο των εγγράφων προς κατηγοριοποίηση	μόνιμο για τα ήδη κατηγοριοποιημένα έγγραφα	μηδενικό	1 ημέρα σε περίπτωση που προστεθούν νέα έγγραφα προς ταξινόμηση	μηδενικό	1-6 μήνες εκπαίδευση προσωπικού για την πολιτική και διαδικασίες διαβάθμισης των πόρων	μηδενικό, η διαδικασία πραγματοποιείται από υπάλληλο του οργανισμού προς τους χρήστες	30	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	web based application	https	100-800 € με εγκατάσταση για 1 χρόνο. Για μεγαλύτερη διάρκεια έκπτωση στο κόστος	μηδενικό	1 ημέρα	Η κρυπτογράφηση αφορά μόνο τη συγκεκριμένη αδυναμία. Διαρκεί για όσο λέει το πακέτο	Μηδενικό. Η κρυπτογράφηση είναι μόνιμη	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη μετά την εγκατάσταση.	100-500 € για ανανέωση της άδειας	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν	25 * 30%	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
		κρυπτογράφηση βάσης	2000-10000 € αν το αγοράσεις. Μηδενικό αν το κάνει υπάλληλος του οργανισμού	μηδενικό	1 εβδομάδα-6 μήνες αν το πάρεις έτοιμο. Μέχρι 1 χρόνο αν το κάνεις μόνος	Η κρυπτογράφηση αφορά μόνο τη συγκεκριμένη αδυναμία. Είναι μόνιμο.	Μηδενικό. Η κρυπτογράφηση είναι μόνιμη	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη μετά την εγκατάσταση.	μηδενικό	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν		Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
		πρόσληψη υπαλλήλου για υλοποίηση έργου	800 € μηνιαίος μισθός αλλά θα κάνει και άλλη εργασία	μηδενικό	Μέχρι 1 χρόνο (προγραμματισμός)	Υπάρχει καθώς ο υπάλληλος μπορεί να απασχολείται και με άλλη εργασία	Μηδενικό. Η κρυπτογράφηση είναι μόνιμη	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη μετά την εγκατάσταση.	Μηδενικό εφόσον προσλαμβάνει υπάλληλο	Μηδενικό αφού ο υπάλληλος είναι εξειδικευμένος	Μηδενικό εφόσον προσλαμβάνει υπάλληλο		Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
	desktop	κρυπτογράφηση εφαρμογής	2000-20000 € κόστος αγοράς αν το αγοράσεις απ' έξω. Μηδενικό αν το κάνεις μόνος	μηδενικό	1 εβδομάδα-6 μήνες	Η κρυπτογράφηση αφορά μόνο τη συγκεκριμένη αδυναμία. Είναι μόνιμο.	Μηδενικό. Η κρυπτογράφηση είναι μόνιμη	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη μετά την εγκατάσταση.	2000 € το χρόνο	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν	Μηδενικό. Οι χρήστες λαμβάνουν ένα έτοιμο κρυπτογραφημένο προϊόν	25 * 70%	Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά
		πρόσληψη υπαλλήλου για υλοποίηση έργου	800 € μηνιαίος μισθός αλλά θα κάνει και άλλη εργασία	μηδενικό	Μέχρι 1 χρόνο (προγραμματισμός)	Υπάρχει καθώς ο υπάλληλος μπορεί να απασχολείται και με άλλη εργασία	Μηδενικό. Η κρυπτογράφηση είναι μόνιμη	Δεν έχει. Η κρυπτογράφηση είναι μόνιμη μετά την εγκατάσταση.	Μηδενικό εφόσον προσλαμβάνει υπάλληλο	Μηδενικό αφού ο υπάλληλος είναι εξειδικευμένος	Μηδενικό εφόσον προσλαμβάνει υπάλληλο		Αντιμετωπίζει την ίδια αδυναμαία για περισσότερα από ένα αγαθά

Η μέθοδος που έχει επιλεγεί για την επίλυση του προβλήματος είναι μία πολυκριτήρια προσέγγιση βασισμένη στον συναινετικό προγραμματισμό. Για την εφαρμογή της επιλεγμένης μεθοδολογίας δίνεται βαρύτητα στο συνολικό κόστος που απαιτείται για την υλοποίηση του μέτρου και την επίδραση που έχει η εφαρμογή του στο επίπεδο της επικινδυνότητας. Τα κριτήρια δηλαδή που λαμβάνονται υπόψη για την εξαγωγή των αποτελεσμάτων είναι αυτά του κόστους αγοράς, του κόστους εγκατάστασης, του κόστους εκπαίδευσης, του κόστους συντήρησης, του κόστους επαναχρησιμοποίησης και της αποτελεσματικότητας. Στο συγκεκριμένο παράδειγμα τυχαίνει όλα τα κόστη πέραν αυτών της αγοράς και συντήρησης να είναι μηδενικά, οπότε δεν συμμετέχουν στου υπολογισμούς.

Έτσι για όλους τους δυνατούς συνδυασμούς μέτρων υπολογίζεται το συνολικό κόστος και το νέο επίπεδο κινδύνου, ενώ στη συνέχεια τα ζευγάρια όλων των δυνατών συνθέσεων αναπαρίστανται σε ένα γράφημα. Οι δυνατοί συνδυασμοί μέτρων, σύμφωνα με τις αθροιστικές και εναλλακτικές δράσεις που φαίνονται στον προηγούμενο πίνακα, μπορεί να περιλαμβάνουν την υλοποίηση ενός έως και επτά μέτρων ταυτόχρονα.

Η γραφική απεικόνιση των αποτελεσμάτων δίνει την δυνατότητα στον αποφασίζοντα να έχει σαφή εικόνα για τις εναλλακτικές δράσεις του προβλήματος της επιλογής μέτρων ασφάλειας και να εντοπίσει ευκολότερα τις λύσεις που είναι κοντινότερα στη βέλτιστη λύση, ώστε να πάρει την τελική του απόφαση για τα μέτρα που πρέπει να υλοποιηθούν.

Στον πίνακα 7.15 παρατίθενται όλα τα στοιχεία που είναι απαραίτητα για τους υπολογισμούς των δύο παραμέτρων που θα ληφθούν υπόψη για την επίλυση του προβλήματος, δηλαδή του συνολικού κόστους και του νέου επιπέδου κινδύνου.

Να σημειωθεί στο σημείο αυτό, ότι με βάση τα όσα έχουμε αναφέρει για την αντιστοιχία αδυναμιών και μέτρων, εφόσον κάθε αδυναμία έχει ένα σταθερό βάρος, τότε η αποτελεσματικότητα κάθε μέτρου ή αλλιώς το βάρος κάθε μέτρου θα είναι ίδιο με αυτό της αδυναμίας που θεραπεύει. Επίσης το νέο σκορ αδυναμίας προκύπτει αφαιρώντας από το παλαιό σκορ αδυναμίας το βάρος του επιπρόσθετου μέτρου που εφαρμόζεται. Τέλος το σκορ επικινδυνότητας υπολογίζεται από τον τύπο και τις αξιολογήσεις που παρουσιάστηκαν στην προηγούμενη ενότητα:

R = οικονομική επίπτωση × τελικός βαθμός αδυναμίας × τελικός βαθμός απειλής,

όπου η οικονομική επίπτωση για το συγκεκριμένο αγαθό είναι σταθερή και ίση με 100.000.000 ευρώ, ο τελικός βαθμός απειλής σταθερός και ίσος με 0,1, ενώ ο τελικός βαθμός αδυναμίας μεταβάλλεται ανάλογα με τα υλοποιούμενα μέτρα.

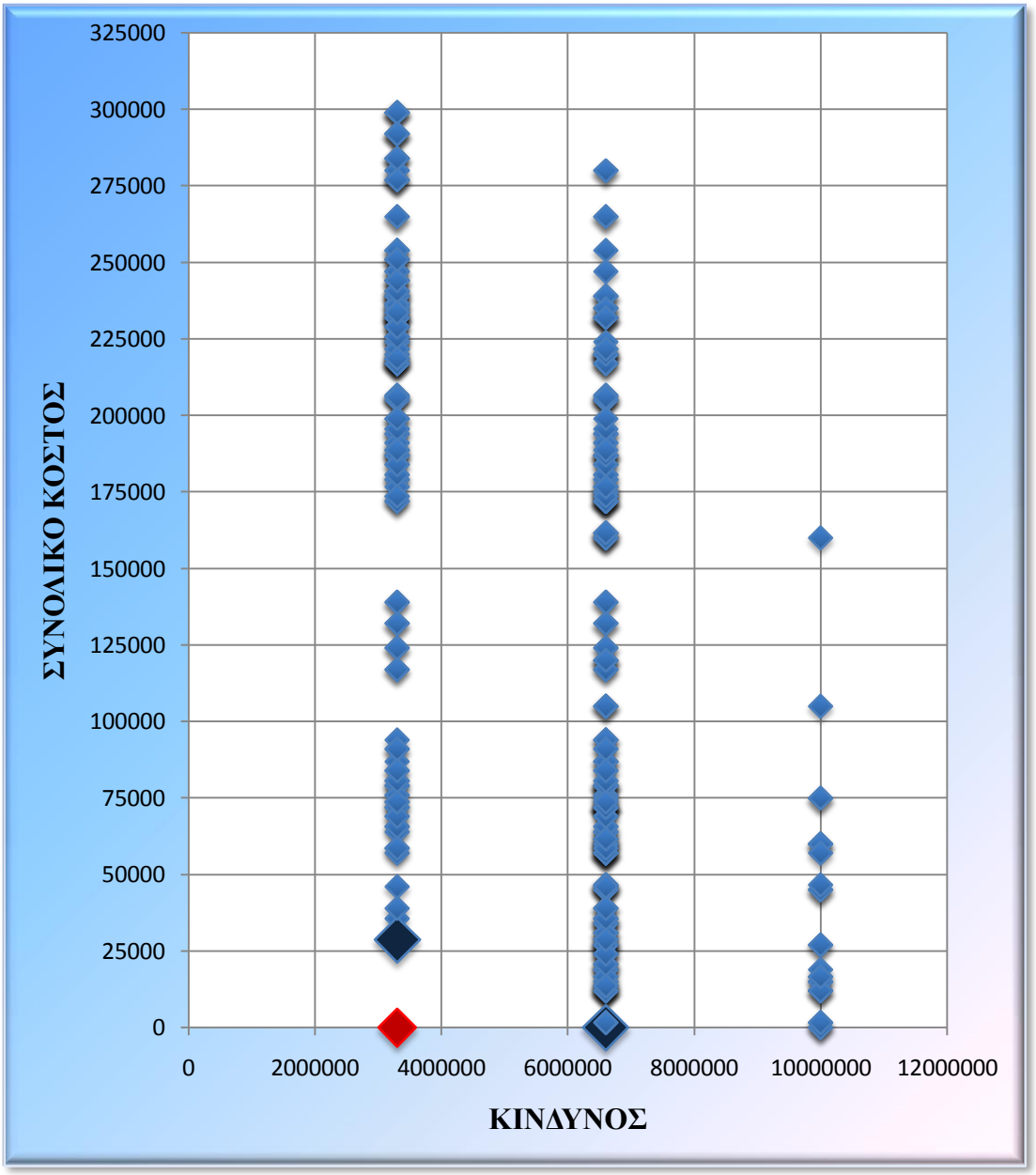
Τα αριθμητικά δεδομένα που χρειάζονται για την εφαρμογή της επιλεγμένης μεθοδολογίας, για όλους τους δυνατούς συνδυασμούς των μέτρων ασφαλείας, που αφορούν στο δίκτυο του πληροφοριακού συστήματος της περίπτωσης που μελετάμε, υπολογίστηκαν και παρατίθενται στο ΠΑΡΑΡΤΗΜΑ Β.

Πίνακας 7. 15 Δεδομένα προς επεξεργασία για εφαρμογή της προτεινόμενης μεθοδολογίας

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ			ΜΕΤΡΟ	ΒΑΡΟΣ ΣΥΝΟΛΙΚΟΥ ΜΕΤΡΟΥ	ΒΑΡΟΣ ΕΠΙΜΕΡΟΥΣ ΜΕΤΡΟΥ	ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΒΑΡΟΣ ΕΠΙΜΕΡΟΥΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ	ΚΡΙΤΗΡΙΑ			
								Κόστος αγοράς	Κόστος συντήρησης	Αποτελε-σματικότητα	Συνολικό κόστος
Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση εξωτερικού μέσου αποθήκευσης (π.χ. κάρτα μνήμης - usb κτλ).	Διαδικασία - set up στο δίκτυο, στο active directory		M1	10	10	0,66	6,6	μηδενικό	μηδενικό	10	0
Τα κρίσιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	70% κρυπτογράφηση laptop		M2	17,5	12,25	1	12,25	1500 € / τεμ.	μηδενικό	12,25	(5+25)άτομα*1500€/άτομο= 45000€
	30% κρυπτογράφηση κινητών		M3		5,25		5,25	500 € / τεμ.	μηδενικό	5,25	(5+25)άτομα*500€/άτομο= 15000 €
Θα πρέπει να υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων	Προϊόν -> DLP		M4	17,5	17,5	1	17,5	100.000 €	10000-20000 € ανανέωση άδειας	17,5	100000€ + (10000+20000)/2 * 4 έτη = 160000€
Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού	Διαδικασία : Πληροφορία κρίσιμη, δημόσια, ιδιωτική		M5	30	30	0,66	19,8	μηδενικό	μηδενικό	30	0
Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	30% web based application	https	M6	25	7,5	1	7,5	100-800 € με εγκατάσταση για 1 χρόνο. Για μεγαλύτερη διάρκεια έκπτωση στο κόστος	100-500 € για ανανέωση της άδειας	7,5	(100+800)/2 για τον πρώτο χρόνο + (100+500)/2*4 για τα επόμενα 4 χρόνια = 1650€
		κρυπτογράφηση βάσης	M7		7,5		7,5	2000-10000 € αν το αγοράσεις. Μηδενικό αν το κάνει υπάλληλος του οργανισμού	μηδενικό		(2000+10000)€ / 2 = 6000€
		πρόσληψη υπαλλήλου για υλοποίηση έργου	M8		7,5		7,5	800 € μηνιαίος μισθός αλλά θα κάνει και άλλη εργασία	Μηδενικό εφόσον προσλαμβάνει υπάλληλο		200€ * 12μήνες * 5έτη = 12000€
	70% desktop	κρυπτογράφηση εφαρμογής	M9		17,5		17,5	2000-20000 € κόστος αγοράς αν το αγοράσεις απ' έξω. Μηδενικό αν το κάνεις μόνος	2000 € το χρόνο	17,5	(2000+20000)€ / 2 + 2000€ * 4 έτη = 19000 €
		πρόσληψη υπαλλήλου για υλοποίηση έργου	M10		17,5		17,5	800 € μηνιαίος μισθός αλλά θα κάνει και άλλη εργασία	Μηδενικό εφόσον προσλαμβάνει υπάλληλο		200€ * 12μήνες * 5έτη = 12000€

Επόμενο βήμα, εφόσον έχουν γίνει οι υπολογισμοί του συνολικού κόστους και του νέου επιπέδου επικινδυνότητας για όλους τους δυνατούς συνδυασμούς μέτρων, τα αποτελέσματα των οποίων παρατίθενται στο ΠΑΡΑΡΤΗΜΑ Β, είναι η γραφική τους απεικόνιση.

Στο γράφημα που ακολουθεί εκτός από τα υπολογισμένα ζευγάρια συνολικού κόστους-επικινδυνότητας απεικονίζεται και η **ιδεώδης λύση**, δηλαδή το σημείο του χώρου που έχει ως συντεταγμένες τη βέλτιστη λύση για κάθε κριτήριο. Στην προκειμένη περίπτωση το βέλτιστο κόστος μπορεί να είναι 0 ευρώ, ενώ το βέλτιστο σκορ επικινδυνότητας μπορεί να είναι R = 3300000.



Γράφημα 7. 1 Απεικόνιση ιδεώδους λύσης και ζευγών συνολικού κόστους-κινδύνου για όλους τους δυνατούς συνδυασμούς μέτρων

Ακολουθώντας την μεθοδολογία του **συναινετικού προγραμματισμού**, η επόμενη κίνηση είναι η αναζήτηση της **συναινετικής λύσης,** δηλαδή της δυνατής λύσης που βρίσκεται σε ελάχιστη απόσταση από το ιδεώδες σημείο το οποίο είναι το (3300000, 0).

Όπως είναι προφανές από το γράφημα τα δύο σημεία που βρίσκονται σε κοντινότερη απόσταση από το ιδεώδες σημείο είναι τα εξής δύο

- Το πρώτο σημείο είναι το (3300000, 28650) το οποίο σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Β αντιστοιχεί στο συνδυασμό μέτρων Μ1, Μ3, Μ5, Μ6 και Μ10.

- Το δεύτερο σημείο είναι το (6600000, 0) το οποίο σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Β αντιστοιχεί στο συνδυασμό μέτρων Μ1 και Μ5.

Η αντιστοίχιση των μέτρων 'Μ' φαίνεται αναλυτικά στον πίνακα 7.15.

Πλέον ο αποφασίζων είναι εκείνος που καλείται να επιλέξει ποιον συνδυασμό μέτρων ασφάλειας θα υλοποιήσει για την προστασία του δικτύου του πληροφοριακού συστήματος που αφορά στην υπηρεσία Car Terminal του εμπορικού λιμένα Χ, από την απειλή που διατρέχει το αγαθό 'πληροφορίες αυτοκινήτων'.

Συγκεκριμένα ο αποφασίζων καλείται να επιλέξει αν θα υλοποιήσει το δεύτερο συνδυασμό μέτρων για τον οποίο το κόστος είναι μηδενικό ενώ το επίπεδο κινδύνου (από 10.000.000 γίνεται 6.600.000) παραμένει πολύ υψηλό (ΠΥ) σύμφωνα με τους πίνακες 7.9 και 7.10, ή τον πρώτο συνδυασμό για τον οποίο ο οργανισμός πρέπει να δαπανήσει 28.650 ευρώ ενώ το επίπεδο κινδύνου (από 10.000.000 γίνεται 3.300.000) μειώνεται από πολύ υψηλό (ΠΥ) σε υψηλό (Υ).

Το ερώτημα δηλαδή που τίθεται στον αποφασίζοντα είναι αν είναι διατεθειμένος να δαπανήσει 28.650 ευρώ (κριτήριο κόστους) για την εφαρμογή του αποτελεσματικότερου συνδυασμού μέτρων (κριτήριο αποτελεσματικότητας) που μειώνει το επίπεδο επικινδυνότητας του υπό εξέταση αγαθού του εμπορικού λιμένα (trade-off).

8ο ΚΕΦΑΛΑΙΟ

Συμπεράσματα και Προοπτικές

8 Συμπεράσματα και Προοπτικές

8.1 Συμπεράσματα

Στην παρούσα ενότητα παρουσιάζονται όλα τα συμπεράσματα που εξήχθησαν κατά την μελέτη της επιλογής μέτρων ασφάλειας για την προστασία των πληροφοριακών συστημάτων εμπορικών λιμένων.

- Οι εμπορικοί λιμένες αποτελούν κρίσιμες υποδομές πληροφορικής καθώς φιλοξενούν κρίσιμα πληροφοριακά συστήματα. Διαχειρίζονται μεγάλο αριθμό ευαίσθητων δεδομένων, κρίσιμων πληροφοριών και υπηρεσιών, ενώ καθημερινά εξυπηρετούν μεγάλο αριθμό χρηστών και αλληλεπιδρούν με άλλους φορείς (π.χ. τράπεζες, τελωνεία, υπουργεία, ναυτιλιακές εταιρείες κλπ.). Όπως λοιπόν γίνεται κατανοητό, η ανάλυση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος ενός εμπορικού λιμένα είναι σημαντική για την ομαλή λειτουργία και την επίτευξη των επιχειρησιακών στόχων, τόσο του ίδιου του οργανισμού, όσο και των συνεργαζόμενων με αυτόν φορέων.

- Στα πλαίσια της προσπάθειας απεικόνισης με όσο το δυνατό πιο ρεαλιστικό τρόπο προβλημάτων λήψης αποφάσεων μεγάλης πολυπλοκότητας της σύγχρονης εποχής, παρατηρείται η εισαγωγή περισσότερων του ενός κριτηρίου στις σχετικές αναλύσεις. Η πολυκριτήρια ανάλυση αποτελεί ένα ευρέως χρησιμοποιούμενο και διαδεδομένο εργαλείο για την υποστήριξη αποφάσεων μέσα από τη συστηματική εξαγωγή τεκμηριωμένων επιλογών. Η ύπαρξη πολλαπλών κριτηρίων καθιστά τον τρόπο συλλογής, επεξεργασίας και αξιοποίησης της πληροφορίας αρκετά πιο σύνθετο και διαφορετικό, σε σχέση με εκείνον των μονοδιάστατων αναλύσεων, ωστόσο προσφέρει μεγαλύτερη ευελιξία και προοπτικές στον αποφασίζοντα διότι εξετάζονται περισσότερες διαστάσεις. Ο τρόπος σύνθεσης όλων των παραγόντων-κριτηρίων για την λήψη ορθολογικών αποφάσεων συνιστά βασικό αντικείμενο της πολυκριτήριας ανάλυσης.

- Η αξιολόγηση των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων εμπορικών λιμένων (εναλλακτικές δράσεις) στηρίχθηκε σε ένα σύστημα βασισμένο στους παρακάτω τέσσερις άξονες προτίμησης:

  α) εφικτότητα,
  β) αειφορία,
  γ) συντήρηση και
  δ) επιπτώσεις-αποτελεσματικότητα.

  Με τη σειρά τους οι άξονες αυτοί οδηγούν στα κριτήρια αξιολόγησης που είναι τα εξής:

- Κόστος Αγοράς
- Κόστος Εγκατάστασης
- Χρόνος Εγκατάστασης
- Επαναχρησιμοποίηση
- Κόστος Επαναχρησιμοποίησης
- Χρόνος Συντήρησης
- Κόστος Συντήρησης
- Χρόνος Εκπαίδευσης
- Κόστος Εκπαίδευσης
- Αποτελεσματικότητα
- Πολυδιάσταση αποτελεσματικότητας

Όλα μαζί τα παραπάνω στοιχεία συνθέτουν την συνεπή οικογένεια κριτηρίων της επιλογής μέτρων ασφάλειας για την προστασία των πληροφοριακών συστημάτων εμπορικών λιμένων.

❖ Για τη σύγκριση και αξιολόγηση των μέτρων ασφάλειας προτείνεται η εφαρμογή μιας πολυκριτήριας προσέγγισης που στηρίζεται στη θεωρία του συναινετικού προγραμματισμού. Για την εφαρμογή της επιλεγμένης μεθοδολογίας δόθηκε βαρύτητα στο συνολικό κόστος που απαιτείται για την υλοποίηση του μέτρου και την επίδραση που έχει η εφαρμογή του στο επίπεδο της επικινδυνότητας. Τα κριτήρια δηλαδή που λήφθηκαν υπόψη για την εξαγωγή των αποτελεσμάτων είναι αυτά του κόστους αγοράς, του κόστους εγκατάστασης, του κόστους εκπαίδευσης, του κόστους συντήρησης, του κόστους επαναχρησιμοποίησης και της αποτελεσματικότητας.

❖ Οι εναλλακτικές δράσεις-μέτρα απεικονίζονται γραφικά, έτσι ώστε οι βέλτιστες λύσεις να είναι κατανοητές και άμεσα εκμεταλλεύσιμες από τους ενδιαφερόμενους – αποφασίζοντες. Έτσι ο αποφασίζον μπορεί να διακρίνει εύκολα ποιες είναι οι εναλλακτικές δράσεις που μπορεί να ακολουθήσει για την επίτευξη του στόχου και να αποφασίσει αν είναι διατεθειμένος να δαπανήσει τα ανάλογα ποσά για την υλοποίηση τους.

8.2 Προοπτικές

Αρχικά, η εξαγωγή των αποτελεσμάτων για το επίπεδο του κινδύνου των αγαθών ενός πληροφοριακού συστήματος βασίστηκε στη συνεργατική μεθοδολογία STORM-RM. Παρόλα αυτά, η εφαρμογή της προτεινόμενης μεθοδολογίας θα μπορούσε να βασιστεί στην ανάλυση επικινδυνότητας και μιας διαφορετικής μεθοδολογίας, που ίσως να εξάγει διαφορετικά συμπεράσματα από την παραπάνω συνεργατική μεθοδολογία.

Επιπλέον η μελέτη όλων των αγαθών ενός πληροφοριακού συστήματος βασίζεται στους πίνακες αντίστοιχης αγαθών-απειλών-αδυναμιών-μέτρων. Ένας τέτοιος ενδεικτικός πίνακας παρατίθεται στο ΠΑΡΑΡΤΗΜΑ Α. Ωστόσο οι πίνακες αυτοί μπορούν και πρέπει να ανανεώνονται με καινούργια δεδομένα, για παράδειγμα μετά την εμφάνιση μιας πρωτόγνωρης αδυναμίας για ένα αγαθό, ώστε να είναι πλήρης η εξέταση του προβλήματος.

Επίσης, για την αντιμετώπιση του προβλήματος της επιλογής μέτρων ασφάλειας σε πληροφοριακά συστήματα εμπορικών λιμένων, η συγκεκριμένη διπλωματική βασίστηκε στη μεθοδολογία του συναινετικού προγραμματισμού. Εντούτοις, θα είχε ενδιαφέρον να δοκιμαστεί και μια προσέγγιση βασισμένη σε ένα διαφορετικό μοντέλο αποφάσεων από εκείνο του συναινετικού προγραμματισμού και να γίνει σύγκριση των τελικών αποτελεσμάτων.

ΠΑΡΑΡΤΗΜΑ Α

Πίνακες αντιστοίχισης Αγαθών - Απειλών - Αδυναμιών - Μέτρων Ασφάλειας πληροφοριακών συστημάτων εμπορικών λιμένων

ΠΑΡΑΡΤΗΜΑ Α: Πίνακες αντιστοίχισης Αγαθών - Απειλών - Αδυναμιών - Μέτρων Ασφάλειας πληροφοριακών συστημάτων εμπορικών λιμένων

Φυσικά Αγαθά

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Πυρκαγιά	Περιοχή ευάλωτη σε φυσικές καταστροφές	Αλλαγή περιοχής εγκατάστασης
	Ύπαρξη εύφλεκτων υλικών σε μη προστατευμένους χώρους	Απόσυρση εύφλεκτων υλικών από μη προστατευμένους χώρους
	Έλλειψη μηχανισμών ανίχνευσης πυρκαγιάς	Εγκατάσταση μηχανισμών ανίχνευσης φωτιάς
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
	Έλλειψη συστήματος πυρασφάλειας	Εγκατάσταση/συντήρηση συστήματος πυρασφάλειας
Σεισμός	Περιοχή ευάλωτη σε φυσικές καταστροφές	Αλλαγή περιοχής εγκατάστασης
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
	Εγκαταστάσεις ευάλωτες σε σεισμικές δονήσεις	Βελτίωση αντισεισμικότητας κτιριακών υποδομών
Πλημμύρα	Περιοχή ευάλωτη σε φυσικές καταστροφές	Αλλαγή περιοχής εγκατάστασης
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
	Ελλιπής συντήρηση κτιριακών υποδομών	Βελτίωση/συντήρηση κτιριακών υποδομών

Παλιρροϊκό κύμα	Περιοχή ευάλωτη σε φυσικές καταστροφές	Αλλαγή περιοχής εγκατάστασης
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
Ρύπανση/Μόλυνση	Περιοχή ευάλωτη σε φυσικές καταστροφές	Αλλαγή περιοχής εγκατάστασης
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
	Μη τήρηση κανονισμών υγιεινής	Συντήρηση εγκαταστάσεων και εξοπλισμού υγιεινής
Ηλεκτρονικές Παρεμβολές	Περιοχή ευάλωτη σε παρεμβολές σημάτων	Αλλαγή περιοχής εγκατάστασης
	Μη ανθεκτικός δικτυακός εξοπλισμός(ασύρματος-ενσύρματος)	Ενίσχυση ανθεκτικότητας δικτυακού εξοπλισμού
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
Κλιματικές Συνθήκες (υγρασία/ θερμοκρασία)	Περιοχή ευάλωτη σε ακραίες συνθήκες υγρασίας και θερμοκρασίας	Αλλαγή περιοχής εγκατάστασης
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου επιχειρηματικής ανάκαμψης (BCP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
	Αδυναμία Σχεδίου Επιχειρηματικής Συνέχειας	Δημιουργία Σχεδίου Επιχειρηματικής Συνέχειας
	Ελλιπής συντήρηση κτιριακών υποδομών	Συντήρηση και ενίσχυση προστασίας κτιριακών υποδομών
	Ανεπαρκής σχεδιασμός αντιμετώπισης κλιματολογικών αλλαγών	Δημιουργία σχεδίου αντιμετώπισης κλιματολογικών αλλαγών

Αγαθά Υλικού (Hardware)

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Ηλεκτρονικές Παρεμβολές	Περιοχή ευάλωτη σε παρεμβολές σημάτων	Αλλαγή περιοχής εγκατάστασης
	Μη ανθεκτικός δικτυακός εξοπλισμός(ασύρματος-ενσύρματος)	Ενίσχυση ανθεκτικότητας δικτυακού εξοπλισμού
	Έλλειψη πλάνου επικοινωνίας σε περίπτωση έκτακτης ανάγκης	Δημιουργία πλάνου έκτακτης ανάγκης
	Έλλειψη σχεδίου ανάκαμψης από καταστροφή (DRP)	Δημιουργία Σχεδίου Επιχειρηματικής Ανάκαμψης
Τεχνικές βλάβες	Ανεπαρκής συντήρηση εγκαταστάσεων και εξοπλισμού	Συντήρηση εγκαταστάσεων και εξοπλισμού
	Μη διαθεσιμότητα των δεδομένων	Εξασφάλιση διαθεσιμότητας δεδομένων
	Προβλήματα δικτύου	Συντήρηση δικτύου
Απώλεια/ διακυμάνσεις ηλεκτρικής ισχύος	Έλλειψη συστήματος UPS	Εγκατάσταση συστήματος UPS
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία εγγράφων ασφαλείας
	Ελλιπής συντήρηση τεχνικού εξοπλισμού	Συντήρηση τεχνικού εξοπλισμού
Σφάλματα Μετάδοσης δεδομένων	Μη διαθεσιμότητα των δεδομένων	Εξασφάλιση διαθεσιμότητας δεδομένων
	Μη διαθεσιμότητα τεχνικού εξοπλισμού	Εξασφάλιση διαθεσιμότητας τεχνικού εξοπλισμού
	Ευάλωτος ενσύρματος και ασύρματος δικτυακός εξοπλισμός	Ενίσχυση ενσύρματου και ασύρματου δικτυακού εξοπλισμού
Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Ανεπαρκής φυσική ασφάλεια	Ενίσχυση φυσικής ασφάλειας
	Ανεπαρκής παρακολούθηση εγκαταστάσεων	Εγκατάσταση συστήματος παρακολούθησης
	Έλλειψη ελέγχου λογαριασμών(audit-logs)	Εφαρμογή συστήματος ελέγχου λογαριασμών(audit-logs)
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
	Ελλιπής αναγνώριση και ταυτοποίηση στοιχείων	Εφαρμογή συστήματος αναγνώρισης και ταυτοποίησης στοιχείων
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία εγγράφων ασφαλείας

	Ελλιπής ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας	Ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
Κλοπή και απάτη	Ανεπαρκής φυσική ασφάλεια	Ενίσχυση φυσικής ασφάλειας
	Ανεπαρκής παρακολούθηση εγκαταστάσεων	Εγκατάσταση συστήματος παρακολούθησης
	Έλλειψη ελέγχου λογαριασμών(audit-logs)	Εφαρμογή συστήματος ελέγχου λογαριασμών(audit-logs)
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
	Ελλιπής αναγνώριση και ταυτοποίηση στοιχείων	Εφαρμογή συστήματος αναγνώρισης και ταυτοποίησης στοιχείων
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία εγγράφων ασφαλείας
	Ελλιπής ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας	Ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
Κακόβουλη καταστροφή δεδομένων και δολιοφθορά	Ανεπαρκής φυσική ασφάλεια	Ενίσχυση φυσικής ασφάλειας
	Ανεπαρκής παρακολούθηση εγκαταστάσεων	Εγκατάσταση συστήματος παρακολούθησης
	Ελλιπής ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας	Ενημέρωση και εκπαίδευση προσωπικού σε ζητήματα ασφαλείας

Αγαθά Λογισμικού (Software)

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Σφάλματα χειρισμού	Χρήση λογισμικού από ανειδίκευτο προσωπικό	Εκπαίδευση προσωπικού για χρήση λογισμικού
	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση προσωπικού σε θέματα ασφαλείας
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Δύσχρηστο λογισμικό	Αλλαγή λογισμικού με κάποιο πιο εύχρηστο
	Έλλειψη ειδικευμένου προσωπικού	Πρόσληψη εξειδικευμένου προσωπικού για χρήση λογισμικού
Σφάλματα ανάπτυξης λογισμικού	Ελλιπής ενημέρωση και εκπαίδευση σε θέματα λογισμικού	Εκπαίδευση προσωπικού σε θέματα ανάπτυξης λογισμικού
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Δύσχρηστο λογισμικό	Αλλαγή λογισμικού με κάποιο πιο εύχρηστο
	Ανεπαρκής έλεγχος προγραμματιστών λογισμικού	Έλεγχος των προγραμματιστών λογισμικού
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ελλιπής έλεγχος λογισμικού για αναφορά προβλημάτων	Συνεχής έλεγχος λογισμικού για παρουσίαση προβλημάτων
	Ανεπαρκείς διαδικασίες ανάπτυξης λογισμικού	Εξασφάλιση επάρκειας διαδικασιών ανάπτυξης λογισμικού
	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση προσωπικού σε θέματα ασφαλείας
	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης

Μη εξουσιοδοτημένες αλλαγές λογισμικού	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκής έλεγχος προγραμματιστών λογισμικού	Έλεγχος των προγραμματιστών λογισμικού
	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση προσωπικού σε θέματα ασφαλείας
	Έλλειψη λογισμικού για διαχείριση αλλαγών	Εγκατάσταση λογισμικού για διαχείριση αλλαγών
	Έλλειψη διαδικασιών παραμετροποίησης λογισμικού	Δημιουργία ειδικών διαδικασιών παραμετροποίησης λογισμικού
	Λανθασμένη παραμετροποίηση λογισμικού	Έλεγχος παραμετροποίησης λογισμικού
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Εγκατάσταση κακόβουλου λογισμικού	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς έλεγχος προγραμματιστών λογισμικού	Έλεγχος των προγραμματιστών λογισμικού
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκείς έλεγχοι συσκευών πριν τη χρήση	Έλεγχος συσκευών πριν τη χρήση για εντοπισμό κακόβουλου λογισμικού

	Ανεπαρκείς πραγματοποίηση ελέγχων για χρήση μη εγκεκριμένου λογισμικού	Πραγματοποίηση ελέγχων για χρήση μη εγκεκριμένου λογισμικού
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ανεπαρκείς έλεγχοι δοκιμών παρείσφρησης	Εγκατάσταση μηχανισμών ελέγχων παρείσφρησης
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Κακόβουλοι εργαζόμενοι	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Ανεπαρκείς έλεγχοι προσωπικού	Πραγματοποίηση ελέγχων του προσωπικού
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Hacking	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση/ισχυροποίηση firewall
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Έλλειψη ιχνών ασφαλείας(audit logs)	Εγκατάσταση συστήματος audit logs
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Μη εξουσιοδοτημένη	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών

πρόσβαση σε δικτυακή ιστοσελίδα	Ελλιπής ισχυροποίηση υποδομών	Ισχυροποίηση υποδομών
	Ανασφαλής αρχιτεκτονική δικτύου	Ισχυροποίηση αρχιτεκτονικής δικτύου
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Άρνηση υπηρεσίας	Ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ελλιπής ισχυροποίηση υποδομών	Ισχυροποίηση υποδομών
Βιομηχανική κατασκοπία	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Έλλειψη ιδιωτικών συμφωνητικών	Υπογραφή ιδιωτικών συμφωνητικών

Εξοπλισμός Δικτύου

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ελλιπής φυσική ασφάλεια	Ενίσχυση φυσικής ασφάλειας
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ανεπαρκείς μηχανισμοί αυθεντικοποίησης	Εγκατάσταση μηχανισμού πιστοποίησης κωδικών και χρηστών
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
Κλοπή και απάτη	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ελλιπής φυσική ασφάλεια	Ενίσχυση φυσικής ασφάλειας
	Ελλιπής κρυπτογράφηση συσκευών	Κρυπτογράφηση συσκευών
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς έλεγχοι προσωπικού	Πραγματοποίηση συχνών ελέγχων του προσωπικού
	Ανεπαρκής εκπαίδευση και ενημέρωση προσωπικού σε	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα

	θέματα ασφαλείας	ασφαλείας
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
	Ελλιπής αναγνώριση και ταυτοποίηση στοιχείων	Εφαρμογή συστήματος αναγνώρισης και ταυτοποίησης στοιχείων
Hacking	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση/ισχυροποίηση firewall
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Έλλειψη ιχνών ασφαλείας(audit logs)	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Ελλιπής ισχυροποίηση εξοπλισμού και υποδομών	Ισχυροποίηση εξοπλισμού και υποδομών
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Μη εξουσιοδοτη-μένες αλλαγές σε λογισμικό	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκής εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ευάλωτοι κωδικοί πρόσβασης/ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
Κακόβουλο λογισμικό	Εσφαλμένα δικαιώματα πρόσβασης	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών

	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών
	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση ή παραμετροποίηση firewall
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
Σφάλματα μετάδοσης	Ανεπαρκής ανθεκτικότητα δικτυακών υποδομών	Ισχυροποίηση εξοπλισμού και υποδομών
	Λανθασμένη λειτουργία δικτυακού εξοπλισμού	Έλεγχος λειτουργίας δικτυακού εξοπλισμού
	Ανεπαρκής προστασία μεταφερόμενων δεδομένων	Κρυπτογράφηση δεδομένων
	Μη διαθεσιμότητα τεχνικού εξοπλισμού	Εξασφάλιση διαθεσιμότητας τεχνικού εξοπλισμού
Σφάλματα χειρισμού	Ανεπαρκής εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας
	Ανεπαρκής ειδίκευση χρηστών εξοπλισμού	Ειδίκευση χρηστών εξοπλισμού
	Δύσχρηστος εξοπλισμός	Χρήση φιλικότερου εξοπλισμού(πιο εύχρηστου) προς τους διαχειριστές
	Ελλιπής αξιολόγηση χρηστών εξοπλισμού	Αξιολόγηση χρηστών εξοπλισμού
	Ελλιπής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
Τεχνικά σφάλματα	Ανεπαρκής συντήρηση εγκαταστάσεων και εξοπλισμού	Συντήρηση δικτύου(εγκαταστάσεις και εξοπλισμός)
	Ανεπαρκής διαχείριση αλλαγών	Επαρκής διαχείριση αλλαγών
	Ανεπαρκής εκπαίδευση και ενημέρωση των χρηστών του δικτύου	Εκπαίδευση και ενημέρωση των χρηστών του δικτύου
	Ελλιπής κάλυψη δικτύου	Ενίσχυση κάλυψης δικτύου
Άρνηση Υπηρεσίας	Έλλειψη πλεονάζοντος εξοπλισμού	Επάρκεια εξοπλισμού(πλεονάζον εξοπλισμός)
	Ανεπαρκής παραμετροποίηση αναχώματος ασφαλείας(firewall)	Επαρκής παραμετροποίηση αναχώματος ασφαλείας-firewall
	Ανεπαρκείς έλεγχοι αποτίμησης αδυναμιών	Εγκατάσταση συστήματος εύρεσης αδυναμιών

	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκής σχεδιασμός δικτύου	Επαρκής σχεδιασμός δικτύου
	Ελλιπής ισχυροποίηση εξοπλισμού και υποδομών	Ισχυροποίηση εξοπλισμού και υποδομών
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
Βιομηχανική κατασκοπία	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Έλλειψη ιδιωτικών συμφωνητικών	Υπογραφή ιδιωτικών συμφωνητικών
Κατάχρηση υποδομών απομακρυσμένης πρόσβασης	Κατάχρηση θυρών απομακρυσμένης πρόσβασης	Έλεγχος κατάχρησης θυρών απομακρυσμένης πρόσβασης
	Έλλειψη ή ανεπάρκεια αναχώματος ασφαλείας(firewall)	Εγκατάσταση/ισχυροποίηση firewall
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εφαρμογή συστήματος αναγνώρισης και ταυτοποίησης στοιχείων
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης

Αγαθά Δεδομένων (Data)

ΑΠΕΙΛΕΣ	ΑΔΥΝΑΜΙΕΣ	ΜΕΤΡΑ
Μη εξουσιοδοτη-μένη πρόσβαση σε δεδομένα	Ελλιπής κρυπτογράφηση κρίσιμων δεδομένων	Κρυπτογράφηση κρίσιμων δεδομένων
	Ελλιπής κρυπτογράφηση συσκευών	Κρυπτογράφηση συσκευών
	Ελλιπής κρυπτογράφηση κωδικών ασφαλείας	Κρυπτογράφηση κωδικών πρόσβασης/ασφαλείας
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ελλιπής κρυπτογράφηση εγγράφων ασφαλείας	Κρυπτογράφηση εγγράφων ασφαλείας
	Ανεπαρκείς έλεγχοι δοκιμών διείσδυσης	Εγκατάσταση συστήματος ανίχνευσης παρείσφρησης (IDS)
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών
	Ελλιπής διακριτικός ή υποχρεωτικός έλεγχος πρόσβασης	Εφαρμογή συστήματος διακριτικού ή υποχρεωτικού ελέγχου πρόσβασης
	Ανεπαρκείς μηχανισμοί αυθεντικοποίησης	Εγκατάσταση μηχανισμού πιστοποίησης κωδικών και χρηστών
	Ελλιπής πολιτική καθαρού γραφείου	Εφαρμογή πολιτικής καθαρού γραφείου
Κακόβουλη καταστροφή δεδομένων	Δυσαρεστημένοι υπάλληλοι	Ικανοποίηση υπαλλήλων
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Ανεπαρκής επικοινωνία της διεύθυνσης με το προσωπικό	Διατήρηση επικοινωνίας μεταξύ διεύθυνσης και προσωπικού
	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκείς μηχανισμοί ταυτοποίησης	Εγκατάσταση μηχανισμού ταυτοποίησης χρηστών

	Ανεπαρκείς μηχανισμοί αυθεντικοποίησης	Εγκατάσταση μηχανισμού πιστοποίησης κωδικών και χρηστών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκείς έλεγχοι προσωπικού	Έλεγχος δραστηριότητας προσωπικού
Κατάχρηση δικαιωμάτων πρόσβασης	Μη διαθεσιμότητα εγγράφων ασφαλείας	Δημιουργία αντιγράφων ασφαλείας
	Ανεπαρκείς μηχανισμοί παρακολούθησης	Εγκατάσταση συστήματος παρακολούθησης εργασιών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκής έλεγχος εργαζομένων	Έλεγχος δραστηριότητας προσωπικού
Σφάλμα χειρισμού	Ανεπαρκής εκπαίδευση προσωπικού σε θέματα ασφαλείας	Εκπαίδευση και ενημέρωση προσωπικού σε θέματα ασφαλείας
	Ανεπαρκής ειδίκευση και εκπαίδευση προσωπικού	Εκπαίδευση και ειδίκευση προσωπικού
Σφάλματα Μετάδοσης δεδομένων	Μη διαθεσιμότητα των δεδομένων	Εξασφάλιση διαθεσιμότητας δεδομένων
	Μη διαθεσιμότητα τεχνικού εξοπλισμού	Εξασφάλιση διαθεσιμότητας τεχνικού εξοπλισμού
	Ευάλωτος ενσύρματος και ασύρματος δικτυακός εξοπλισμός	Ενίσχυση ενσύρματου και ασύρματου δικτυακού εξοπλισμού
Κοινωνική μηχανή	Ανεπαρκής εκπαίδευση και ενημέρωση για την απειλή της κοινωνικής μηχανής	Εκπαίδευση και ενημέρωση προσωπικού για την απειλή της κοινωνικής μηχανής
	Ανεπαρκής ειδίκευση και εκπαίδευση προσωπικού	Εκπαίδευση και ειδίκευση προσωπικού
Βιομηχανική κατασκοπία	Εσφαλμένα δικαιώματα πρόσβασης	Έλεγχος χρηστών για ορθή ανάθεση δικαιωμάτων χρήσης
	Ανεπαρκής καθορισμός/διαχωρισμός διαδικασιών μεταξύ του προσωπικού	Έλεγχος καθορισμού/διαχωρισμού των διαδικασιών/λειτουργιών των χρηστών
	Έλλειψη ιχνών ασφαλείας	Εγκατάσταση συστήματος ιχνών ασφαλείας(audit logs)
	Έλλειψη ιδιωτικών συμφωνητικών	Υπογραφή ιδιωτικών συμφωνητικών

ΠΑΡΑΡΤΗΜΑ Β

Πίνακες δεδομένων δυνατών συνδυασμών μέτρων ασφάλειας

ΠΑΡΑΡΤΗΜΑ Β: Πίνακες δεδομένων δυνατών συνδυασμών μέτρων ασφάλειας

Υλοποίηση ενός μέτρου

ΜΕΤΡΟ	ΒΑΡΟΣ ΜΕΤΡΟΥ	ΚΟΣΤΟΣ ΜΕΤΡΟΥ	ΒΑΡΟΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ	ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
M1	10	0	6,6	79,8	1	10000000
M2	12,25	45000	12,25	74,15	1	10000000
M3	5,25	15000	5,25	81,15	1	10000000
M4	17,5	160000	17,5	68,9	1	10000000
M5	30	0	19,8	66,6	1	10000000
M6	7,5	1650	7,5	78,9	1	10000000
M7	7,5	60000	7,5	78,9	1	10000000
M8	7,5	12000	7,5	78,9	1	10000000
M9	17,5	19000	17,5	68,9	1	10000000
M10	17,5	12000	17,5	68,9	1	10000000

Υλοποίηση δύο μέτρων

ΣΥΝΔΥΑΣΜΟΣ ΔΥΟ ΜΕΤΡΩΝ	ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ	ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ	ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
M1M2	45000	67,55	1	10000000
M1M3	15000	74,55	1	10000000
M1M4	160000	62,3	0,66	6600000
M1M5	0	60	0,66	6600000
M1M6	1650	72,3	1	10000000
M1M7	60000	72,3	1	10000000
M1M8	12000	72,3	1	10000000
M1M9	19000	62,3	0,66	6600000
M1M10	12000	62,3	0,66	6600000
M2M3	60000	68,9	1	10000000
M2M4	205000	56,65	0,66	6600000
M2M5	45000	54,35	0,66	6600000
M2M6	46650	66,65	1	10000000
M2M7	105000	66,65	1	10000000
M2M8	57000	66,65	1	10000000
M2M9	64000	56,65	0,66	6600000
M2M10	57000	56,65	0,66	6600000

M3M4	175000	63,65	0,66	6600000
M3M5	15000	61,35	0,66	6600000
M3M6	16650	73,65	1	10000000
M3M7	75000	73,65	1	10000000
M3M8	27000	73,65	1	10000000
M3M9	34000	63,65	0,66	6600000
M3M10	27000	63,65	0,66	6600000
M4M5	160000	49,1	0,66	6600000
M4M6	161650	61,4	0,66	6600000
M4M7	220000	61,4	0,66	6600000
M4M8	172000	61,4	0,66	6600000
M4M9	179000	51,4	0,66	6600000
M4M10	172000	51,4	0,66	6600000
M5M6	1650	59,1	0,66	6600000
M5M7	60000	59,1	0,66	6600000
M5M8	12000	59,1	0,66	6600000
M5M9	19000	49,1	0,66	6600000
M5M10	12000	49,1	0,66	6600000
M6M9	20650	61,4	0,66	6600000
M6M10	13650	61,4	0,66	6600000
M7M9	79000	61,4	0,66	6600000
M7M10	72000	61,4	0,66	6600000
M8M9	31000	61,4	0,66	6600000
M8M10	24000	61,4	0,66	6600000

Υλοποίηση τριών μέτρων

ΣΥΝΔΥΑΣΜΟΣ ΤΡΙΩΝ ΜΕΤΡΩΝ	ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ	ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ	ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
M1M2M3	60000	62,3	0,66	6600000
M1M2M4	205000	50,05	0,66	6600000
M1M2M5	45000	47,75	0,66	6600000
M1M2M6	46650	60,05	0,66	6600000
M1M2M7	105000	60,05	0,66	6600000
M1M2M8	57000	60,05	0,66	6600000
M1M2M9	64000	50,05	0,66	6600000
M1M2M10	57000	50,05	0,66	6600000
M1M3M4	175000	57,05	0,66	6600000
M1M3M5	15000	54,75	0,66	6600000
M1M3M6	16650	67,05	1	10000000
M1M3M7	75000	67,05	1	10000000

M1M3M8	27000	67,05	1	10000000
M1M3M9	34000	57,05	0,66	6600000
M1M3M10	27000	57,05	0,66	6600000
M1M4M5	160000	42,5	0,66	6600000
M1M4M6	161650	54,8	0,66	6600000
M1M4M7	220000	54,8	0,66	6600000
M1M4M8	172000	54,8	0,66	6600000
M1M4M9	179000	44,8	0,66	6600000
M1M4M10	172000	44,8	0,66	6600000
M1M5M6	1650	52,5	0,66	6600000
M1M5M7	60000	52,5	0,66	6600000
M1M5M8	12000	52,5	0,66	6600000
M1M5M9	19000	42,5	0,66	6600000
M1M5M10	12000	42,5	0,66	6600000
M1M6M9	20650	54,8	0,66	6600000
M1M6M10	13650	54,8	0,66	6600000
M1M7M9	79000	54,8	0,66	6600000
M1M7M10	72000	54,8	0,66	6600000
M1M8M9	31000	54,8	0,66	6600000
M1M8M10	24000	54,8	0,66	6600000
M2M3M4	220000	51,4	0,66	6600000
M2M3M5	60000	49,1	0,66	6600000
M2M3M6	61650	61,4	0,66	6600000
M2M3M7	120000	61,4	0,66	6600000
M2M3M8	72000	61,4	0,66	6600000
M2M3M9	79000	51,4	0,66	6600000
M2M3M10	72000	51,4	0,66	6600000
M2M4M5	205000	36,85	0,66	6600000
M2M4M6	206650	49,15	0,66	6600000
M2M4M7	265000	49,15	0,66	6600000
M2M4M8	217000	49,15	0,66	6600000
M2M4M9	224000	39,15	0,66	6600000
M2M4M10	217000	39,15	0,66	6600000
M2M5M6	46650	46,85	0,66	6600000
M2M5M7	105000	46,85	0,66	6600000
M2M5M8	57000	46,85	0,66	6600000
M2M5M9	64000	36,85	0,66	6600000
M2M5M10	57000	36,85	0,66	6600000
M2M6M9	65650	49,15	0,66	6600000
M2M6M10	58650	49,15	0,66	6600000
M2M7M9	124000	49,15	0,66	6600000
M2M7M10	117000	49,15	0,66	6600000
M2M8M9	76000	49,15	0,66	6600000
M2M8M10	69000	49,15	0,66	6600000
M3M4M5	175000	43,85	0,66	6600000

M3M4M6	176650	56,15	0,66	6600000
M3M4M7	235000	56,15	0,66	6600000
M3M4M8	187000	56,15	0,66	6600000
M3M4M9	194000	46,15	0,66	6600000
M3M4M10	187000	46,15	0,66	6600000
M3M5M6	16650	53,85	0,66	6600000
M3M5M7	75000	53,85	0,66	6600000
M3M5M8	27000	53,85	0,66	6600000
M3M5M9	34000	43,85	0,66	6600000
M3M5M10	27000	43,85	0,66	6600000
M3M6M9	35650	56,15	0,66	6600000
M3M6M10	28650	56,15	0,66	6600000
M3M7M9	94000	56,15	0,66	6600000
M3M7M10	87000	56,15	0,66	6600000
M3M8M9	46000	56,15	0,66	6600000
M3M8M10	39000	56,15	0,66	6600000
M4M5M6	161650	41,6	0,66	6600000
M4M5M7	220000	41,6	0,66	6600000
M4M5M8	172000	41,6	0,66	6600000
M4M5M9	179000	31,6	0,33	3300000
M4M5M10	172000	31,6	0,33	3300000
M4M6M9	180650	43,9	0,66	6600000
M4M6M10	173650	43,9	0,66	6600000
M4M7M9	239000	43,9	0,66	6600000
M4M7M10	232000	43,9	0,66	6600000
M4M8M9	191000	43,9	0,66	6600000
M4M8M10	184000	43,9	0,66	6600000
M5M6M9	20650	41,6	0,66	6600000
M5M6M10	13650	41,6	0,66	6600000
M5M7M9	79000	41,6	0,66	6600000
M5M7M10	72000	41,6	0,66	6600000
M5M8M9	31000	41,6	0,66	6600000
M5M8M10	24000	41,6	0,66	6600000

Υλοποίηση τεσσάρων μέτρων

ΣΥΝΔΥΑΣΜΟΙ ΤΕΣΣΑΡΩΝ ΜΕΤΡΩΝ									
ΣΥΝΔΥΑΣΜΟΣ ΤΡΙΩΝ ΜΕΤΡΩΝ	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΜΕΤΡΟ**	**ΚΟΣΤΟΣ ΜΕΤΡΟΥ**	**ΒΑΡΟΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ**
M1M2M3	60000	62,3	M4	160000	17,5	220000	44,8	0,66	6600000
			M5	0	19,8	60000	42,5	0,66	6600000
			M6	1650	7,5	61650	54,8	0,66	6600000
			M7	60000	7,5	120000	54,8	0,66	6600000
			M8	12000	7,5	72000	54,8	0,66	6600000
			M9	19000	17,5	79000	44,8	0,66	6600000
			M10	12000	17,5	72000	44,8	0,66	6600000
M1M2M4	205000	50,05	M5	0	19,8	205000	30,25	0,33	3300000
			M6	1650	7,5	206650	42,55	0,66	6600000
			M7	60000	7,5	265000	42,55	0,66	6600000
			M8	12000	7,5	217000	42,55	0,66	6600000
			M9	19000	17,5	224000	32,55	0,33	3300000
			M10	12000	17,5	217000	32,55	0,33	3300000
M1M2M5	45000	47,75	M6	1650	7,5	46650	40,25	0,66	6600000
			M7	60000	7,5	105000	40,25	0,66	6600000
			M8	12000	7,5	57000	40,25	0,66	6600000
			M9	19000	17,5	64000	30,25	0,33	3300000
			M10	12000	17,5	57000	30,25	0,33	3300000
M1M2M6	46650	60,05	M9	19000	17,5	65650	42,55	0,66	6600000

			M10	12000	17,5	58650	42,55	0,66	6600000
M1M2M7	105000	60,05	M9	19000	17,5	124000	42,55	0,66	6600000
			M10	12000	17,5	117000	42,55	0,66	6600000
M1M2M8	57000	60,05	M9	19000	17,5	76000	42,55	0,66	6600000
			M10	12000	17,5	69000	42,55	0,66	6600000
M1M3M4	175000	57,05	M5	0	19,8	175000	37,25	0,66	6600000
			M6	1650	7,5	176650	49,55	0,66	6600000
			M7	60000	7,5	235000	49,55	0,66	6600000
			M8	12000	7,5	187000	49,55	0,66	6600000
			M9	19000	17,5	194000	39,55	0,66	6600000
			M10	12000	17,5	187000	39,55	0,66	6600000
M1M3M5	15000	54,75	M6	1650	7,5	16650	47,25	0,66	6600000
			M7	60000	7,5	75000	47,25	0,66	6600000
			M8	12000	7,5	27000	47,25	0,66	6600000
			M9	19000	17,5	34000	37,25	0,66	6600000
			M10	12000	17,5	27000	37,25	0,66	6600000
M1M3M6	16650	67,05	M9	19000	17,5	35650	49,55	0,66	6600000
			M10	12000	17,5	28650	49,55	0,66	6600000
M1M3M7	75000	67,05	M9	19000	17,5	94000	49,55	0,66	6600000
			M10	12000	17,5	87000	49,55	0,66	6600000
M1M3M8	27000	67,05	M9	19000	17,5	46000	49,55	0,66	6600000
			M10	12000	17,5	39000	49,55	0,66	6600000
M1M4M5	160000	42,5	M6	1650	7,5	161650	35	0,66	6600000
			M7	60000	7,5	220000	35	0,66	6600000
			M8	12000	7,5	172000	35	0,66	6600000
			M9	19000	17,5	179000	25	0,33	3300000

			M10	12000	17,5	172000	25	0,33	3300000
M1M4M6	161650	54,8	M9	19000	17,5	180650	37,3	0,66	6600000
			M10	12000	17,5	173650	37,3	0,66	6600000
M1M4M7	220000	54,8	M9	19000	17,5	239000	37,3	0,66	6600000
			M10	12000	17,5	232000	37,3	0,66	6600000
M1M4M8	172000	54,8	M9	19000	17,5	191000	37,3	0,66	6600000
			M10	12000	17,5	184000	37,3	0,66	6600000
M1M5M6	1650	52,5	M9	19000	17,5	20650	35	0,66	6600000
			M10	12000	17,5	13650	35	0,66	6600000
M1M5M7	60000	52,5	M9	19000	17,5	79000	35	0,66	6600000
			M10	12000	17,5	72000	35	0,66	6600000
M1M5M8	12000	52,5	M9	19000	17,5	31000	35	0,66	6600000
			M10	12000	17,5	24000	35	0,66	6600000
M2M3M4	220000	51,4	M5	0	19,8	220000	31,6	0,33	3300000
			M6	1650	7,5	221650	43,9	0,66	6600000
			M7	60000	7,5	280000	43,9	0,66	6600000
			M8	12000	7,5	232000	43,9	0,66	6600000
			M9	19000	17,5	239000	33,9	0,66	6600000
			M10	12000	17,5	232000	33,9	0,66	6600000
M2M3M5	60000	49,1	M6	1650	7,5	61650	41,6	0,66	6600000
			M7	60000	7,5	120000	41,6	0,66	6600000
			M8	12000	7,5	72000	41,6	0,66	6600000
			M9	19000	17,5	79000	31,6	0,33	3300000
			M10	12000	17,5	72000	31,6	0,33	3300000
M2M3M6	61650	61,4	M9	19000	17,5	80650	43,9	0,66	6600000
			M10	12000	17,5	73650	43,9	0,66	6600000

M2M3M7	120000	61,4	M9	19000	17,5	139000	43,9	0,66	6600000
			M10	12000	17,5	132000	43,9	0,66	6600000
M2M3M8	72000	61,4	M9	19000	17,5	91000	43,9	0,66	6600000
			M10	12000	17,5	84000	43,9	0,66	6600000
M2M4M5	205000	36,85	M6	1650	7,5	206650	29,35	0,33	3300000
			M7	60000	7,5	265000	29,35	0,33	3300000
			M8	12000	7,5	217000	29,35	0,33	3300000
			M9	19000	17,5	224000	19,35	0,33	3300000
			M10	12000	17,5	217000	19,35	0,33	3300000
M2M4M6	206650	49,15	M9	19000	17,5	225650	31,65	0,33	3300000
			M10	12000	17,5	218650	31,65	0,33	3300000
M2M4M7	265000	49,15	M9	19000	17,5	284000	31,65	0,33	3300000
			M10	12000	17,5	277000	31,65	0,33	3300000
M2M4M8	217000	49,15	M9	19000	17,5	236000	31,65	0,33	3300000
			M10	12000	17,5	229000	31,65	0,33	3300000
M2M5M6	46650	46,85	M9	19000	17,5	65650	29,35	0,33	3300000
			M10	12000	17,5	58650	29,35	0,33	3300000
M2M5M7	105000	46,85	M9	19000	17,5	124000	29,35	0,33	3300000
			M10	12000	17,5	117000	29,35	0,33	3300000
M2M5M8	57000	46,85	M9	19000	17,5	76000	29,35	0,33	3300000
			M10	12000	17,5	69000	29,35	0,33	3300000
M3M4M5	175000	43,85	M6	1650	7,5	176650	36,35	0,66	6600000
			M7	60000	7,5	235000	36,35	0,66	6600000
			M8	12000	7,5	187000	36,35	0,66	6600000
			M9	19000	17,5	194000	26,35	0,33	3300000
			M10	12000	17,5	187000	26,35	0,33	3300000

M3M4M6	176650	56,15	M9	19000	17,5	195650	38,65	0,66	6600000
			M10	12000	17,5	188650	38,65	0,66	6600000
M3M4M7	235000	56,15	M9	19000	17,5	254000	38,65	0,66	6600000
			M10	12000	17,5	247000	38,65	0,66	6600000
M3M4M8	187000	56,15	M9	19000	17,5	206000	38,65	0,66	6600000
			M10	12000	17,5	199000	38,65	0,66	6600000
M3M5M6	16650	53,85	M9	19000	17,5	35650	36,35	0,66	6600000
			M10	12000	17,5	28650	36,35	0,66	6600000
M3M5M7	75000	53,85	M9	19000	17,5	94000	36,35	0,66	6600000
			M10	12000	17,5	87000	36,35	0,66	6600000
M3M5M8	27000	53,85	M9	19000	17,5	46000	36,35	0,66	6600000
			M10	12000	17,5	39000	36,35	0,66	6600000
M4M5M6	161650	41,6	M9	19000	17,5	180650	24,1	0,33	3300000
			M10	12000	17,5	173650	24,1	0,33	3300000
M4M5M7	220000	41,6	M9	19000	17,5	239000	24,1	0,33	3300000
			M10	12000	17,5	232000	24,1	0,33	3300000
M4M5M8	172000	41,6	M9	19000	17,5	191000	24,1	0,33	3300000
			M10	12000	17,5	184000	24,1	0,33	3300000

Υλοποίηση πέντε μέτρων

ΣΥΝΔΥΑΣΜΟΙ ΠΕΝΤΕ ΜΕΤΡΩΝ									
ΣΥΝΔΥΑΣΜΟΣ ΤΕΣΣΑΡΩΝ ΜΕΤΡΩΝ	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΜΕΤΡΟ**	**ΚΟΣΤΟΣ ΜΕΤΡΟΥ**	**ΒΑΡΟΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ**
M1M2M3M4	220000	44,8	M5	0	19,8	220000	25	0,33	3300000

			M6	1650	7,5	221650	37,3	0,66	6600000
			M7	60000	7,5	280000	37,3	0,66	6600000
			M8	12000	7,5	232000	37,3	0,66	6600000
			M9	19000	17,5	239000	27,3	0,33	3300000
			M10	12000	17,5	232000	27,3	0,33	3300000
M1M2M3M5	60000	42,5	M6	1650	7,5	61650	35	0,66	6600000
			M7	60000	7,5	120000	35	0,66	6600000
			M8	12000	7,5	72000	35	0,66	6600000
			M9	19000	17,5	79000	25	0,33	3300000
			M10	12000	17,5	72000	25	0,33	3300000
M1M2M3M6	61650	54,8	M9	19000	17,5	80650	37,3	0,66	6600000
			M10	12000	17,5	73650	37,3	0,66	6600000
M1M2M3M7	120000	54,8	M9	19000	17,5	139000	37,3	0,66	6600000
			M10	12000	17,5	132000	37,3	0,66	6600000
M1M2M3M8	72000	54,8	M9	19000	17,5	91000	37,3	0,66	6600000
			M10	12000	17,5	84000	37,3	0,66	6600000
M1M2M4M5	205000	30,25	M6	1650	7,5	206650	22,75	0,33	3300000
			M7	60000	7,5	265000	22,75	0,33	3300000
			M8	12000	7,5	217000	22,75	0,33	3300000
			M9	19000	17,5	224000	12,75	0,33	3300000
			M10	12000	17,5	217000	12,75	0,33	3300000
M1M2M4M6	206650	42,55	M9	19000	17,5	225650	25,05	0,33	3300000
			M10	12000	17,5	218650	25,05	0,33	3300000
M1M2M4M7	265000	42,55	M9	19000	17,5	284000	25,05	0,33	3300000
			M10	12000	17,5	277000	25,05	0,33	3300000
M1M2M4M8	217000	42,55	M9	19000	17,5	236000	25,05	0,33	3300000

			M10	12000	17,5	229000	25,05	0,33	3300000
M1M2M5M6	46650	40,25	M9	19000	17,5	65650	22,75	0,33	3300000
			M10	12000	17,5	58650	22,75	0,33	3300000
M1M2M5M7	105000	40,25	M9	19000	17,5	124000	22,75	0,33	3300000
			M10	12000	17,5	117000	22,75	0,33	3300000
M1M2M5M8	57000	40,25	M9	19000	17,5	76000	22,75	0,33	3300000
			M10	12000	17,5	69000	22,75	0,33	3300000
M1M3M4M5	175000	37,25	M6	1650	7,5	176650	29,75	0,33	3300000
			M7	60000	7,5	235000	29,75	0,33	3300000
			M8	12000	7,5	187000	29,75	0,33	3300000
			M9	19000	17,5	194000	19,75	0,33	3300000
			M10	12000	17,5	187000	19,75	0,33	3300000
M1M3M4M6	176650	49,55	M9	19000	17,5	195650	32,05	0,33	3300000
			M10	12000	17,5	188650	32,05	0,33	3300000
M1M3M4M7	235000	49,55	M9	19000	17,5	254000	32,05	0,33	3300000
			M10	12000	17,5	247000	32,05	0,33	3300000
M1M3M4M8	187000	49,55	M9	19000	17,5	206000	32,05	0,33	3300000
			M10	12000	17,5	199000	32,05	0,33	3300000
M1M3M5M6	16650	47,25	M9	19000	17,5	35650	29,75	0,33	3300000
			M10	12000	17,5	28650	29,75	0,33	3300000
M1M3M5M7	75000	47,25	M9	19000	17,5	94000	29,75	0,33	3300000
			M10	12000	17,5	87000	29,75	0,33	3300000
M1M3M5M8	27000	47,25	M9	19000	17,5	46000	29,75	0,33	3300000
			M10	12000	17,5	39000	29,75	0,33	3300000
M1M4M5M6	161650	35	M9	19000	17,5	180650	17,5	0,33	3300000
			M10	12000	17,5	173650	17,5	0,33	3300000

M1M4M5M7	220000	35	M9	19000	17,5	239000	17,5	0,33	3300000
			M10	12000	17,5	232000	17,5	0,33	3300000
M1M4M5M8	172000	35	M9	19000	17,5	191000	17,5	0,33	3300000
			M10	12000	17,5	184000	17,5	0,33	3300000
M2M3M4M5	220000	31,6	M6	1650	7,5	221650	24,1	0,33	3300000
			M7	60000	7,5	280000	24,1	0,33	3300000
			M8	12000	7,5	232000	24,1	0,33	3300000
			M9	19000	17,5	239000	14,1	0,33	3300000
			M10	12000	17,5	232000	14,1	0,33	3300000
M2M3M4M6	221650	43,9	M9	19000	17,5	240650	26,4	0,33	3300000
			M10	12000	17,5	233650	26,4	0,33	3300000
M2M3M4M7	280000	43,9	M9	19000	17,5	299000	26,4	0,33	3300000
			M10	12000	17,5	292000	26,4	0,33	3300000
M2M3M4M8	232000	43,9	M9	19000	17,5	251000	26,4	0,33	3300000
			M10	12000	17,5	244000	26,4	0,33	3300000
M2M3M5M6	61650	41,6	M9	19000	17,5	80650	24,1	0,33	3300000
			M10	12000	17,5	73650	24,1	0,33	3300000
M2M3M5M7	120000	41,6	M9	19000	17,5	139000	24,1	0,33	3300000
			M10	12000	17,5	132000	24,1	0,33	3300000
M2M3M5M8	72000	41,6	M9	19000	17,5	91000	24,1	0,33	3300000
			M10	12000	17,5	84000	24,1	0,33	3300000
M2M4M5M6	206650	29,35	M9	19000	17,5	225650	11,85	0,33	3300000
			M10	12000	17,5	218650	11,85	0,33	3300000
M2M4M5M7	265000	29,35	M9	19000	17,5	284000	11,85	0,33	3300000
			M10	12000	17,5	277000	11,85	0,33	3300000
M2M4M5M8	217000	29,35	M9	19000	17,5	236000	11,85	0,33	3300000

			M10	12000	17,5	229000	11,85	0,33	3300000
M3M4M5M6	176650	36,35	M9	60000	7,5	236650	28,85	0,33	3300000
			M10	12000	7,5	188650	28,85	0,33	3300000
M3M4M5M7	235000	36,35	M9	19000	17,5	254000	18,85	0,33	3300000
			M10	12000	17,5	247000	18,85	0,33	3300000
M3M4M5M8	187000	36,35	M9	19000	17,5	206000	18,85	0,33	3300000
			M10	12000	17,5	199000	18,85	0,33	3300000

Υλοποίηση έξι μέτρων

ΣΥΝΔΥΑΣΜΟΙ ΕΞΙ ΜΕΤΡΩΝ									
ΣΥΝΔΥΑΣΜΟΣ ΠΕΝΤΕ ΜΕΤΡΩΝ	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΜΕΤΡΟ**	**ΚΟΣΤΟΣ ΜΕΤΡΟΥ**	**ΒΑΡΟΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ**
M1M2M3M4M5	220000	25	M6	1650	7,5	221650	17,5	0,33	3300000
			M7	60000	7,5	280000	17,5	0,33	3300000
			M8	12000	7,5	232000	17,5	0,33	3300000
			M9	19000	17,5	239000	7,5	0,33	3300000
			M10	12000	17,5	232000	7,5	0,33	3300000
M1M2M3M4M6	221650	37,3	M9	19000	17,5	240650	19,8	0,33	3300000
			M10	12000	17,5	233650	19,8	0,33	3300000
M1M2M3M4M7	280000	37,3	M9	19000	17,5	299000	19,8	0,33	3300000
			M10	12000	17,5	292000	19,8	0,33	3300000
M1M2M3M4M8	232000	37,3	M9	19000	17,5	251000	19,8	0,33	3300000

			M10	12000	17,5	244000	19,8	0,33	3300000
M1M2M3M5M6	61650	35	M9	19000	17,5	80650	17,5	0,33	3300000
			M10	12000	17,5	73650	17,5	0,33	3300000
M1M2M3M5M7	120000	35	M9	19000	17,5	139000	17,5	0,33	3300000
			M10	12000	17,5	132000	17,5	0,33	3300000
M1M2M3M5M8	72000	35	M9	19000	17,5	91000	17,5	0,33	3300000
			M10	12000	17,5	84000	17,5	0,33	3300000
M1M2M4M5M6	206650	22,75	M9	19000	17,5	225650	5,25	0,33	3300000
			M10	12000	17,5	218650	5,25	0,33	3300000
M1M2M4M5M7	265000	22,75	M9	19000	17,5	284000	5,25	0,33	3300000
			M10	12000	17,5	277000	5,25	0,33	3300000
M1M2M4M5M8	217000	22,75	M9	19000	17,5	236000	5,25	0,33	3300000
			M10	12000	17,5	229000	5,25	0,33	3300000
M1M3M4M5M6	176650	29,75	M9	19000	17,5	195650	12,25	0,33	3300000
			M10	12000	17,5	188650	12,25	0,33	3300000
M1M3M4M5M7	235000	29,75	M9	19000	17,5	254000	12,25	0,33	3300000
			M10	12000	17,5	247000	12,25	0,33	3300000
M1M3M4M5M8	187000	29,75	M9	19000	17,5	206000	12,25	0,33	3300000
			M10	12000	17,5	199000	12,25	0,33	3300000
M2M3M4M5M6	221650	24,1	M9	19000	17,5	240650	6,6	0,33	3300000
			M10	12000	17,5	233650	6,6	0,33	3300000
M2M3M4M5M7	280000	24,1	M9	19000	17,5	299000	6,6	0,33	3300000
			M10	12000	17,5	292000	6,6	0,33	3300000
M2M3M4M5M8	232000	24,1	M9	19000	17,5	251000	6,6	0,33	3300000
			M10	12000	17,5	244000	6,6	0,33	3300000

Υλοποίηση επτά μέτρων

ΣΥΝΔΥΑΣΜΟΙ 7 ΜΕΤΡΩΝ									
ΣΥΝΔΥΑΣΜΟΣ ΕΞΙ ΜΕΤΡΩΝ	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΜΕΤΡΟ**	**ΚΟΣΤΟΣ ΜΕΤΡΟΥ**	**ΒΑΡΟΣ ΜΕΤΡΟΥ * ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΚΟΣΤΟΣ ΣΥΝΔΥΑΣΜΟΥ ΜΕΤΡΩΝ**	**ΣΚΟΡ ΑΔΥΝΑΜΙΑΣ**	**ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ**	**ΣΚΟΡ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ**
M1M2M3M4M5M6	221650	17,5	M9	19000	17,5	240650	0	0,33	3300000
			M10	12000	17,5	233650	0	0,33	3300000
M1M2M3M4M5M7	280000	17,5	M9	19000	17,5	299000	0	0,33	3300000
			M10	12000	17,5	292000	0	0,33	3300000
M1M2M3M4M5M8	232000	17,5	M9	19000	17,5	251000	0	0,33	3300000
			M10	12000	17,5	244000	0	0,33	3300000

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] AbeleWigert I., Dunn M., "An Inventory of 20 National and 6 International Critical Infrastructure Protection Policies", International CIIP Handbook 2006 (Vol. I), in: A. Wenger, V. Mauer (Eds.), for Security Studies, ETH Zurich, 2006.

[2] B. Hammerli, A. Renda, Protecting critical infrastructure in the EU, Centre for European Policy Studies, Belgium, 2010.

[3] T. Ntouskas, N. Polemi, "A secure, collaborative environment for the security management of port information systems", in Proc. of the 5th International Conference on the Internet and Web Applications and Services, pp. 374-379, IEEE Press, Spain, 2010.

[4] ENISA, Workshop on cyber security aspects in the maritime sector, Brussels, 2011.

[5] N. Polemi, T. Ntouskas, "Open issues and proposals in the IT security management of commercial ports: The S-Port national case", in Proc. of the 27th IFIP International Information Security and Privacy Conference, pp. 567-572, Springer (IFIP AICT 376), Greece, 2012.

[6] Polemi N., Ntouskas T., "Open Issues and Proposals in the IT Security Management of Commercial Ports: The S-PORT National Case". In: D. Gritzalis, S. Furnell, and M. Theoharidou (Eds.): SEC 2012, IFIP AICT 376, pp. 567–572, 2012.

[7] N. Polemi, Security management of the ports' information systems ENISA project, http://www.enisa.europa.eu (accessed 20 March 2013).

[8] M. Theoharidou, D. Gritzalis, "A Common Body of Knowledge for information security", IEEE Security & Privacy, Vol. 5, No. 2, pp. 64-67, March/April 2007.

[9] Παναγιώτης Κοτζανικολάου, Σημειώσεις μαθήματος Τεχνολογίες και Πολιτικές Ασφάλειας, Έκδοση 2η (Οκτώβριος 2007).

[10] ISO/IEC 27001:2005: Information technology - Security techniques - Information security management systems – Requirements, International Organization for Standardization, Geneva, Switzerland, 2005.

[11] ISO/IEC 27002:2005: Information technology - Security techniques - Code of practice for information security management, International Organization for Standardization, Geneva, Switzerland, 2005.

[12] ISO/IEC 27005:2008: Information Technology - Security Techniques - Information Security Risk Management, 2008.

[13] National Institute for Standards and Technology, Risk management guide for information technology systems, NIST Special Publication 800-30, USA, July 2002.

[14] ISO/IEC 17799:2005: Information technology - Security techniques - Code of practice for information security management, 2005.

[15] ENISA, The Risk Management Process, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process.

[16] ENISA, Risk Assessment, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment.

[17] ENISA, Risk Treatment , http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

[18] ENISA, Risk Acceptance, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-acceptance.

[19] ENISA, Inventory of Risk Management / Risk Assessment Methods.

[20] CRAMM, http://www.cramm.com.

[21] Insight Consulting, CRAMM User Guide, Issue 5.1, United Kingdom, 2005.

[22] Ebios, http://ebios.cases-cc.org.

[23] Expression of Needs and Identification of Security Objectives PREMIER MINISTRE Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil. Available www.ssi.gouv.fr.

[24] Magerit, http://www.csi.map.es/csi/pg5m20.htm.

[25] Magerit, http://www.ccn.cni.es - http://www.ar-tools.com.

[26] Club de la Securite de L' information Francais Methods Commision, Mehari 2010 Risk analysis and treatment Guide, France, August 2010 (accessed December2010) http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk- Analysis-and-Treatment-Guide.pdf.

[27] OCTAVE Method Implementation Guide Version 2.0, Carnegie Mellon University, June 2001 http://www.cert.org/octave/ (accessed December 2011).

[28] Θεόδωρος Ν. Ντούσκας, Διδακτορική Διατριβή «Συνεργατική, πολυκριτηριακή διαχείριση ασφάλειας Πληροφοριακών Συστημάτων», Πειραιάς, Σεπτέμβριος 2012.

[29] STORM-RM Secure Tool for Risk management, http://www.storm-rm.com, http://www.storm-rm.com/main/phases.

[30] Πολυκριτήρια Συστήματα Αποφάσεων – Δρ. Μιχάλης Δούμπος – Πολυτεχνείο Κρήτης, Τμήμα Μηχανικών Παραγωγής και Διοίκησης – Χανιά 2003.

[31] Pardalos, P.M., Siskos, Y., Zopounidis, C., "Advances in multicriteria analysis", Kluwer Academic Publishers, Dordrecht, 1995.

[32] Roy, B. , "Méthodologie Multicritère d'Aide à la Décision", Economica, Paris, (1985).

[33] Σίσκος, Ι., 2008. Μοντέλα αποφάσεων. Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

[34] Σίσκος, Γ. (1998). Γραμμικός Προγραμματισμός, Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

[35] Roy, B. and Bouyssou, D., Aide Multicritère à la Décision: Méthodes et Cas, Economica, Paris, 1993.

[36] Roy, B., 1990. Decision aid and decision making. In: C.A. Bana e Costa (Editor), Readings in Multiple Criteria Decision Aid. Springer, Berlin, pp. 17-35.

[37] Bernard Roy, Daniel Vanderpooten, "The European School of MCDA: Emergence, Basic Features and Current Works", Journal of Multi-Criteria Decision Analysis, Vol.5, pp22-38, 1996.

[38] Siskos, Y., Spyridakos, A., (1999), Intelligent multicriteria support: Overview and perspectives, European Journal of Operational Research, 113, 236-246.

[39] Roy, B., Vincke, Ph., (1981), Multicriteria analysis: survey and new directions,European Journal of Operational Research, 8, 207-218.

[40] Von Winterfeldt D, Edwards W., 1993. *Decision Analysis and Behavioral Research*. Cambridge University Press, New York.

[41] Doumpos, M. and C. Zopounidis, Multicriteria decision aid classification methods, Kluwer Academic Publishers, Dordrecht, 2002.

[42] Γρηγορούδης, Ε., Μ. Δούμπος, Κ. Ζοπουνίδης και Ν.Ματσατσίνης (Εκδ.), Πολυκριτήρια ανάλυση αποφάσεων: Μεθολογικές προσεγγίσεις και εφαρμογές, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[43] Ματσατσίνης, Ν. και Κ. Ζοπουνίδης (Εκδ.), Συστήματα αποφάσεων με πολλαπλά κριτήρια, Κλειδάριθμος, Αθήνα 2007.

[44] Κοσμίδου, Κ., Κ. Ζοπουνίδης και Μ. Δούμπος (Εκδ.), Αποφάσεις με πολλαπλά κριτήρια, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2005.

[45] Πραστάκος, Γ.Π., Διοικητική Επιστήμη: Λήψη Επιχειρησιακών αποφάσεων στην κοινωνία της πληροφορίας, Εκδόσεις Σταμούλη, Αθήνα,2006.