Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάλυση και Διαχείριση Κινδύνου σε Συστήματα Διαχείρισης Πληροφοριών**
Ονοματεπώνυμο Φοιτητή	ΕΥΣΤΑΘΙΟΥ ΔΗΜΗΤΡΙΟΣ
Αριθμός Μητρώου	ΜΠΣΠ08005
Κατεύθυνση	ΣΥΣΤΗΜΑΤΑ ΥΠΟΣΤΗΡΙΞΗΣ ΑΠΟΦΑΣΕΩΝ
Επιβλέπων Καθηγητής	ΔΟΥΛΗΓΕΡΗΣ ΧΡΗΣΤΟΣ
Συνεπιβλέπων	ΜΗΤΡΟΠΟΥΛΟΣ ΣΑΡΑΝΤΗΣ

Ημερομηνία Παράδοσης Οκτώβριος 2011

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δουληγέρης Χρήστος Καθηγητής	Βέργαδος Δημήτριος Λέκτορας	Κοτζανικολάου Παναγιώτης Λέκτορας

Περίληψη.

Η δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης κινδύνων αποτελεί σημαντική συνιστώσα ενός ολοκληρωμένου προγράμματος ασφαλείας σε επίπεδο IT και ταυτόχρονα συλλογική ευθύνη της διοίκησης ενός οργανισμού. Για τον εντοπισμό και την αξιολόγηση των κενών ασφάλειας και την υλοποίηση των απαραίτητων ελέγχων, είναι απαραίτητη η διεξαγωγή δύο βασικών σταδίων, του εντοπισμού και αξιολόγησης κινδύνων (IT risk assessment) και του περιορισμού των κινδύνων (Risk Mitigation). Στην παρούσα εργασία παρουσιάζεται μια μεθοδολογία εντοπισμού και αξιολόγησης κινδύνων, που περιλαμβάνει εννέα στάδια (Χαρακτηρισμός Συστήματος, Προσδιορισμός Απειλών, Αναγνώριση Αδυναμιών, Ανάλυση Ελέγχων, Προσδιορισμός Πιθανοτήτων, Ανάλυση Επιπτώσεων, Προσδιορισμός των Κινδύνων, Συστάσεις Ελέγχων, Τεκμηρίωση Αποτελεσμάτων). Παρουσιάζεται επίσης μια μεθοδολογία περιορισμού των κινδύνων, η οποία περιλαμβάνει επτά στάδια (Προτεραιοποίηση Ενεργειών/ Δράσεων, Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων, Διεξαγωγή Ανάλυσης Κόστους – Οφέλους, Επιλογή Ελέγχων, Ανάθεση Αρμοδιοτήτων, Ανάπτυξη Πλάνου Υλοποίησης Προστασίας, Υλοποίηση Επιλεγμένων Ελέγχων). Η αντιμετώπιση και ο περιορισμός των κινδύνων αυτών, απαντάται συνήθως από ένα Οργανισμό με μία ή περισσότερες από επιλογές όπως ανάληψη, αποφυγή, περιορισμός ή μετακύληση κινδύνου. Τέλος, οι παραπάνω μεθοδολογίες για την αξιολόγηση και τον περιορισμό των κινδύνων, αποτυπώνονται σε πρακτικό επίπεδο στη μελέτη περίπτωσης που παρατίθεται στην παρούσα εργασία και αφορά σε ένα Τραπεζικό Οργανισμό.

Ευχαριστίες.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω θερμά τον κύριο Δουληγέρη για την ευκαιρία που μου έδωσε να υλοποιήσω το συγκεκριμένο θέμα διπλωματικής εργασίας, καθώς και τον κύριο Μητρόπουλο που με αμεσότητα και ευστοχία με κατεύθυνε σε όλη την διαδικασία συγγραφής της εργασίας.

Πίνακας Περιεχομένων Εργασίας

Περίληψη Εργασίας.

Η Διαχείριση Κινδύνων (Risk Management) διαδραματίζει κρίσιμο ρόλο στην προστασία των πληροφοριών και των περιουσιακών στοιχείων του Οργανισμού. Επομένως, η δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης κινδύνων αποτελεί σημαντική συνιστώσα ενός ολοκληρωμένου προγράμματος ασφαλείας σε επίπεδο IT και ταυτόχρονα συλλογική ευθύνη της Διοίκησης ενός Οργανισμού. Για το λόγο αυτό εμπλέκεται ένας σημαντικός αριθμός ρόλων και ανθρώπινων πόρων και πρέπει να ενσωματωθεί πλήρως σε όλο το εύρος του Κύκλου Ζωής των συστημάτων. Για τον εντοπισμό και την αξιολόγηση των κενών ασφάλειας και την υλοποίηση των απαραίτητων ελέγχων, είναι απαραίτητη η διεξαγωγή αξιολόγησης IT κινδύνων (IT risk assessment) η οποία εστιάζει σε σημεία όπως αρχιτεκτονική και στρατηγική ασφάλειας πληροφοριών και συστημάτων και αξιολόγηση τεχνολογικών και πληροφοριακών κινδύνων, εντοπίζοντας τις πηγές απειλών και τα τρωτά σημεία των συστημάτων και αξιολογώντας τις επιπτώσεις αυτών για τον Οργανισμό. Το αποτέλεσμα αυτής της αξιολόγησης βοηθά εν συνεχεία στον εντοπισμό κατάλληλων ελέγχων, η εφαρμογή των οποίων θα οδηγήσει στη μείωση ή την εξάλειψη των κινδύνων αυτών (risk mitigation – elimination). Στην παρούσα εργασία παρουσιάζεται μια μεθοδολογία εντοπισμού και αξιολόγησης κινδύνων, που περιλαμβάνει εννέα στάδια (Χαρακτηρισμός Συστήματος, Προσδιορισμός Απειλών, Αναγνώριση Αδυναμιών, Ανάλυση Ελέγχων, Προσδιορισμός Πιθανοτήτων, Ανάλυση Επιπτώσεων, Προσδιορισμός των Κινδύνων, Συστάσεις Ελέγχων, Τεκμηρίωση Αποτελεσμάτων). Παρουσιάζεται επίσης μια μεθοδολογία περιορισμού των κινδύνων (risk mitigation), η οποία περιλαμβάνει επτά στάδια (Προτεραιοποίηση Ενεργειών / Δράσεων, Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων, Διεξαγωγή Ανάλυσης Κόστους – Οφέλους, Επιλογή Ελέγχων, Ανάθεση Αρμοδιοτήτων, Ανάπτυξη Πλάνου Υλοποίησης Προστασίας, Υλοποίηση Επιλεγμένων Ελέγχων) και στοχεύει στη μείωση των κινδύνων που αντιμετωπίζει ένας Οργανισμός. Η αντιμετώπιση και ο περιορισμός των κινδύνων αυτών, απαντάται συνήθως από ένα Οργανισμό με μία ή περισσότερες από επιλογές όπως ανάληψη, αποφυγή, περιορισμός ή μετακύληση κινδύνου. Τέλος, οι παραπάνω μεθοδολογίες για την αξιολόγηση και τον περιορισμό των κινδύνων, αποτυπώνονται σε πρακτικό επίπεδο στη μελέτη περίπτωσης που παρατίθεται στην παρούσα εργασία και αφορά σε ένα Τραπεζικό Οργανισμό XYZ.

Abstract.

Risk Management plays a critical role in protecting information and assets in an Organization. Thus, the creation of an effective risk management process is an important component of a comprehensive security program at IT level. At the same time, this process is responsibility of Organization's Management. The process itself involves a significant number of roles and human resources and should be fully integrated throughout the entire lifecycle of systems. To identify and assess gaps in security and implement the necessary controls, it is necessary to conduct an IT risk assessment, which focuses on areas such as architecture and security strategy of information systems. This assessment tries to identify sources of threats and vulnerabilities of the IT systems and assess their impact on the mission of the Organization. The result of this evaluation further helps in identifying appropriate controls, the implementation of which will reduce or eliminate risks (risk mitigation - elimination). This paper presents a methodology for identifying and assessing risks, including nine stages (System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, Results Documentation). Also, at this work we present a methodology for risk mitigation, which includes seven stages (Prioritize Actions, Evaluate Recommended Control Options, Conduct Cost-Benefit Analysis, Select Control, Assign Responsibility, Develop a Safeguard Implementation Plan, Implement Selected Controls) and aims to reduce the risks an Organization runs. Tackling and reducing these risks, is usually done by an Organization with one or more options such as withdrawal, avoidance, reduction or shift risk. The proposed methodologies for assessing and mitigating risk, are used in practice in the case study included in this work regarding XYZ Bank.

1. Εκτελεστική Σύνοψη (Executive Summary)

Ο κύριος στόχος κάθε Οργανισμού είναι η όσο το δυνατό καλύτερη παρακολούθηση της λειτουργίας και των επιδόσεών του αλλά και η υποστήριξη στη λήψη αποφάσεων. Ειδικότερα, η Διαχείριση Κινδύνων (Risk Management) διαδραματίζει έναν κρίσιμο ρόλο στην προστασία των πληροφοριών-περιουσιακών στοιχείων του Οργανισμού και ως εκ τούτου, η δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης κινδύνων αποτελεί σημαντική συνιστώσα ενός ολοκληρωμένου προγράμματος ασφαλείας σε επίπεδο IT. Επιπλέον, η διαδικασία διαχείρισης των κινδύνων δεν πρέπει να αντιμετωπίζεται ως μια «τεχνική» λειτουργία που διεξάγεται από ειδικούς του IT, αλλά ως μια βασική λειτουργία του Οργανισμού συνολικά.

Στην παρούσα εργασία εξετάζονται οι δυνατές επιλογές ενός Οργανισμού για να εφαρμόσει ελέγχους ασφαλείας. Οι έλεγχοι αυτοί μπορούν να χρησιμοποιηθούν για τον περιορισμό των κινδύνων για την καλύτερη προστασία των κρίσιμων πληροφοριών και των συστημάτων πληροφορικής που αποθηκεύουν και μεταφέρουν αυτές τις πληροφορίες. Οι προτεινόμενοι έλεγχοι μπορούν να επεκταθούν περαιτέρω ή να συντομευθούν ανάλογα με τις ιδιαιτερότητες και τις εξειδικευμένες ανάγκες του Οργανισμού.

Η διαχείριση κινδύνων αποτελεί συλλογική ευθύνη της Διοίκησης ενός Οργανισμού. Για το λόγο αυτό εμπλέκεται ένας σημαντικός αριθμός ρόλων και κατά συνέπεια ένας μεγάλος αριθμός ανθρώπινων πόρων. Για να είναι αποτελεσματική η διαδικασία διαχείρισης κινδύνων θα πρέπει να ενσωματωθεί πλήρως σε όλο το εύρος του Κύκλου Ζωής Συστημάτων (System Life Cycle), δηλαδή κατά την έναρξη, ανάπτυξη / απόκτηση, υλοποίηση, λειτουργία / συντήρηση και διάθεση κάθε συστήματος.

Απαραίτητη για κάθε Οργανισμό είναι η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας συστημάτων και πληροφοριών. Η διασφάλιση των αρχών αυτών προϋποθέτει τον αποτελεσματικό σχεδιασμό και τη διαρκή αξιολόγηση της ασφάλειας συστημάτων και πληροφοριών ([G04]). Για τον εντοπισμό και την αξιολόγηση των κενών ασφάλειας και την υλοποίηση των απαραίτητων ελέγχων, είναι απαραίτητη η διεξαγωγή μιας διαδικασίας αξιολόγησης IT κινδύνων (IT risk assessment) η οποία εστιάζει σε σημεία όπως αρχιτεκτονική και στρατηγική ασφάλειας πληροφοριών και συστημάτων και αξιολόγηση τεχνολογικών και πληροφοριακών κινδύνων, εντοπίζοντας τις πηγές απειλών και τα τρωτά σημεία των συστημάτων και αξιολογώντας τις επιπτώσεις αυτών στον Οργανισμό ([LC03]).

Ο εντοπισμός και η αξιολόγηση κινδύνων (risk assessment) είναι το πρώτο βήμα που ακολουθείται σε όλες σχεδόν τις μεθοδολογίες διαχείρισης κινδύνων. Κατά το βήμα αυτό, οι Οργανισμοί καθορίζουν το εύρος των δυνητικών απειλών για τα IT συστήματα και των κινδύνων που απορρέουν σε όλο τον Κύκλο Ζωής των συστημάτων. Το αποτέλεσμα αυτής της διαδικασίας βοηθά εν συνεχεία στον εντοπισμό κατάλληλων ελέγχων η εφαρμογή των οποίων θα οδηγήσει στη μείωση ή την εξάλειψη των κινδύνων αυτών (risk mitigation – elimination), διαδικασία η οποία αποτελεί επόμενο βήμα της προτεινόμενης μεθοδολογίας. Για να προσδιοριστεί η πιθανότητα ενός μελλοντικού ανεπιθύμητου γεγονότος, οι απειλές για ένα IT σύστημα θα πρέπει να αναλυθούν σε συνδυασμό με τις πιθανές αδυναμίες και τους ελέγχους που είναι εν ισχύ για το εν λόγω σύστημα.

Στην παρούσα εργασία παρουσιάζεται μια μεθοδολογία εντοπισμού και αξιολόγησης κινδύνων, που περιλαμβάνει εννέα στάδια. Συνοπτικά τα στάδια αυτά είναι:

- Χαρακτηρισμός Συστήματος
- Προσδιορισμός Απειλών
- Αναγνώριση Αδυναμιών
- Ανάλυση Ελέγχων

- Προσδιορισμός Πιθανοτήτων
- Ανάλυση Επιπτώσεων
- Προσδιορισμός των Κινδύνων
- Συστάσεις Ελέγχων
- Τεκμηρίωση Αποτελεσμάτων

Ο περιορισμός των κινδύνων (risk mitigation) είναι μια συστηματική μεθοδολογία που στοχεύει στη μείωση των κινδύνων που αντιμετωπίζει ένας Οργανισμός οι οποίοι μπορεί να έχουν αντίκτυπο στην εκπλήρωση της αποστολής του. Η αντιμετώπιση και ο περιορισμός των κινδύνων αυτών, απαντάται συνήθως από ένα Οργανισμό με μία ή περισσότερες από επιλογές όπως ανάληψη, αποφυγή, περιορισμός ή μετακύληση κινδύνου. Οι στόχοι και η αποστολή του Οργανισμού θα πρέπει να λαμβάνονται υπόψη για την χρησιμοποίηση ή όχι οποιασδήποτε από τις παραπάνω επιλογές. Κατά κανόνα, δεν είναι πρακτικά εφικτό για ένα Οργανισμό να αντιμετωπίσει όλους τους κινδύνους που έχουν εντοπιστεί, επομένως πρέπει να δίνεται προτεραιότητα σε εκείνα τα ζεύγη απειλών / αδυναμιών που δυνητικά μπορούν να προκαλέσουν σημαντικές βλάβες και να έχουν σοβαρό αντίκτυπο στην επίτευξη της αποστολής του Οργανισμού.

Τα βασικά στάδια της προτεινόμενης στην παρούσα εργασία μεθοδολογίας περιορισμού των κινδύνων, είναι:

- Προτεραιοποίηση Ενεργειών / Δράσεων.
- Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων.
- Διεξαγωγή Ανάλυσης Κόστους – Οφέλους.
- Επιλογή Ελέγχων.
- Ανάθεση Αρμοδιοτήτων.
- Ανάπτυξη Πλάνου Υλοποίησης Προστασίας.
- Υλοποίηση Επιλεγμένων Ελέγχων.

Για την κατανομή των πόρων (υλικών και ανθρώπινων) και την υλοποίηση αποδοτικών και αποτελεσματικών ελέγχων, οι Οργανισμοί, μετά τον εντοπισμό

όλων των δυνατών ελέγχων και την αξιολόγηση της εφικτότητας και της αποτελεσματικότητάς τους, θα πρέπει να προβαίνουν σε ανάλυση κόστους-οφέλους για κάθε προτεινόμενο έλεγχο για να καθορίσουν τελικά τους έλεγχους που θα υλοποιήσουν. Η ανάλυση κόστους - οφέλους μπορεί να είναι ποιοτική ή ποσοτική. Στόχος της είναι να καταδείξει ότι το κόστος υλοποίησης των ελέγχων μπορεί να αιτιολογηθεί από τη μείωση του επιπέδου κινδύνου.

Οι παραπάνω μεθοδολογίες για την αξιολόγηση και τον περιορισμό των κινδύνων, αποτυπώνονται σε πρακτικό επίπεδο στη μελέτη περίπτωσης που παρατίθεται στην παρούσα εργασία και αφορά σε ένα Τραπεζικό Οργανισμό XYZ.

Συμπερασματικά, θα μπορούσαμε να πούμε ότι τα πρότυπα ασφάλειας ενός Οργανισμού πρέπει να εμπεριέχουν ένα σύνολο ελέγχων και κατευθυντήριων γραμμών οι οποίοι να διασφαλίζουν ότι οι διαδικασίες ασφαλείας που διέπουν τη χρήση των IT συστημάτων και των πόρων του Οργανισμού, εφαρμόζονται ορθά και είναι ευθυγραμμισμένες με τους στόχους και την αποστολή του.

2. Εισαγωγή - Ανασκόπηση Θεματικής Περιοχής

Στη σύγχρονη τεχνολογικά εποχή που διανύουμε, σχεδόν κάθε Οργανισμός χρησιμοποιεί τις Τεχνολογίες Πληροφοριών (Information Management – IT) για την ταχύτερη, ακριβέστερη και εν γένει αποτελεσματικότερη διαχείριση και επεξεργασία των πληροφοριών του. Ο κύριος στόχος είναι η όσο το δυνατό καλύτερη παρακολούθηση της λειτουργίας και των επιδόσεων του Οργανισμού αλλά και η υποστήριξη στη λήψη αποφάσεων. Μέσα στο πλαίσιο αυτό, η Διαχείριση Κινδύνων (Risk Management) διαδραματίζει έναν κρίσιμο ρόλο στην προστασία των πληροφοριών-περιουσιακών στοιχείων του Οργανισμού. Ως εκ τούτου, η δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης κινδύνων αποτελεί σημαντική συνιστώσα ενός ολοκληρωμένου προγράμματος ασφαλείας σε επίπεδο IT. Ο κύριος στόχος της διαδικασίας διαχείρισης κινδύνων του Οργανισμού θα πρέπει να είναι η προστασία του Οργανισμού και η διασφάλιση ότι θα έχει τη δυνατότητα να εκτελέσει την αποστολή του. Επομένως, η διαδικασία διαχείρισης των κινδύνων δεν πρέπει να αντιμετωπίζεται ως μια «τεχνική» λειτουργία που διεξάγεται από ειδικούς του IT, αλλά ως μια βασική λειτουργία του Οργανισμού συνολικά. Σύμφωνα με τον ([LC03]), οι διαρκώς μεταβαλλόμενες συνθήκες σε θέματα ανταγωνισμού και τεχνολογίας, καθώς επίσης και το ευμετάβλητο κοινωνικο-οικονομικό περιβάλλον, έχουν σημαντικά αυξήσει τον πιθανό αντίκτυπο δυσλειτουργιών που αφορούν στη λειτουργία ενός Οργανισμού.

Αν επιχειρήσουμε να ορίσουμε τον κίνδυνο, θα μπορούσαμε να πούμε ότι είναι η καθαρή αρνητική επίδραση που θα προέκυπτε σε περίπτωση που λάμβανε χώρα κάποιο ή κάποια γεγονότα τα οποία έχουν αντίκτυπο στην ομαλή λειτουργία του Οργανισμού, λαμβάνοντας υπόψη τόσο την πιθανότητα όσο και τον αντίκτυπο των γεγονότων αυτών. Διαχείριση κινδύνων είναι η διαδικασία προσδιορισμού και εκτίμησης του κινδύνου και η λήψη των κατάλληλων μέτρων

για τον περιορισμό τους σε αποδεκτά επίπεδα ([JA05]). Στην παρούσα εργασία, προτείνουμε τις βασικές κατευθύνσεις για την ανάπτυξη ενός αποτελεσματικού προγράμματος διαχείρισης IT κινδύνων, ενώ δίνεται ιδιαίτερη έμφαση στους ορισμούς και την πρακτική καθοδήγηση που απαιτείται για την αξιολόγηση και τον περιορισμό των κινδύνων που εντοπίζονται στα πληροφοριακά συστήματα.

Είναι βεβαίως σημαντικό η διαχείριση των IT κινδύνων να στοχεύει στη διατήρηση μιας ισορροπίας μεταξύ των απαραίτητων μέτρων ασφαλείας και του κόστους που τα μέτρα αυτά συνεπάγονται, ώστε το τελικό αποτέλεσμα αυτή να προσθέτει πραγματική αξία στον Οργανισμό ([SCL]). Είναι επίσης ιδιαίτερα σημαντικό για κάθε Οργανισμό, να κατανοεί σε βάθος τους κινδύνους και τις απαραίτητες διαδικασίες και σημεία ελέγχου των λειτουργιών που υποστηρίζονται από τα πληροφοριακά συστήματα, ώστε να είναι σε θέση να παρέχει τη διαβεβαίωση ότι όλα τα συστήματα του Οργανισμού πληρούν τις προδιαγραφές ασφάλειας και είναι σύμφωνα με ελεγκτικά πρότυπα και οδηγίες.

Στην παρούσα εργασία εξετάζονται οι δυνατές επιλογές του Οργανισμού για να εφαρμόσει ελέγχους ασφαλείας. Οι έλεγχοι αυτοί μπορούν να χρησιμοποιηθούν για τον περιορισμό των κινδύνων για την καλύτερη προστασία των κρίσιμων πληροφοριών και των συστημάτων πληροφορικής που αποθηκεύουν και μεταφέρουν αυτές τις πληροφορίες. Οι προτεινόμενες διαδικασίες / έλεγχοι μπορούν να επεκταθούν περαιτέρω ή να συντομευθούν ανάλογα με τις ιδιαιτερότητες και τις εξειδικευμένες ανάγκες του Οργανισμού.

Επιπλέον, απαραίτητη για κάθε Οργανισμό είναι η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας συστημάτων και πληροφοριών ([SCL], [N02]). Η διασφάλιση των αρχών αυτών προϋποθέτει τον αποτελεσματικό σχεδιασμό και διαρκή αξιολόγηση της ασφάλειας συστημάτων και πληροφοριών ([G04]). Για τον εντοπισμό και την αξιολόγηση των κενών ασφάλειας και την υλοποίηση των απαραίτητων ελέγχων, είναι απαραίτητη η διεξαγωγή μιας διαδικασίας αξιολόγησης IT κινδύνων (IT risk assessment). Η

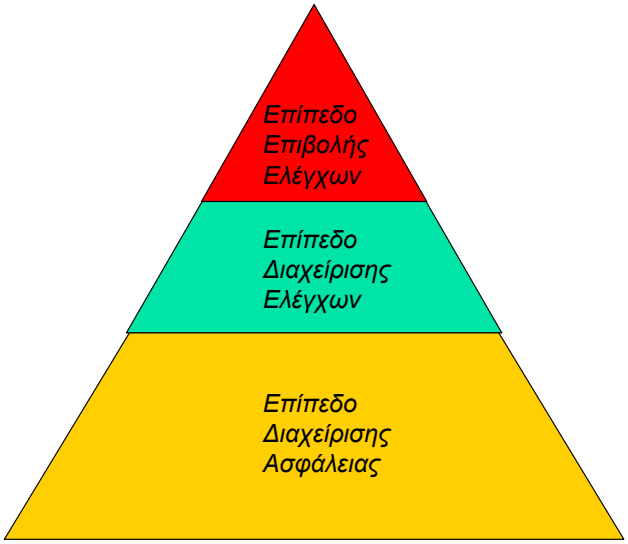
διαδικασία αξιολόγησης IT κινδύνων σε ένα Οργανισμό πρέπει να εστιάζει σε σημεία όπως ([JA05], [N02]):

- Σχεδιασμός αρχιτεκτονικής και στρατηγικής ασφάλειας πληροφοριών, συστημάτων και επιχειρησιακής συνέχειας.
- Ανάπτυξη και διαχείριση επιχειρησιακού προγράμματος για την ασφάλεια συστημάτων και πληροφοριών.
- Αξιολόγηση τεχνολογικών και πληροφοριακών κινδύνων, εντοπίζοντας τις πηγές απειλών και τα τρωτά σημεία των συστημάτων και αξιολογώντας τις επιπτώσεις αυτών στον Οργανισμό.
- Διαρκής αποτίμηση της αποτελεσματικότητας του σχεδιασμού και της εφαρμογής των απαραίτητων δικλείδων ασφάλειας στα συστήματα.
- Κατανόηση και τεκμηρίωση πολύπλοκων διαδικασιών και σημείων ελέγχου, αξιοποιώντας εξειδικευμένες τεχνικές.
- Χρήση αυτοματοποιημένων τεχνικών ελέγχου.
- Εφαρμογή λύσεων για την αντιμετώπιση βασικών τεχνολογικών κινδύνων, όπως αυτών που σχετίζονται με τον έλεγχο και τη διαχείριση των προσβάσεων χρηστών σε συστήματα και πληροφορίες (εξουσιοδοτημένη πρόσβαση, ταυτοποίηση, κλπ.).
- Αξιολόγηση των διαδικασιών ελέγχου σε εταιρικό επίπεδο και των δυνητικών κινδύνων απάτης (fraud).
- Ανάπτυξη σχεδίου επιχειρησιακής συνέχειας (business continuity plan) και επαναλειτουργίας μετά από καταστροφή (disaster recovery).

Θα πρέπει εδώ να αναφερθεί ότι η εφαρμογή μιας συνολικής πολιτικής ασφαλείας που να καλύπτει όλη τη τεχνολογική υποδομή του IT, δεν είναι απλή υπόθεση αφού προσκρούει ενίοτε στη χρήση αναποτελεσματικών εργαλείων διαχείρισης, τα οποία εστιάζουν μόνο σε επιμέρους τμήματα της ευρύτερης πολιτικής ασφαλείας. Δεδομένης της ολοένα αυξανόμενης τεχνολογικής πολυπλοκότητας και του κατακερματισμού των συστημάτων σχεδόν σε κάθε Οργανισμό, το πλαίσιο διαχείρισης IT κινδύνων απασχολεί εδώ και αρκετά χρόνια έντονα την ερευνητική κοινότητα. Η απλοποίηση της εν λόγω διαχείρισης

κινδύνων είναι πλέον ζητούμενο και για το λόγο αυτό έχει προταθεί ένα πλαίσιο ασφάλειας συστημάτων και πληροφοριών ([G04], [JA05], [SCL], [A08]), αποτελούμενο από τρία επίπεδα (layers), τα οποία θα πρέπει να συνεργάζονται αρμονικά, προκειμένου να γίνει εφικτή η αποτελεσματική διαχείριση των τεχνολογικών κινδύνων:

Σχήμα 1: Τα 3 Επίπεδα Ασφάλειας Συστημάτων και Πληροφοριών



1. Επίπεδο Επιβολής Ελέγχων (Controls Enforcement Layer). Εδώ πραγματοποιείται η ανίχνευση του επιπέδου ασφαλείας για το σύνολο της υποδομής IT. Σε ένα καλά δομημένο τεχνολογικό περιβάλλον, πολλοί επιμέρους ελεγκτικοί μηχανισμοί είναι ενσωματωμένοι σε τμήματα της υποδομής, όπως λειτουργικά συστήματα και δίκτυα και διασφαλίζουν την ύπαρξη ελέγχων ασφάλειας χωρίς να απαιτείται η εγκατάσταση και διαχείριση επιμέρους εφαρμογών για το σκοπό αυτό.
2. Επίπεδο Διαχείρισης Ελέγχων (Controls Management Layer). Από το επίπεδο αυτό οι υπεύθυνοι ασφαλείας κάθε Οργανισμού μπορούν να ορίσουν τους απαραίτητους μηχανισμούς ασφαλείας και να επιβλέψουν τη λειτουργία τους. Η δημιουργία ενός τέτοιου επιπέδου ελέγχου δίνει

συνήθως τη δυνατότητα ενοποίησης ενός μεγάλου αριθμού εφαρμογών ασφαλείας.

3. Επίπεδο Διαχείρισης Ασφαλείας (Security Management Layer). Στο επίπεδο αυτό ορίζεται η πολιτική ασφαλείας που ακολουθεί ένας Οργανισμός για το σύνολο της υποδομής IT που διαθέτει, βάσει των απαιτήσεων συμμόρφωσης (compliance) και των βέλτιστων πρακτικών του. Οι απαιτήσεις συμμόρφωσης της υποδομής IT με διαρκώς και πιο απαιτητικά standards, έχουν αυξηθεί με δραματικούς ρυθμούς την τελευταία δεκαετία ([K10]). Στο επίπεδο αυτό, συσχετίζονται τα διάφορα συστήματα και πληροφορίες, ώστε να εκτιμηθεί ο βαθμός συμμόρφωσης της υποδομής IT με την πολιτική ασφαλείας και να ληφθούν τα κατάλληλα μέτρα όπου κριθεί απαραίτητο.

Τέλος, θα πρέπει να σημειώσουμε την επικάλυψη που υπάρχει μεταξύ διαδικασιών διαχείρισης κινδύνων και εταιρικής διακυβέρνησης (corporate governance), ειδικότερα σε τομείς στρατηγικού ελέγχου όπως έχει παρατηρηθεί από τους ([LKA]), οι οποίοι μάλιστα προτείνουν και την παράλληλη δημιουργία και συνεργασία των σχετικών μεθόδων και εργαλείων/ εφαρμογών.

3. Γενική Περιγραφή – Βασικές Αρχές

Βασική επιδίωξη των προγραμμάτων διαχείρισης κινδύνων σε ένα Οργανισμό είναι ([N02]) να υποστηρίξουν τον Οργανισμό στην εκπλήρωση των επιχειρηματικών του στόχων. Αυτό πρακτικά μπορεί να επιτευχθεί

- με την καλύτερη θωράκιση των συστημάτων IT που αποθηκεύουν, επεξεργάζονται και μεταδίδουν τις πληροφορίες.
- παρέχοντας τη δυνατότητα στη Διοίκηση του Οργανισμού να λαμβάνει αποφάσεις που αφορούν τη διαχείριση κινδύνων στηριζόμενος στην ορθή πληροφόρηση και να αιτιολογεί τις σχετικές δαπάνες.
- παρέχοντας τη δυνατότητα στη Διοίκηση του Οργανισμού να αποδεικνύει την ορθή χρήση των IT συστημάτων στηριζόμενη στην πλήρη τεκμηρίωση των ελέγχων και των αποτελεσμάτων που προκύπτουν από την εφαρμογή της διαδικασίας διαχείρισης των κινδύνων.

Για την υλοποίηση προγραμμάτων διαχείρισης κινδύνων σε ένα Οργανισμό, εμπλέκονται πολλά και διαφορετικά τμήματα και προσωπικό το οποίο μπορεί να είναι έμπειρο ή άπειρο, τεχνικό ή μη τεχνικό. Ειδικότερα, οι επιμέρους ρόλοι και το προσωπικό που εμπλέκεται σε προγράμματα διαχείρισης κινδύνων παρουσιάζονται στην Ενότητα 3.2. Επίσης καθίσταται ολοένα και πιο σημαντική η χρήση λογισμικού και εφαρμογών που βοηθούν στην κατεύθυνση της αυτοματοποίησης διαδικασιών ελέγχουν και της αυτόματης αναζήτησης και εντοπισμού απειλών, ενώ προς τη κατεύθυνση αυτή συμβάλουν και ερευνητικές προσπάθειες ([G04]).

3.1. Σπουδαιότητα Διαχείρισης Κινδύνων

Αν και τα αξιόπιστα συστήματα αποτελούν πολύτιμα περιουσιακά στοιχεία για ένα Οργανισμό, η ύπαρξη τρωτών σημείων, η ελλιπής συντήρηση και η ανεπαρκής παρακολούθηση είναι πιθανό να οδηγήσουν τον Οργανισμό σε σημαντικές απώλειες εσόδων, φήμης και απόδοσης. Πόσο πιθανό είναι να συμβεί κάτι τέτοιο; Γενικά η πιθανότητα αυτή είναι ανάλογη του εύρους αλλά και του χρόνου χρήσης κάθε συστήματος ([N95]). Κατά συνέπεια, αν δε ληφθούν τα απαραίτητα μέτρα, όσο πολυπλοκότερη είναι η υποκείμενη τεχνολογία και όσο μεγαλύτερος ο χρόνος χρήσης της, τόσο πιθανότερο είναι για ένα Οργανισμό να πέσει θύμα παραβίασης και υποστεί τις συνέπειες ενός γεγονότος παραβίασης ασφάλειας. Θα πρέπει επομένως σε κάθε Οργανισμό να ληφθεί μέριμνα τόσο σε επιχειρησιακό όσο και σε τεχνικό επίπεδο ώστε να πραγματοποιείται με τρόπο αποτελεσματικό η διαχείριση των «τεχνολογικών» κινδύνων. Η σύνδεση και συσχέτιση κινδύνων με το business του Οργανισμού γίνεται ολοένα και σημαντικότερη, ενώ γίνεται εμφανέστερη σε ακραία συμβάντα, όπως για παράδειγμα η κατάρρευση των «Δίδυμων Πύργων» στις ΗΠΑ ([DR03]).

Βασικό αντικείμενο της διαδικασίας διαχείρισης IT κινδύνων είναι, όπως ήδη αναφέρθηκε, να προσδιοριστεί αν οι κίνδυνοι που αντιμετωπίζει το IT ενός Οργανισμού είναι σε ένα αποδεκτό επίπεδο ή εάν απαιτείται η εφαρμογή πρόσθετων δικλείδων ασφαλείας για την περαιτέρω μείωση ή την πλήρη εξάλειψη τους. Η Διαχείριση Κινδύνων είναι μια διαδικασία που επιτρέπει στους Οργανισμούς να «ζυγίσουν» το επιχειρησιακό και οικονομικό κόστος μέτρων προστασίας και να πάρουν αποφάσεις οι οποίες θα ενισχύσουν τη δυνατότητα εκπλήρωσης της αποστολής και των στόχων του Οργανισμού, προστατεύοντας τα IT συστήματα και τα δεδομένα.

Για να είναι εφικτή η αποτελεσματική διαχείριση των κινδύνων, θα πρέπει η ανώτατη διοίκηση να είναι σε θέση να καθορίσει τις επιθυμητές λειτουργίες ασφαλείας που πρέπει να υποστηρίζουν τα IT συστήματα, ώστε να παρέχουν το απαιτούμενο επίπεδο στήριξης για την αντιμετώπιση των δυνητικών απειλών

παραβίασης της ασφάλειας των συστημάτων και των δεδομένων του Οργανισμού ([N02], [SCL]). Δεδομένου του περιορισμένου προϋπολογισμού που συνήθως διατίθεται για την ασφάλεια των IT συστημάτων, οι όποιες δαπάνες θα πρέπει να εξετάζονται πολύ προσεκτικά και οι όποιες αποφάσεις να είναι καλά τεκμηριωμένες και εμπεριστατωμένες. Μια καλά δομημένη διαδικασία διαχείρισης κινδύνων, όταν χρησιμοποιείται αποτελεσματικά, μπορεί να βοηθήσει τη Διοίκηση να εντοπίσει τους κρίσιμους ελέγχους που πρέπει να υποστηρίζονται από το IT για να είναι εφικτή η απρόσκοπτη υποστήριξη εκπλήρωσης της αποστολής του Οργανισμού, υποβοηθώντας με τον τρόπο αυτό τη σωστή και έγκαιρη λήψη αποφάσεων στον εν λόγω τομέα.

3.2. Ρόλοι

Η διαχείριση κινδύνων αποτελεί συλλογική ευθύνη της Διοίκησης ενός Οργανισμού. Αυτή η ενότητα περιγράφει τους βασικούς ρόλους που εμπλέκονται στη διαδικασία διαχείρισης των κινδύνων ([N02]).

1. Ανώτατη Διοίκηση (Senior Management). Τα ανώτερα διοικητικά στελέχη, ως φορείς της τελικής ευθύνης για την εκπλήρωση των στόχων και της αποστολής του Οργανισμού, πρέπει να διασφαλίσουν τους απαραίτητους πόρους για την ανάπτυξη των συστημικών δυνατοτήτων που απαιτούνται για την όσο το δυνατό πληρέστερη διαχείριση των κινδύνων. Θα πρέπει επίσης να είναι σε θέση να αξιολογούν και να ενσωματώνουν τα αποτελέσματα των δραστηριοτήτων αξιολόγησης κινδύνων στη διαδικασία λήψης αποφάσεων. Για να επιτύχει τους στόχους του ένα πρόγραμμα διαχείρισης IT κινδύνων απαιτείται απαραίτητα η στήριξη και συμμετοχή των ανωτέρων στελεχών του Οργανισμού.
2. Διευθυντής Πληροφορικής (Chief Information Officer -CIO). Ο CIO είναι υπεύθυνος για το σύνολο των δραστηριοτήτων της Υπηρεσίας Πληροφορικής ενός Οργανισμού. Οι αρμοδιότητες αυτές μεταξύ άλλων

περιλαμβάνουν τον προγραμματισμό και την υλοποίηση ενεργειών σχετικών με ζητήματα ασφάλειας των συστημάτων και πληροφοριών. Οι αποφάσεις που λαμβάνονται σε αυτούς τους τομείς θα πρέπει να βασίζονται σε ένα αποτελεσματικό πρόγραμμα διαχείρισης κινδύνων.

3. «Ιδιοκτήτες» Συστημάτων και Πληροφοριών (System and Information Owners). Οι Ιδιοκτήτες Συστημάτων και Πληροφοριών είναι υπεύθυνοι για τη διασφάλιση της ύπαρξης των ενδεδειγμένων ελέγχων, ώστε να τηρούνται οι αρχές της ακεραιότητας, της εμπιστευτικότητας, και της διαθεσιμότητας των IT συστημάτων αλλά και των υποκείμενων δεδομένων. Συνήθως, οι Ιδιοκτήτες Συστημάτων και Πληροφοριών είναι υπεύθυνοι για το σχεδιασμό και την υλοποίηση αλλαγών στα συστήματα. Είναι αυτοί που πρέπει να εγκρίνουν και να υπογράψουν για παράδειγμα, επεκτάσεις συστημάτων, σημαντικές αλλαγές στο λογισμικό (software) ή το υλικό (hardware). Οι Ιδιοκτήτες Συστημάτων και Πληροφοριών πρέπει επομένως να κατανοούν τη σημαντικότητα του ρόλου τους στη διαδικασία του IT risk management και να την υποστηρίζουν ενεργά.
4. Διευθυντές Επιχειρησιακών και Λειτουργικών Μονάδων (Business and Functional Managers). Οι Διευθυντές οι οποίοι είναι υπεύθυνοι για τις επιχειρησιακές δραστηριότητες πρέπει να διαδραματίσουν ενεργό ρόλο στη διαδικασία διαχείρισης IT κινδύνων. Ο ρόλος τους είναι καίριος και ουσιώδης για την εκπλήρωση της αποστολής του Οργανισμού. Η άμεση εμπλοκή και συμμετοχή τους στη διαδικασία διαχείρισης IT κινδύνων κάνει εφικτή την εξέταση των ζητημάτων ασφάλειας από την πλευρά των επιχειρησιακών και λειτουργικών δραστηριοτήτων που κατά κανόνα υλοποιούνται από τους τελικούς χρήστες των συστημάτων.
5. Υπεύθυνοι Ασφάλειας Πληροφοριακών Συστημάτων (Information System Security Officers – ISSO). Ο Διευθυντές του προγράμματος ασφάλειας IT και οι υπεύθυνοι ασφάλειας των υπολογιστικών συστημάτων καλούνται να διαδραματίσουν ηγετικό ρόλο στην καθιέρωση της κατάλληλης και ορθά δομημένης μεθοδολογίας διαχείρισης IT κινδύνων και να βοηθήσουν στον προσδιορισμό, την αξιολόγηση και την ελαχιστοποίηση των κινδύνων των IT

συστημάτων που είναι κρίσιμα για τον Οργανισμό. Οι ISSOs επίσης κατά κανόνα λειτουργούν ως σημαντικοί σύμβουλοι υποστήριξης των ανώτερων διευθυντικών στελεχών ώστε να διασφαλιστεί ότι η διαδικασία αυτή θα διεξάγεται σε συνεχή βάση.

6. Επαγγελματίες Ασφάλειας IT (IT Security Practitioners). Οι Επαγγελματίες Ασφάλειας IT (Δικτύων, Συστημάτων, Εφαρμογών και Βάσεων Δεδομένων, Σύμβουλοι και Αναλυτές ασφάλειας) είναι υπεύθυνοι για την ορθή υλοποίηση των απαιτήσεων ασφαλείας στα συστήματα. Δεδομένων των συνεχών αλλαγών που λαμβάνουν χώρα στο υφιστάμενο περιβάλλον συστημάτων IT (π.χ. επεκτάσεις δικτύων, αλλαγές στις υπάρχουσες υποδομές, εισαγωγή νέων τεχνολογιών), οι Επαγγελματίες Ασφάλειας IT πρέπει να είναι σε θέση να υποστηρίζουν και να χρησιμοποιούν τη διαδικασία διαχείρισης κινδύνων για τον εντοπισμό και την αξιολόγηση νέων δυνητικών κινδύνων και την υλοποίηση νέων ελέγχων ασφαλείας, οι οποίοι κρίνονται απαραίτητοι για τη διασφάλιση της απρόσκοπτης λειτουργίας των συστημάτων.
7. Εκπαιδευτές σε Θέματα Ασφάλειας (Security Awareness Trainers). Η χρήση των IT συστημάτων και των δεδομένων σύμφωνα με τις πολιτικές και τις κατευθυντήριες γραμμές του Οργανισμού, καθώς επίσης και η τήρηση κανόνων συμπεριφοράς είναι ζωτικής σημασίας για τον μετριασμό των κινδύνων και την προστασία των IT πόρων του Οργανισμού. Για να ελαχιστοποιηθεί ο κίνδυνος για τα συστήματα πληροφορικής, είναι απαραίτητο οι χρήστες των συστημάτων και εφαρμογών να έχουν εκπαιδευτεί και ενημερωθεί σε θέματα ασφάλειας. Ως εκ τούτου, οι Εκπαιδευτές σε Θέματα Ασφάλειας, πρέπει να είναι σε θέση να κατανοούν τη διαδικασία διαχείρισης IT κινδύνων ώστε να μπορούν να αναπτύξουν το κατάλληλο εκπαιδευτικό υλικό και να ενσωματώσουν την αξιολόγηση των κινδύνων (risk assessment) στα εκπαιδευτικά προγράμματα.

3.3. Κύκλος Ζωής Συστημάτων και Διαχείριση Κινδύνων

Η ελαχιστοποίηση των αρνητικών επιπτώσεων σε ένα Οργανισμό από δυνητικές απειλές καθώς επίσης και η ανάγκη για αξιόπιστες διαδικασίες λήψης αποφάσεων είναι οι θεμελιώδεις αιτίες που οδηγούν τους Οργανισμούς στην υιοθέτηση και εφαρμογή διαδικασιών διαχείρισης κινδύνων για τα συστήματα πληροφορικής τους. Για να είναι αποτελεσματική, η διαδικασία διαχείρισης κινδύνων θα πρέπει να ενσωματωθεί πλήρως σε όλο το εύρος του Κύκλου Ζωής Συστημάτων (ΚΖΣ - System Life Cycle). Ο Κύκλος Ζωής ενός συστήματος IT εμπεριέχει συνοπτικά πέντε φάσεις ([A08], [C06], [N02]):

1. Έναρξη (initiation)
2. Ανάπτυξη/ Απόκτηση (development/ acquisition)
3. Υλοποίηση (implementation)
4. Λειτουργία/ Συντήρηση (operation/ maintenance)
5. Διάθεση (disposal)

Σε ορισμένες περιπτώσεις, ένα σύστημα πληροφορικής μπορεί να συμπεριλάβει αρκετές από αυτές τις φάσεις, ταυτόχρονα. Ωστόσο, η μεθοδολογία διαχείρισης κινδύνων είναι ανεξάρτητη από τη φάση του ΚΖΣ της οποίας η αξιολόγηση διεξάγεται. Η διαχείριση κινδύνων είναι μια επαναληπτική διαδικασία που μπορεί να εκτελεστεί κατά τη διάρκεια κάθε σημαντικής φάσης του ΚΖΣ. Ο Πίνακας 1 περιγράφει τα χαρακτηριστικά της κάθε φάσης ΚΖΣ και δείχνει πώς η διαδικασία διαχείρισης κινδύνων μπορεί να υλοποιηθεί ώστε να υποστηρίζει κάθε φάση.

Πίνακας 1: Διαδικασία Διαχείρισης Κινδύνων σε Σχέση με τον Κύκλο Ζωής Συστήματος

ΦΑΣΗ ΚΥΚΛΟΥ ΖΩΗΣ	**ΠΕΡΙΓΡΑΦΗ**	**ΣΥΣΧΕΤΙΣΗ ΜΕ ΤΗ ΔΙΑΔΙΚΑΣΙΑ RISK MANAGEMENT**
Έναρξη	Περιγράφονται και τεκμηριώνονται οι ανάγκες, οι στόχοι και η εμβέλεια των IT συστημάτων	Οι κίνδυνοι που εντοπίζονται χρησιμοποιούνται κατά την ανάπτυξη προδιαγραφών σε ζητήματα ασφάλειας σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο

Ανάπτυξη/ Απόκτηση	Το σύστημα σχεδιάζεται και αναπτύσσεται ή αγοράζεται και παραμετροποιείται	Οι κίνδυνοι που εντοπίζονται χρησιμοποιούνται κατά την ανάλυση ασφάλειας του IT συστήματος και λαμβάνονται υπόψη σε αποφάσεις αρχιτεκτονικής
Υλοποίηση	Τα χαρακτηριστικά ασφάλειας του συστήματος προσαρμόζονται, ενεργοποιούνται και ελέγχονται	Οι εντοπιζόμενοι κίνδυνοι λαμβάνονται υπόψη κατά την υλοποίηση ώστε η υλοποίηση του συστήματος να συμπεριλάβει τα απαραίτητα χαρακτηριστικά ασφαλείας
Λειτουργία/ Συντήρηση	Το σύστημα έχει τεθεί σε λειτουργία. Απαιτείται δυναμική συντήρηση/ προσαρμογή των επιμέρους τμημάτων και χαρακτηριστικών του	Διαδικασίες διαχείρισης κινδύνων εκτελούνται ανά τακτά χρονικά διαστήματα ή όταν συντελούνται αλλαγές ευρείας κλίμακας στο σύστημα
Διάθεση	Το σύστημα αποσύρεται και πρέπει να πραγματοποιηθούν οι σχετικές ενέργειες για τα τμήματά του και τις συσχετιζόμενες πληροφορίες	Διαδικασίες διαχείρισης κινδύνων πρέπει να εκτελεστούν για να διασφαλιστεί ότι για το υλικό, το λογισμικό και τα συσχετιζόμενα δεδομένα εκτελούνται οι ενδεδειγμένες ενέργειες με ασφαλή και συστηματικό τρόπο

Δεδομένου ότι η ανάπτυξη λογισμικού γίνεται με ολοένα και συστηματικότερο τρόπο και υποστηρίζεται από σχετικά εργαλεία, και λόγω του υπερτονισμού της χρήσης της τεχνολογίας, οι πιθανοί κίνδυνοι αυξάνονται, αλλά η βαρύτητα που δίνεται στη διαχείρισή τους δεν αυξάνεται με τον ίδιο ρυθμό ώστε να αντιμετωπιστούν αποτελεσματικά οι αυξανόμενοι IT κίνδυνοι ([SAA]). Η διαχείριση IT κινδύνων, αποτελεί πλέον υψηλής προτεραιότητας τομέα για πολλούς Οργανισμούς και τα διάφορα στάδια που αποτελούν τον κύκλο ζωής της εν λόγω δραστηριότητας (π.χ. risk assessment, risk mitigation) έχουν μελετηθεί και αναλυθεί από πολλούς ερευνητές, όπως ο ([S11]).

3.4. Προτεινόμενη Μεθοδολογία

Η προτεινόμενη στην παρούσα εργασία μεθοδολογία αποτελείται από δύο βασικά τμήματα, τον Εντοπισμό των Κινδύνων (Risk Assessment) και τον Περιορισμό των Κινδύνων (Risk Mitigation). Το γενικό πλαίσιο της προτεινόμενης μεθοδολογίας ακολουθεί την αντίστοιχη μεθοδολογία που περιγράφεται στο ([N02]) και η οποία συνθέτει πολλά διαφορετικά στοιχεία από μεθόδους που συναντώνται στην ευρύτερη περιοχή της αξιολόγησης και διαχείρισης IT κινδύνων ([LKA], [N95]). Η μεθοδολογία που προτείνουμε εξειδικεύει τα επιμέρους βήματα του εν λόγω πλαισίου και καθορίζει επαρκώς τα απαιτούμενα ποσοτικά στοιχεία (κλίμακες διαβάθμισης, ποσοτικοί δείκτες, κ.λπ.) αλλά και τους δείκτες ποιοτικής αξιολόγησης (π.χ. 5 κλίμακες διαβάθμισης των κινδύνων) και διαβάθμισης των πιθανοτήτων εμφάνισης κάποιου συμβάντος (π.χ. 5 κλίμακες διαβάθμισης των πιθανοτήτων). Μ' άλλα λόγια η προτεινόμενη στην παρούσα εργασία μεθοδολογία υιοθετεί το γενικότερο πλαίσιο της μεθοδολογίας που περιγράφεται στο ([N02]) καθορίζοντας κλίμακες, διαβαθμίσεις και άλλους ποσοτικούς ή ποιοτικούς δείκτες, ώστε να καταστήσει τη μεθοδολογία αυτή πρακτικά εφαρμόσιμη, κάτι που στη συνέχεια αποδεικνύεται και επαληθεύεται μέσα από τη μελέτη περίπτωσης (case study) που παρατίθεται στο Κεφάλαιο 7.

Ειδικότερα, στο Κεφάλαιο 4 παρουσιάζεται το πρώτο βασικό τμήμα της μεθοδολογίας, το Risk Assessment, το οποίο αποτελείται από 9 επιμέρους στάδια. Ένα από τα σημαντικότερα σημεία της προτεινόμενης μεθόδου είναι η ποσοτικοποίηση της Διαβάθμισης Κινδύνων, διαδικασία κατά την οποία ορίζονται οι κλίμακες διαβάθμισης των IT κινδύνων, όπως αυτές προκύπτουν από το συνδυασμό της πιθανότητας πραγματοποίησης μιας απειλής και της έκτασης των επιπτώσεων της απειλής αυτής. Η μεθοδολογία που προτείνεται κωδικοποιεί σε πέντε επίπεδα (Πολύ Υψηλό, Υψηλό, Μέτριο, Χαμηλό, Πολύ Χαμηλό) τόσο την πιθανότητα πραγματοποίησης μιας απειλής, όσο και τον αντίκτυπο των απειλών. Σε κάθε διαβάθμιση αντιστοιχίζεται ένα score και σε κάθε συνδυασμό το γινόμενο των επιμέρους scores. Εν συνεχεία, σε κάθε συνδυασμό αποδίδεται ένας ποιοτικός χαρακτηρισμός, ο οποίος προέρχεται και

πάλι από μια διαβάθμιση πέντε επιπέδων ανάλογα με το εύρος τιμών στο οποίο ανήκει το συνδυαστικό score.

Στο Κεφάλαιο 5 παρουσιάζεται το δεύτερο τμήμα της προτεινόμενης μεθοδολογίας, το Risk Mitigation. Η προτεινόμενη μεθοδολογία περιορισμού των κινδύνων αποτελείται από 7 Στάδια, των οποίων τελικός στόχος είναι, αξιοποιώντας τα ευρήματα της διαδικασίας εντοπισμού των κινδύνων που έχει προηγηθεί, να προτείνει και να υλοποιήσει δράσεις περιορισμού των απειλών, των κινδύνων και του αντίκτυπού τους στον Οργανισμό.

Σε ένα πρώτο επίπεδο καταγραφής, τα πλεονεκτήματα της προτεινόμενης μεθόδου είναι ότι:

1. Είναι καλά δομημένη και τυποποιημένη.
2. Έχει διακριτά και ξεκάθαρα στάδια.
3. Έχει παραδοτέα (deliverables) σε όλα τα στάδια.
4. Καθορίζει πλήρως τις αρμοδιότητες και τους ρόλους των εμπλεκόμενων.
5. Είναι κατά βάση ποιοτική, αλλά περιέχει και σημαντικά ποσοτικά στοιχεία και Key Performance Indicators (KPIs), όπως η Διαβάθμιση Κινδύνων.
6. Παρέχει τη δυνατότητα προσαρμογής των επιμέρους σταδίων, ώστε να αντανακλούν τον επιχειρησιακό προσανατολισμό (business orientation) και το βαθμό ανάληψης κινδύνων (risk appetite) κάθε Οργανισμού (π.χ. 3, 5, ή 7 επίπεδα διαβάθμισης πιθανοτήτων και επιπτώσεων, διαφορετικές αριθμητικές κλίμακες για τη διαβάθμιση των κινδύνων - π.χ. 1-100, 0-1, κλπ.).

Ως μειονεκτήματα της προτεινόμενης μεθοδολογίας θα μπορούσαμε να σημειώσουμε ότι:

1. Είναι πολύ λεπτομερής και αναλυτική και ως εκ τούτου η πλήρης υλοποίησή της μπορεί να αποδειχθεί χρονοβόρα και "ακριβή" για ένα Οργανισμό.

2. Είναι μερικώς ποσοτικοποιημένη και δίνει μεγαλύτερη έμφαση στην ποιοτική αξιολόγηση των επιμέρους παραμέτρων.

4. Εντοπισμός και Αξιολόγηση Κινδύνων (Risk Assessment)

Ο εντοπισμός και αξιολόγηση κινδύνων (risk assessment) είναι το πρώτο βήμα που ακολουθείται σε όλες σχεδόν τις μεθοδολογίες διαχείρισης κινδύνων ([N01a], [N02]). Κατά το βήμα αυτό, οι Οργανισμοί καθορίζουν το εύρος των δυνητικών απειλών για τα IT συστήματα και των κινδύνων που απορρέουν σε όλο τον Κύκλο Ζωής των συστημάτων. Το αποτέλεσμα αυτής της διαδικασίας βοηθά εν συνεχεία στον εντοπισμό κατάλληλων ελέγχων η εφαρμογή των οποίων θα οδηγήσει στη μείωση ή την εξάλειψη των κινδύνων αυτών (risk mitigation – elimination), διαδικασία η οποία αποτελεί επόμενο βήμα της προτεινόμενης μεθοδολογίας.

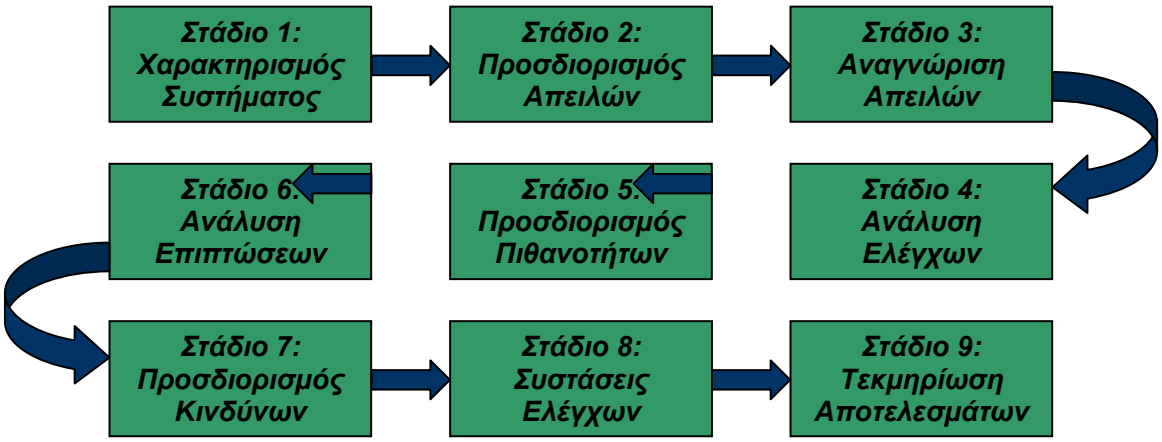
Ο κίνδυνος είναι συνάρτηση της πιθανότητας να πραγματοποιηθεί μια συγκεκριμένη απειλή, εκμεταλλευόμενη πιθανή αδυναμία του συστήματος, και των επιπτώσεων που μπορεί να έχει η απειλή αυτή στην ομαλή λειτουργία του Οργανισμού ([N02]). Για να προσδιοριστεί η πιθανότητα ενός μελλοντικού ανεπιθύμητου γεγονότος, οι απειλές για ένα IT σύστημα θα πρέπει να αναλυθούν σε συνδυασμό με τις πιθανές αδυναμίες και τους ελέγχους που είναι εν ισχύ για το εν λόγω σύστημα.

Ο όρος «επιπτώσεις», αναφέρεται στο μέγεθος της βλάβης που θα μπορούσε να προκληθεί από την πραγματοποίηση μιας απειλής. Πρακτικά αυτό σημαίνει την επίπτωση που η εν λόγω βλάβη θα είχε στην εκπλήρωση της αποστολής του Οργανισμού και το βαθμό στον οποίο θα επηρέαζε την αξία των περιουσιακών στοιχείων και των πόρων του IT που εμπλέκονται ([LC03]). Η μεθοδολογία εντοπισμού και αξιολόγησης κινδύνων, περιλαμβάνει σύμφωνα με το ([N02]) εννέα στάδια, τα οποία περιγράφονται αναλυτικά στις ενότητες που ακολουθούν. Συνοπτικά τα στάδια αυτά είναι:

1. Χαρακτηρισμός Συστήματος (System Characterization)
2. Προσδιορισμός Απειλών (Threat Identification)
3. Αναγνώριση Αδυναμιών (Vulnerability Identification)
4. Ανάλυση Ελέγχων (Control Analysis)
5. Προσδιορισμός Πιθανοτήτων (Likelihood Determination)
6. Ανάλυση Επιπτώσεων (Impact Analysis)
7. Προσδιορισμός των Κινδύνων (Risk Determination)
8. Συστάσεις Ελέγχων (Control Recommendations)
9. Τεκμηρίωση Αποτελεσμάτων (Results Documentation)

Το Σχήμα 2 απεικονίζει τα προαναφερθέντα στάδια.

Σχήμα 2: Στάδια Εντοπισμού και Αξιολόγησης Κινδύνων



Ακολούθως, περιγράφουμε τα ανωτέρω στάδια, τα οποία έχουμε κατηγοριοποιήσει και εντάξει σε τέσσερις βασικές ενότητες: **Εντοπισμός Απειλών** (Στάδια 1 και 2), **Διενέργεια Έλεγχων** (Στάδια 3 και 4), **Ανάλυση Επιπτώσεων και Προσδιορισμός Κινδύνων** (Στάδια 5, 6 και 7) και **Προτάσεις και Τεκμηρίωση** (Στάδια 8 και 9).

4.1. Εντοπισμός Απειλών

4.1.1. Στάδιο 1: Χαρακτηρισμός Συστήματος (System Characterization)

Κατά την αξιολόγηση των κινδύνων για ένα IT σύστημα, το πρώτο μας βήμα είναι να χαρακτηρίσουμε το σύστημα, δηλαδή να αποκτήσουμε σαφή εικόνα για τα όριά του, τα επιμέρους τμήματά του και τις πληροφορίες που αυτό εμπεριέχει και διαχειρίζεται. Ο χαρακτηρισμός ενός IT συστήματος καθορίζει το πεδίο εφαρμογής της προσπάθειας αξιολόγησης των κινδύνων, σκιαγραφεί τα όρια της επιχειρησιακής λειτουργίας στο συγκεκριμένο τομέα και παρέχει πληροφορίες (υλικό, λογισμικό, διασυνδεσιμότητα, και αρμόδιο τμήμα ή προσωπικό υποστήριξης) οι οποίες είναι θεμελιώδους σημασίας για τον καθορισμό του κινδύνου. Στις ενότητες που ακολουθούν περιγράφονται οι πληροφορίες συστήματος που είναι απαραίτητες κατά τη διαδικασία χαρακτηρισμού του συστήματος και προτείνονται τεχνικές συλλογής πληροφοριών που μπορούν να χρησιμοποιηθούν για τη συλλογή πληροφοριών σχετικά με το IT σύστημα. Η μεθοδολογία που περιγράφεται εδώ, μπορεί να εφαρμοστεί σε αξιολογήσεις απλών ή πολλαπλών, συσχετιζόμενων συστημάτων. Ειδικότερα για την περίπτωση πολλαπλών ή συσχετιζόμενων συστημάτων, είναι σημαντικό να υπάρχει πληροφόρηση και για όλες οι διεπαφές (interfaces) ώστε οι εξαρτήσεις να είναι με σαφήνεια και ακρίβεια προσδιορισμένα πριν από την εφαρμογή της μεθοδολογίας.

4.1.1.1. Πληροφορίες Συστήματος

Ο εντοπισμός των κινδύνων για ένα IT σύστημα προϋποθέτει τη σε βάθος κατανόηση του ευρύτερου περιβάλλοντος μέσα στο οποίο είναι τοποθετημένο και λειτουργεί το σύστημα. Αυτοί που διενεργούν την αξιολόγηση κινδύνων

πρέπει ως εκ τούτου πρώτα απ' όλα να συγκεντρώσουν πληροφορίες σχετικές με το σύστημα. Οι πληροφορίες αυτές μπορούν να συνοψιστούν στα ακόλουθα ([N95], [N01b]):

- Υλικό
- Λογισμικό
- Διεπαφές του συστήματος (εσωτερικές και εξωτερικές συνδέσεις)
- Δεδομένα και πληροφορίες
- Υπεύθυνοι υποστήριξης και χρήστες του συστήματος
- Αποστολή του συστήματος (π.χ. οι εργασίες που εκτελούνται από το σύστημα)
- Κρισιμότητα συστήματος και δεδομένων (αξία του συστήματος ή σημαντικότητά του για τον Οργανισμό)
- Ευαισθησία συστήματος και πληροφοριών. Ουσιαστικά πρόκειται για το επίπεδο προστασίας που απαιτείται για τη διατήρηση της ακεραιότητας συστήματος και δεδομένων, την εμπιστευτικότητα και τη διαθεσιμότητα.

Επιπλέον απαραίτητες είναι και πληροφορίες σχετικά με τη λειτουργικότητα του συστήματος και τα δεδομένα που περιλαμβάνει ([N01b]), όπως:

- Οι λειτουργικές απαιτήσεις (functional requirements) του συστήματος.
- Οι κατηγορίες χρηστών του συστήματος (π.χ. χρήστες που παρέχουν τεχνική υποστήριξη, χρήστες που χρησιμοποιούν το σύστημα για την εκτέλεση επιχειρηματικών λειτουργιών, κλπ.).
- Οι πολιτικές ασφάλειας συστήματος που προσδιορίζονται από την ευρύτερη πολιτική ασφάλειας του Οργανισμού, τη νομοθεσία, τις οδηγίες εποπτικών οργάνων και τις βέλτιστες πρακτικές του κλάδου στον οποίο υπάγεται ο Οργανισμός.
- Η αρχιτεκτονική ασφάλειας του συστήματος.
- Η τρέχουσα τοπολογία του δικτύου.
- Ο τρόπος προστασίας των αποθηκευμένων πληροφοριών που διασφαλίζει τη διαθεσιμότητα συστήματος και δεδομένων, την ακεραιότητα και την εμπιστευτικότητα.

- Η ροή πληροφοριών από και προς το σύστημα (διασυνδέσεις, εισόδους και έξοδοι).
- Οι υφιστάμενοι έλεγχοι που διενεργούνται από το IT σύστημα (π.χ. ενσωματωμένοι έλεγχοι, πρόσθετα προϊόντα ασφάλειας που υποστηρίζουν την ταυτοποίηση και πιστοποίηση χρηστών, τον προαιρετικό ή υποχρεωτικό έλεγχο πρόσβασης, δυνατότητες audit, μεθόδους κρυπτογράφησης).
- Οι διοικητικοί έλεγχοι (management controls) που χρησιμοποιούνται για το σύστημα (π.χ. κανόνες συμπεριφοράς).
- Οι διαχειριστικοί-λειτουργικοί έλεγχοι - διαδικασίες που χρησιμοποιούνται για το σύστημα (π.χ. εμπλεκόμενο προσωπικό ασφαλείας, διαδικασίες backup, διαδικασίες έκτακτης ανάγκης και επαναλειτουργίας μετά από σοβαρά περιστατικά, διαδικασία συντήρησης του συστήματος, διαδικασίες δημιουργίας, μεταβολής και διαγραφής χρηστών, έλεγχοι τήρησης του «διαχωρισμού καθηκόντων», κλπ.).
- Το περιβάλλον «φυσικής» και περιβαλλοντικής ασφάλειας του συστήματος (π.χ. ασφάλεια εγκαταστάσεων, πολιτικές του data center, έλεγχοι υγρασίας, νερού, ενέργειας, ρύπανσης, θερμοκρασίας, χημικών, κλπ).

Για ένα σύστημα το οποίο βρίσκεται σε φάση αρχικής λειτουργίας ή σε φάση σχεδιασμού, οι απαιτούμενες πληροφορίες για το σύστημα μπορούν να εξαχθούν από έγγραφα σχεδιασμού ή κατάρτισης προδιαγραφών. Για ένα σύστημα που είναι υπό ανάπτυξη, είναι απαραίτητο να προσδιοριστούν οι βασικοί κανόνες και τα χαρακτηριστικά ασφαλείας που θα πρέπει να καλύπτονται όταν αυτό τεθεί σε λειτουργία. Τα έγγραφα σχεδιασμού του συστήματος και το πλάνο ασφάλειας μπορούν να παράσχουν χρήσιμες πληροφορίες σχετικά με την ασφάλεια ενός υπό ανάπτυξη συστήματος.

Τέλος, για ένα σύστημα λειτουργικής υποστήριξης (operational system), τα δεδομένα που θα χρησιμοποιηθούν, συμπεριλαμβανομένων και των δεδομένων

για την παραμετροποίηση του συστήματος, πρέπει να συλλέγονται σε περιβάλλον παραγωγής. Επίσης σημαντικές πληροφορίες αποτελούν οι σχετικές με τη διασυνδεσιμότητα του συστήματος, καθώς και τεκμηριωμένες, ή μη, διαδικασίες και πρακτικές που εφαρμόζονται από τους χρήστες.

4.1.1.2. Τεχνικές Συλλογής Πληροφοριών

Οποιεσδήποτε, από τις παρακάτω τεχνικές (μεμονωμένα ή συνδυαστικά) μπορούν να χρησιμοποιηθούν για τη συγκέντρωση πληροφοριών σχετικά με IT συστήματα ([NF98]):

1. Ερωτηματολόγια. Για να συλλέξει τις σχετικές πληροφορίες, το προσωπικό που διενεργεί αξιολόγηση των κινδύνων μπορεί να αναπτύξει ερωτηματολόγια σχετικά με τους διοικητικούς και λειτουργικούς ελέγχους που έχουν σχεδιαστεί ή που χρησιμοποιούνται από το υπό εξέταση σύστημα. Τα ερωτηματολόγια αυτά πρέπει να διανεμηθούν στο κατάλληλο προσωπικό (τεχνικό και διοικητικό), το οποίο σχεδιάζει ή υποστηρίζει το σύστημα.
2. «Επί Τόπου» Συνεντεύξεις. Η διαδικασία των συνεντεύξεων με το υποστηρικτικό και διοικητικό προσωπικό του IT μπορεί να υποβοηθήσει τη διαδικασία αξιολόγησης κινδύνων μέσω της συλλογής χρήσιμων πληροφοριών σχετικά με το πληροφοριακό σύστημα (π.χ. πώς το σύστημα λειτουργεί και ποια είναι η διαδικασία διαχείρισης). Κατά τη διάρκεια επιτόπιων επισκέψεων και συνεντεύξεων θα μπορούσε επίσης να χρησιμοποιηθεί και ερωτηματολόγιο για τη διευκόλυνση και επιτάχυνση της διαδικασίας.
3. Εξέταση Εγγράφων. Έγγραφα που καθορίζουν τις εφαρμοζόμενες πολιτικές (π.χ. νομοθετικά κείμενα, επίσημες οδηγίες), έγγραφα τεκμηρίωσης του συστήματος (π.χ. εγχειρίδια χρήσης, διαχείρισης, σχεδιασμού και απαιτήσεων του συστήματος) και έγγραφα σχετικά με την ασφάλεια (π.χ. προηγούμενες εκθέσεις ελέγχου, εκθέσεις αξιολόγησης

κινδύνων, αποτελέσματα δοκιμών, πλάνα και πολιτικές ασφάλειας του συστήματος), μπορούν να χρησιμοποιηθούν για να παράσχουν σφαιρική ενημέρωση σχετικά με την ασφάλεια του IT συστήματος και τους σχετικούς ελέγχους ασφαλείας. Επιπλέον, αναφορές ανάλυσης των επιπτώσεων δυνητικών απειλών στην αποστολή του Οργανισμού ή αξιολογήσεις της κρισιμότητας των περιουσιακών στοιχείων του Οργανισμού, μπορούν επίσης να παράσχουν πληροφορίες σχετικά με την κρισιμότητα και ευαισθησία των δεδομένων και του συστήματος.

4. Χρήση Εργαλείων Αυτοματοποιημένης Αναζήτησης. Προληπτικές μέθοδοι μπορούν να χρησιμοποιηθούν για να συλλέξουν πληροφορίες συστήματος άμεσα και αποτελεσματικά. Για παράδειγμα, ένα εργαλείο «χαρτογράφησης» του δικτύου (network mapping tool) μπορεί να εντοπίσει τα προγράμματα που εκτελούνται σε μια ομάδα IT συστημάτων και να παράσχει γρήγορα ένα κατάλογο επιμέρους χαρακτηριστικών ανά IT σύστημα.

Θα πρέπει τέλος να σημειώσουμε ότι η συλλογή των πληροφοριών μπορεί να διεξαχθεί κατά τη διαδικασία αξιολόγησης κινδύνων, σε όλα τα στάδια, από το Στάδιο 1 (Χαρακτηρισμός Συστήματος) μέχρι το Στάδιο 9 (Τεκμηρίωση Αποτελεσμάτων).

Αποτέλεσμα Σταδίου 1: **Χαρακτηρισμός του υπό αξιολόγηση IT συστήματος, μια καλή εικόνα και οριοθέτηση του περιβάλλοντος του συστήματος.**

4.1.2. Στάδιο 2: Εντοπισμός Απειλών (Threat Identification)

Θα μπορούσαμε να ορίσουμε μια απειλή (threat) ως δυνητική απειλή για τον Οργανισμό, όταν υφίσταται (έστω και μικρή) πιθανότητα μια συγκεκριμένη πηγή απειλής (threat source) να εκμεταλλευτεί κάποια αδυναμία (vulnerability) του

Οργανισμού ([N02]). Η αδυναμία αυτή θα μπορούσε να είναι μια αδυναμία που μπορεί να ενεργοποιηθεί τυχαία ή σκοπίμως. Μια πηγή απειλής δε θεωρείται επικίνδυνη, όταν δεν υπάρχει πιθανότητα να προκαλέσει την εμφάνιση κάποιας αδυναμίας του Οργανισμού. Κατά τη διαδικασία καθορισμού της πιθανότητας εμφάνισης μιας απειλής, πρέπει να ληφθούν υπόψη όλες οι πηγές απειλών και όλες οι δυνητικές αδυναμίες των IT συστημάτων του Οργανισμού που θα μπορούσαν να εκμεταλλευτούν οι απειλές αυτές, καθώς επίσης και οι ήδη υφιστάμενοι έλεγχοι. Στις επόμενες ενότητες εξετάζεται λεπτομερέστερα η διαδικασία εντοπισμού των απειλών.

4.1.2.1. Εντοπισμός Πηγών Απειλής

Ο στόχος αυτού του σταδίου είναι να εντοπίσει τις πιθανές πηγές απειλών και να καταρτίσει και επεξεργαστεί μια λίστα ενδεχόμενων πηγών απειλών για το υπό αξιολόγηση IT σύστημα.

Θα μπορούσαμε να ορίσουμε την πηγή απειλής ως κάθε περίσταση ή συμβάν που είναι δυνατόν να προκαλέσει βλάβη σε ένα IT σύστημα. Οι συνηθέστερες πηγές απειλών προέρχονται από τη φύση, τον ανθρώπινο παράγοντα, ή το περιβάλλον ([ΚΓ04], [CBR], [JA05], [KPS]). Αναλυτικότερα:

- Φυσικές Απειλές: Παραδείγματα τέτοιων απειλών είναι σεισμοί, πλημμύρες, ανεμοστρόβιλοι, κατολισθήσεις και άλλα παρόμοια φυσικά φαινόμενα.
- Ανθρώπινες Απειλές: Πρόκειται για εκδηλώσεις που προκαλούνται άμεσα ή έμμεσα από τον άνθρωπο. Παραδείγματα τέτοιων απειλών είναι είτε ακούσιες πράξεις (π.χ. ακούσια εισαγωγή δεδομένων), είτε εσκεμμένες ενέργειες (δικτυακές επιθέσεις, φόρτωση κακόβουλου λογισμικού, μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες, κλπ.).

- Περιβαλλοντικές Απειλές: Ως παραδείγματα τέτοιων απειλών μπορούμε να αναφέρουμε τις παρατεταμένες διακοπές παροχής ενέργειας, τη ρύπανση, τη διαρροή χημικών ουσιών, κλπ.

Κατά την αξιολόγηση των πηγών απειλών, είναι σημαντικό όπως ήδη είπαμε να λαμβάνονται υπόψη όλες οι πιθανές πηγές απειλών που θα μπορούσαν να προκαλέσουν βλάβη σε ένα σύστημα και το ευρύτερο περιβάλλον στο οποίο λειτουργεί. Για παράδειγμα, αν η απειλή πλημμύρας δεν είναι υπαρκτή για ένα IT σύστημα που είναι τοποθετημένο στην έρημο, λόγω της εξαιρετικά χαμηλής πιθανότητας εκδήλωσης ενός τέτοιου συμβάντος, εξακολουθούν να υφίστανται περιβαλλοντικές απειλές, όπως η έκρηξη ενός αγωγού, η οποία μπορεί να πλημμυρίσει την αίθουσα υπολογιστικών συστημάτων και να προκαλέσει εκτεταμένες βλάβες.

Ο ανθρώπινος παράγοντας μπορεί επίσης όπως προαναφέρθηκε να αποτελέσει πηγή απειλής, μέσω εσκεμμένων ενεργειών, όπως εσκεμμένες επιθέσεις από κακόβουλα άτομα ή δυσαρεστημένους εργαζόμενους, ή ακόμη και ακούσιες πράξεις, όπως η αμέλεια και ανθρώπινα λάθη. Μια εσκεμμένη επίθεση μπορεί να είναι είτε:

- μια κακόβουλη προσπάθεια με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα IT σύστημα (π.χ. με την εύρεση των κωδικών πρόσβασης) με στόχο τη δημιουργία κινδύνων στην ακεραιότητα των δεδομένων, τη διαθεσιμότητα ή την εμπιστευτικότητα, ή
- μία καλοπροαίρετη, αλλά παρ' όλα αυτά σκόπιμη, προσπάθεια παράκαμψης της ασφάλειας του συστήματος. Ένα παράδειγμα τέτοιας επίθεσης είναι η περίπτωση όπου ένας προγραμματιστής γράφει ένα «δούρειο ίππο» με στόχο την παράκαμψη της ασφάλειας του συστήματος, προκειμένου να ολοκληρώσει τη δουλειά του γρηγορότερα.

4.1.2.2. Κίνητρα και Τρόπος Υλοποίησης Απειλών

Τα κίνητρα και τα μέσα που χρησιμοποιούνται για την εκτέλεση μιας επίθεσης καθιστούν τον ανθρώπινο παράγοντα, όπως ήδη αναφέραμε, δυνητικά επικίνδυνη πηγή απειλών. Ο Πίνακας 2 παρουσιάζει μια επισκόπηση των συνηθέστερων ανθρώπινων απειλών, τα πιθανά κίνητρά τους, τη μεθοδολογία και τις ενέργειες υλοποίησης των επιθέσεων αυτών. Οι πληροφορίες που παρατίθενται είναι ιδιαίτερα χρήσιμες για τους Οργανισμούς για να μελετήσουν τα δικά τους περιβάλλοντα ανθρώπινης απειλής και να τα προσαρμόσουν κατάλληλα. Επιπλέον, μια σειρά άλλων ενεργειών, οι οποίες μπορούν να βοηθήσουν ένα Οργανισμό να καταλάβει καλύτερα τις ανθρώπινες πηγές απειλών κατά τη διάρκεια συγκέντρωσης των πληροφοριών, είναι ([NG96]):

- Το ιστορικό παραβιάσεων του συστήματος
- Οι υφιστάμενες εκθέσεις παραβίασης ασφάλειας
- Οι αναφορές των περιστατικών
- Συνεντεύξεις με τους διαχειριστές συστημάτων, το προσωπικό υποστήριξης (help desk) και τους τελικούς χρήστες.

Πίνακας 2: Ανθρώπινες Απειλές

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΚΙΝΗΤΡΑ**	**ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ**
Εισβολείς (Hackers/ Crackers)	Πρόκληση, εγωισμός, αυτοεπιβεβαίωση	Επιθετική εισβολή (Hacking), Κοινωνική μηχανική (Social engineering), Παραβίαση συστήματος (System intrusion), Μη εξουσιοδοημένη πρόσβαση
Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	Απόσπαση ή/και παράνομη δημοσιοποίηση πληροφοριών, Χρηματικό όφελος, Μη εξουσιοδοτημένη αλλοίωση δεδομένων	Ηλεκτρονικό έγκλημα, Απάτη (fraud), Πλαστογράφηση πληροφορίας, Παραβίαση συστήματος
Τρομοκράτες	Εκβιασμός, Αντιπερισπασμός, Εκμετάλλευση, Εκδίκηση	Τρομοκρατικές/ βομβιστικές ενέργειες, «Πόλεμος» πληροφοριών, Επίθεση και εισχώρηση στο σύστημα
Βιομηχανική κατασκοπία (εταιρίες,	Ανταγωνιστικό πλεονέκτημα, Οικονομική κατασκοπία	Οικονομική εκμετάλλευση, Κλοπή πληροφοριών, Παραβίαση προσωπικής ιδιοκτησίας, Κοινωνική μηχανική,

κυβερνήσεις, κλπ.)		Εισβολή στο σύστημα, Μη εξουσιοδοτημένη πρόσβαση
Εχθροί «εκ των έσω» (ελλιπώς εκπαιδευμένοι, δυσαρεστημένοι, εχθρικοί, απρόσεκτοι, δόλιοι, απολυμένοι)	Περιέργεια, Εγωισμός, Ευφυΐα, Οικονομικά οφέλη, Εκδίκηση, Ακούσια λάθη και παραλήψεις	Επίθεση σε εργαζόμενο, Εκβιασμός, Αναζήτηση περιουσιακών πληροφοριών, Παράνομη χρήση συστήματος, Απάτη, Κλοπή, Πλαστογράφηση πληροφοριών, Εισαγωγή ψευδών δεδομένων, Interception, Εχθρικά προγράμματα, Πώληση προσωπικών πληροφοριών, σφάλματα (bugs) συστήματος, Εισβολή στο σύστημα, σαμποτάζ, Μη εξουσιοδοτημένη πρόσβαση

Αμέσως μετά τον εντοπισμό των πιθανών πηγών απειλών και προκειμένου ο Οργανισμός να είναι σε θέση να καθορίσει την πιθανότητα πραγματοποίησης μιας απειλής, αλλά και τον αντίκτυπό της στη λειτουργία κάθε συστήματος, θα πρέπει να λαμβάνει χώρα μια εκτίμηση των κινήτρων, των μέσων και των δυνατοτήτων που μπορεί να χρειαστούν για να έχει επιτυχή εξέλιξη μια σχεδιαζόμενη επίθεση.

Θα πρέπει επίσης να σημειώσουμε ότι η δήλωση απειλών (threat statement), ή η λίστα των πιθανών πηγών κινδύνου, θα πρέπει επίσης να προσαρμόζεται ανάλογα με τα δεδομένα του κάθε Οργανισμού (π.χ. τις συνήθειες των τελικών χρηστών), ενώ σε γενικές γραμμές, οι πληροφορίες σχετικά με τις φυσικές απειλές (π.χ. πλημμύρες, σεισμοί, κλπ.) θα πρέπει να είναι άμεσα διαθέσιμες.

Ένας αριθμός ήδη γνωστών απειλών έχουν εντοπιστεί από κάποιους Οργανισμούς. Σε αυτές στηρίζονται τα εργαλεία ανίχνευσης, τα οποία γίνονται όλο και περισσότερο δημοφιλή. Οι Οργανισμοί που τα χρησιμοποιούν, συλλέγουν και τροφοδοτούν στα συστήματα αυτά συνεχώς νέα δεδομένα σχετικά με συμβάντα ασφάλειας από διάφορες πηγές πληροφόρησης, βελτιώνοντας έτσι τη δυνατότητα να εκτιμήσουν ρεαλιστικά τις απειλές. Πηγές τέτοιας πληροφόρησης περιλαμβάνουν, αλλά δεν περιορίζονται στις εξής:

- Υπηρεσίες πληροφοριών

- Μέσα μαζικής ενημέρωσης. Ειδικότερα, τα διαδικτυακά μέσα, είναι ιδιαίτερα δημοφιλή ([I1], [I2], [I3] και [I4]).

Αποτέλεσμα Σταδίου 2. **Μια αναφορά απειλών (threat statement), η οποία περιέχει ένα κατάλογο των πηγών κινδύνου, που θα μπορούσαν να εκμεταλλευτούν αδυναμίες του συστήματος.**

4.2. Διενέργεια Ελέγχων

4.2.1. Στάδιο 3: Εντοπισμός Αδυναμιών (Vulnerability Identification)

Ευπάθεια (vulnerability) ενός συστήματος είναι ένα ελάττωμα ή αδυναμία στις διαδικασίες ασφάλειας του συστήματος, το σχεδιασμό ή την υλοποίησή του, ή ακόμη και στους ελέγχους που υποστηρίζει, το οποίο θα μπορούσε να το εκμεταλλευτεί κάποιος (ακούσια ή εκούσια) και να επιτύχει μικρής ή μεγαλύτερης κλίμακας παραβίαση της ασφάλειας του συστήματος ([C06], [N02]). Ως εκ τούτου, η ευπάθεια αναφέρεται συχνά στην παρούσα εργασία και ως αδυναμία ή τρωτό σημείο. Γίνεται επομένως κατανοητό, γιατί η ανάλυση των απειλών για ένα IT σύστημα θα πρέπει οπωσδήποτε να συσχετίζεται και με μια ανάλυση των τρωτών σημείων του.

Ο στόχος αυτού του σταδίου είναι να αναπτύξει μια λίστα των τρωτών σημείων του συστήματος που θα μπορούσαν να αξιοποιηθούν από τις πιθανές πηγές απειλών. Ο Πίνακας 3 παρουσιάζει παραδείγματα ζευγών αδυναμιών / απειλών.

Τρεις μέθοδοι συναντώνται ευρύτατα στη βιβλιογραφία ([A08], [B01], [C06]) για τον προσδιορισμό των τρωτών σημείων των IT συστημάτων και είναι:

- η χρήση των πηγών ευπάθειας
- ο έλεγχος των επιδόσεων κατά τη διάρκεια δοκιμών ασφαλείας,
- η δημιουργία ενός καταλόγου (checklist) ελέγχου απαιτήσεων ασφαλείας.

Πίνακας 3: Συσχέτιση Απειλών - Αδυναμιών

ΑΔΥΝΑΜΙΑ	**ΠΗΓΗ ΑΠΕΙΛΗΣ**	**ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ**
Οι προσβάσεις απολυμένων εργαζόμενων δεν αφαιρούνται από το σύστημα	Απολυμένοι εργαζόμενοι	Είσοδος στο δίκτυο του Οργανισμού και απόκτηση κρίσιμων εταιρικών στοιχείων
Το τείχος προστασίας (firewall) και το σύστημα του Οργανισμού επιτρέπει πρόσβαση σε μη μόνιμους χρήστες (guests)	Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), απολυμένοι εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Χρήση της πρόσβασης μη μόνιμων χρηστών
Κενά ασφάλειας στο σύστημα που έχουν εντοπιστεί αλλά δεν έχουν ακόμη επιλυθεί από τους προμηθευτές συστημάτων	Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα σημεία (αδυναμίες) που το σύστημα είναι ευπαθές
Έλλειψη εξοπλισμού προστασίας από νερό του συστήματος πυρόσβεσης	Πυρκαγιά, Αμέλεια προσωπικού	Ενεργοποίηση του συστήματος πυρόσβεσης

Τα είδη των τρωτών σημείων που πρέπει να εξεταστούν αλλά και η μεθοδολογία που απαιτείται για να καθοριστεί αν υφίστανται τρωτά σημεία, συνήθως διαφοροποιείται ανάλογα με τη φύση του IT συστήματος και τη φάση του κύκλου ζωής (ΚΖΣ) στην οποία το σύστημα βρίσκεται. Ειδικότερα:

- Αν το πληροφοριακό σύστημα δεν έχει ακόμη σχεδιαστεί, η αναζήτηση σημείων αδυναμίας πρέπει να βασιστεί κυρίως στις πολιτικές ασφάλειας του Οργανισμού, τις διαδικασίες ασφαλείας που έχουν σχεδιαστεί, τους ορισμούς και απαιτήσεις του συστήματος, καθώς και σε αναλύσεις ασφάλειας που προέρχονται από τους κατασκευαστές του λογισμικού.
- Αν το IT σύστημα είναι υπό υλοποίηση, ο προσδιορισμός των σημείων αδυναμίας πρέπει να διευρυνθεί ώστε να συμπεριλάβει πιο εξειδικευμένες πληροφορίες, όπως τα χαρακτηριστικά ασφαλείας που περιγράφονται στα έγγραφα τεκμηρίωσης και τα αποτελέσματα δοκιμών πιστοποίησης και αξιολόγησης του συστήματος.
- Αν το IT σύστημα είναι σε λειτουργία, η διαδικασία προσδιορισμού των σημείων αδυναμίας πρέπει οπωσδήποτε να συμπεριλάβει ανάλυση των χαρακτηριστικών ασφαλείας του συστήματος καθώς επίσης και των υφιστάμενων ελέγχων ασφαλείας (τεχνικών και διαδικαστικών) που χρησιμοποιούνται για την προστασία του συστήματος.

4.2.1.1. Πηγές Αδυναμίας

Τα τρωτά σημεία ενός IT υπολογιστικού περιβάλλοντος μπορούν να εντοπιστούν μέσω των τεχνικών συλλογής πληροφοριών που έχουν περιγραφεί στην Ενότητα 4.1.1.2. Μια ανασκόπηση των πηγών ευπάθειας, άλλων Οργανισμών αντίστοιχης επιχειρηματικής δραστηριότητας, είναι ιδιαίτερα χρήσιμη για την προετοιμασία των συνεντεύξεων και την ανάπτυξη αποτελεσματικών ερωτηματολογίων που θα χρησιμοποιηθούν για τον προσδιορισμό των τρωτών σημείων συγκεκριμένων IT συστημάτων. Το διαδίκτυο, είναι μια άλλη πηγή πληροφόρησης για τα γνωστά τρωτά σημεία συστημάτων που έχουν δημοσιευτεί από τους κατασκευαστές λογισμικού, μαζί με τα προγράμματα διόρθωσης (service packs, patches, fixes) και άλλα διορθωτικά μέτρα που μπορούν να εφαρμοστούν για να εξαλείψουν ή να μειώσουν τα τρωτά σημεία. Τεκμηριωμένες πηγές ευπάθειας που πρέπει να

ληφθούν υπόψη σε μια διεξοδική ανάλυση ευπάθειας περιλαμβάνουν, τα ακόλουθα:

- Προηγούμενη τεκμηρίωση διαδικασίας αξιολόγησης κινδύνων ενός IT συστήματος.
- Εκθέσεις ελέγχου (audits) του συστήματος, εκθέσεις μη ομαλής λειτουργίας, εκθέσεις ανασκόπησης της ασφάλειας, και εκθέσεις δοκιμών και αξιολόγησης του συστήματος.
- Λίστες ευπάθειας που περιέχονται σε βάσεις δεδομένων, όπως η NIST I-CAT ([I5]).
- Συμβουλές προμηθευτών λογισμικού.
- Υπηρεσίες υποστήριξης περιστατικών παραβιάσεων IT συστημάτων, ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης και λίστες ειδικών σε σχετικές ιστοσελίδες (π.χ. [I1]).
- Αναλύσεις ασφάλειας συστήματος από εξειδικευμένο λογισμικό.

4.2.1.2. Έλεγχος με Δοκιμές Ασφάλειας

Προληπτικές μέθοδοι, οι οποίες αξιοποιούν μηχανισμούς δοκιμών συστήματος, μπορούν να χρησιμοποιηθούν για να εντοπίσουν τα τρωτά του σημεία αποτελεσματικά, ανάλογα βέβαια με την κρισιμότητα του εκάστοτε υπό εξέταση συστήματος και των διαθέσιμων πόρων (π.χ. ποσά που έχουν δεσμευτεί, διαθέσιμη τεχνολογία, άτομα με τεχνογνωσία στη διεξαγωγή ελέγχων, κλπ.), αφού είναι προφανές ότι η προσέγγιση αυτή συνεπάγεται αυξημένο κόστος. Συνοπτικά, οι μέθοδοι δοκιμών ασφαλείας περιλαμβάνουν:

1. <u>Εργαλεία αυτοματοποιημένης αναζήτησης αδυναμιών:</u> Τα εργαλεία αυτοματοποιημένης αναζήτησης τρωτών σημείων ([A08], [CBR], [JA05]) χρησιμοποιούνται για να «σαρώσουν» μια ομάδα συστημάτων ή δικτύων για τον εντοπισμό γνωστών αδυναμιών (π.χ. το σύστημα επιτρέπει την ανώνυμη μεταφορά αρχείων – anonymous ftp). Ωστόσο, θα πρέπει να σημειωθεί ότι ορισμένες από τις αδυναμίες που εντοπίζονται από τα

αυτοματοποιημένα εργαλεία αναζήτησης είναι πιθανό να μην αποτελούν πραγματικά τρωτά σημεία του συστήματος στο συγκεκριμένο περιβάλλον λειτουργίας του. Αυτό συμβαίνει γιατί ορισμένα από τα εργαλεία αναζήτησης αδυναμιών, «σκοράρουν» τις δυνητικές αδυναμίες χωρίς να εξετάζουν το συγκεκριμένο περιβάλλον και τις απαιτήσεις του Οργανισμού. Έτσι, η μέθοδος αυτή μπορεί κάποιες φορές να παράξει παραπλανητικά αποτελέσματα.

2. Δοκιμές ασφάλειας που εφαρμόζονται απευθείας στο σύστημα. Η μέθοδος αυτή περιλαμβάνει ([ΚΓ04], [Α08]) την ανάπτυξη και εκτέλεση του πλάνου ελέγχων (π.χ. σενάρια και διαδικασίες δοκιμών και τα αναμενόμενα αποτελέσματα). Ο σκοπός των δοκιμών ασφαλείας του συστήματος είναι να δοκιμαστεί η αποτελεσματικότητα των ελέγχων ασφαλείας του, όπως αυτά εφαρμόζονται στο επιχειρησιακό περιβάλλον. Ο στόχος είναι να διασφαλιστεί ότι οι εφαρμοζόμενοι έλεγχοι πληρούν τις εγκεκριμένες προδιαγραφές ασφαλείας για το λογισμικό και το υλικό και εν γένει υλοποιούν την πολιτική ασφάλειας του οργανισμού και πληρούν τα πρότυπα του συγκεκριμένου επιχειρηματικού κλάδου.
3. Έλεγχοι διείσδυσης (penetration testing). Η μεθοδολογία διεξαγωγής ελέγχων διείσδυσης περιγράφεται στο ([N01a]). Οι Έλεγχοι Διείσδυσης μπορεί να χρησιμοποιηθούν για να συμπληρώσουν τους ελέγχους ασφάλειας και να διασφαλίσουν ότι όλα τα επιμέρους τμήματα ενός ΙΤ συστήματος είναι ασφαλή. Όταν οι έλεγχοι διείσδυσης ενσωματώνονται στη διαδικασία αξιολόγησης κινδύνων, μπορεί να χρησιμοποιηθούν για να εκτιμήσουν την ικανότητα ενός συστήματος να αντέξει σε εκούσιες προσπάθειες παράκαμψης της ασφάλειάς του. Ο στόχος τους είναι να δοκιμαστεί το σύστημα από την οπτική γωνία μιας πηγής απειλής και να εντοπισθούν πιθανές αστοχίες στους μηχανισμούς προστασίας του συστήματος.

Τα αποτελέσματα των τύπων του προαιρετικού ελέγχου ασφαλείας που αναφέρθηκαν παραπάνω, συμβάλλουν στον προσδιορισμό των τρωτών σημείων ενός συστήματος.

4.2.1.3. Δημιουργία Καταλόγου Ελέγχου Απαιτήσεων Ασφάλειας

Σε αυτό το βήμα, το προσωπικό που συμμετέχει στην αξιολόγηση των κινδύνων, καθορίζει εάν οι απαιτήσεις ασφάλειας που προβλέπονται για το IT σύστημα και συγκεντρώθηκαν κατά το 1^{ο} Στάδιο της διαδικασίας (Χαρακτηρισμός του Συστήματος), καλύπτονται από τους υφιστάμενους ή τους προβλεπόμενους ελέγχους ασφαλείας. Συνήθως, οι απαιτήσεις ασφάλειας του συστήματος παρουσιάζονται σε μορφή πίνακα, με κάθε απαίτηση να συνοδεύεται από μια επεξήγηση του τρόπου με τον οποίο το σύστημα ικανοποιεί τη συγκεκριμένη απαίτηση ελέγχου ασφαλείας.

Μια λίστα απαιτήσεων ελέγχων ασφαλείας περιέχει τους βασικούς κανόνες ασφάλειας που μπορούν να χρησιμοποιηθούν για τη συστηματική αξιολόγηση και τον εντοπισμό των τρωτών σημείων των εμπλεκόμενων, όπως είναι το προσωπικό, το υλικό, το λογισμικό, τα δεδομένα, οι μη αυτοματοποιημένες διαδικασίες και διεργασίες και η μεταφορά πληροφοριών.

Ο Πίνακας 4 περιέχει μια λίστα από προτεινόμενα κριτήρια ασφάλειας για να χρησιμοποιηθούν για τον εντοπισμό των τρωτών σημείων ενός IT συστήματος σε κάθε περιοχή ασφάλειας (διοικητική, λειτουργική, τεχνική).

Πίνακας 4: Προτεινόμενα Κριτήρια Ασφάλειας

ΠΕΡΙΟΧΗ ΑΣΦΑΛΕΙΑΣ	**ΚΡΙΤΗΡΙΑ ΑΣΦΑΛΕΙΑΣ**
Διοικητική	Ανάθεση αρμοδιοτήτων, Συνεχής υποστήριξη, Ικανότητα αντίδρασης σε συμβάντα, Περιοδική επαναξιολόγηση μηχανισμών ασφάλειας, Διασφάλιση ακεραιότητας προσωπικού, Αξιολόγηση κινδύνων (Risk assessment), Εκπαίδευση σε θέματα ασφάλειας, Διαχωρισμός καθηκόντων, Εξουσιοδοτημένη πρόσβαση, Πλάνο ασφάλειας συστήματος
Λειτουργική	Έλεγχος περιβάλλοντος (υγρασία, θερμοκρασία, καπνός, σκόνη, χημικά), ορθής ηλεκτροδότησης, τρόπου διατήρησης περιφερειακών συσκευών και διακίνησης των δεδομένων, Προστασία εγκαταστάσεων
Τεχνική	Τρόπος δικτυακής διασύνδεσης και επικοινωνίας, Τεχνικές κρυπτογράφησης, έλεγχος πρόσβασης, ταυτοποίηση και εξουσιοδότηση, Ανίχνευση εισβολών, Έλεγχος συστήματος (System audit)

Το αποτέλεσμα αυτής της διαδικασίας είναι όπως είπαμε ένας κατάλογος απαιτήσεων ασφαλείας. Πηγές που μπορούν να χρησιμοποιηθούν για την κατάρτιση ενός τέτοιου καταλόγου περιλαμβάνουν:

- Νομοθετικές διατάξεις και οδηγίες περί ιδιωτικότητας και προσωπικών δεδομένων.
- Σχέδιο ασφάλειας του υπό εκτίμηση IT συστήματος.
- Πολιτικές, κατευθυντήριες γραμμές και πρότυπα ασφάλειας του Οργανισμού.
- Οι πρακτικές του αντίστοιχου ευρύτερου επιχειρησιακού κλάδου.

Τα αποτελέσματα του καταλόγου ελέγχων μπορεί να χρησιμοποιηθούν ως πρώτη ύλη για την αξιολόγηση της ασφάλειας. Η διαδικασία αυτή εντοπίζει συστημικές, και διαδικαστικές αδυναμίες που μπορεί να οδηγήσουν σε προβλήματα. Δεδομένου ότι η έκθεση αξιολόγησης κινδύνων δεν αποτελεί έκθεση ελέγχου (audit report), θα πρέπει εδώ να σημειώσουμε πολλές φορές η διαδικασία εντοπισμού των τρωτών σημείων, χαρακτηρίζεται ως διαδικασία «παρατήρησης» και όχι ως διαδικασία «διαπίστωσης».

Τέλος, ο κατάλογος απαιτήσεων ασφάλειας μπορεί να χρησιμοποιηθεί για να επικυρώσει τη συμμόρφωση του Οργανισμού με τις απαιτήσεις ασφάλειας. Είναι επομένως ουσιώδες για λόγους διασφάλισης της εγκυρότητας του καταλόγου, να επικαιροποιείται σε τακτική βάση ώστε να αντικατοπτρίζει με όσο το δυνατό μεγαλύτερη ακρίβεια τις αλλαγές που συντελούνται στο περιβάλλον ελέγχων ενός Οργανισμού (π.χ. αλλαγές στις πολιτικές, τις μεθόδους και τις απαιτήσεις ασφάλειας).

Αποτέλεσμα Σταδίου 3. **Μια λίστα με τα τρωτά σημεία του συστήματος τα οποία θα μπορούσαν να εκμεταλλευτούν οι πιθανές πηγές κινδύνου.**

4.2.2. Στάδιο 4: Ανάλυση Ελέγχων (Control Analysis)

Ο βασικός στόχος αυτού του σταδίου είναι να αναλύσει τους ελέγχους που έχουν υλοποιηθεί, ή σχεδιάζονται, από τον Οργανισμό για να ελαχιστοποιήσει ή να εξαλείψει την πιθανότητα κάποια απειλή να πλήξει τα τρωτά σημεία του συστήματος. Για να γίνει εφικτή μια συνολική κατάταξη / διαβάθμιση των πιθανοτήτων ότι μια πηγή απειλής θα πλήξει το υπό εξέταση υπολογιστικό περιβάλλον / σύστημα, πρέπει να ληφθεί υπόψη ο τρόπος υλοποίησης των υφιστάμενων ή προβλεπόμενων ελέγχων. Για παράδειγμα, μια συστημική ή διαδικαστική αδυναμία δεν είναι ιδιαίτερα πιθανό να πραγματοποιηθεί, αν η πηγή απειλής μπορεί να ασκήσει μόνο χαμηλά επίπεδα επιρροής ή εάν υπάρχουν αποτελεσματικοί έλεγχοι ασφαλείας που μπορούν να εξαλείψουν ή να μειώσουν το μέγεθος της πιθανής βλάβης. Η ανάλυση των ελέγχων εξετάζεται λεπτομερέστερα στις ενότητες που ακολουθούν.

4.2.2.1. Μεθοδολογία Ελέγχων

Οι έλεγχοι ασφαλείας περιλαμβάνουν τη χρήση τεχνικών αλλά και μη τεχνικών μεθόδων. Οι τεχνικοί έλεγχοι ([N95]) κατά κανόνα ενσωματώνονται στο υλικό, ή το λογισμικό του συστήματος (π.χ. μηχανισμοί ελέγχου πρόσβασης, αναγνώρισης και πιστοποίησης χρηστών, κρυπτογράφησης και ανίχνευσης λογισμικού διείσδυσης). Οι μη τεχνικοί έλεγχοι ([SCL]) είναι διοικητικοί, διαχειριστικοί και λειτουργικοί έλεγχοι, όπως ευρύτερες πολιτικές ασφάλειας του Οργανισμού, επιχειρησιακές διαδικασίες, θέματα προσωπικού, φυσική και περιβαλλοντική ασφάλεια, κλπ.

4.2.2.2. Κατηγορίες Ελέγχων

Οι κατηγορίες ελέγχων είναι οι τεχνικοί και οι μη τεχνικοί έλεγχοι και μπορεί να ταξινομηθούν περαιτέρω ως αποτρεπτικοί ή ανιχνευτικοί. Αυτές οι δύο υποκατηγορίες θα μπορούσαν αναλυτικότερα να περιγραφούν ως εξής ([N02]):

- Οι αποτρεπτικοί έλεγχοι αναστέλλουν προληπτικά απόπειρες παραβίασης της πολιτικής ασφάλειας. Περιλαμβάνουν ελέγχους πρόσβασης, κρυπτογράφησης και ελέγχου ταυτότητας.
- Οι ανιχνευτικοί έλεγχοι προειδοποιούν για παραβιάσεις ή απόπειρες παραβιάσεων της πολιτικής ασφάλειας. Περιλαμβάνει ελέγχους όπως εντοπισμός ίχνους (audit trail) και μεθόδους ανίχνευσης εισβολής.

Η εφαρμογή αυτών των ελέγχων πραγματοποιείται κατά τη διάρκεια της διαδικασίας μείωσης ή εξάλειψης κινδύνων (risk mitigation, βλ. Ενότητα 5) και είναι το άμεσο αποτέλεσμα της αναγνώρισης των αδυναμιών των υφιστάμενων ελέγχων κατά τη διάρκεια της διαδικασίας εκτίμησης κινδύνων (δηλ. δεν υφίστανται επαρκείς έλεγχοι ή οι έλεγχοι δεν εφαρμόζονται σωστά).

Αποτέλεσμα Σταδίου 4. **Μια λίστα των υφιστάμενων ελέγχων που χρησιμοποιούνται από ένα IT σύστημα, με στόχο την ελαχιστοποίηση των πιθανοτήτων πραγματοποίησης μιας απειλής και τη μείωση των επιπτώσεων ενός τέτοιου δυσμενούς γεγονότος.**

4.3. Ανάλυση Επιπτώσεων και Προσδιορισμός Κινδύνων

4.3.1. Στάδιο 5: Καθορισμός Πιθανοτήτων (Likelihood Determination)

Για να καταλήξουμε σε μια συνολική εκτίμηση της πιθανότητας υλοποίησης μιας απειλής, θα πρέπει να λάβουμε υπόψη τους ακόλουθους παράγοντες ([NG96], [NF98]):

- Τα κίνητρα και τις δυνατότητες της πηγής απειλής.
- Τη φύση (το είδος) της αδυναμίας, του τρωτού σημείου του συστήματος.
- Την ύπαρξη και την αποτελεσματικότητα των υφιστάμενων ελέγχων.

Η πιθανότητα ότι μια πηγή απειλής θα «χτυπήσει» κάποιο τρωτό σημείο του συστήματος, μπορεί να χαρακτηριστεί ως πολύ υψηλή, υψηλή, μεσαία, χαμηλή ή πολύ χαμηλή. Ο Πίνακας 5 περιγράφει αυτά τα πέντε επίπεδα πιθανοτήτων.

Πίνακας 5: Διαβάθμιση Πιθανοτήτων Πραγματοποίησης Απειλών

ΔΙΑΒΑΘΜΙΣΗ ΠΙΘΑΝΟΤΗΤΑΣ	**ΟΡΙΣΜΟΣ ΠΙΘΑΝΟΤΗΤΑΣ**
Πολύ Υψηλή	Η πηγή απειλής έχει πολύ ισχυρό κίνητρο και πολύ μεγάλες ικανότητες και οι υφιστάμενοι έλεγχοι συστήματος είναι εμφανώς ανεπαρκείς
Υψηλή	Η πηγή απειλής έχει ισχυρό κίνητρο και μεγάλες ικανότητες και οι υφιστάμενοι έλεγχοι συστήματος είναι ανεπαρκείς
Μέτρια	Η πηγή απειλής έχει κίνητρο και επαρκείς ικανότητες αλλά οι υφιστάμενοι έλεγχοι συστήματος λειτουργούν αποτρεπτικά
Χαμηλή	Η πηγή απειλής στερείται κινήτρου και ικανοτήτων, ή οι υφιστάμενοι έλεγχοι συστήματος είναι επαρκείς για να αποτρέψουν δυνητικές επιθέσεις
Πολύ Χαμηλή	Η πηγή απειλής στερείται σε μεγάλο βαθμό κινήτρου και ικανοτήτων, ή οι υφιστάμενοι έλεγχοι συστήματος είναι σε σημαντικό βαθμό επαρκείς για να

	αποτρέψουν δυνητικές επιθέσεις

Αποτέλεσμα Σταδίου 5. **Χαρακτηρισμός Πιθανότητας *(Πολύ Υψηλή, Υψηλή, Μέτρια, Χαμηλή, Πολύ Χαμηλή)***

4.3.2. Στάδιο 6: Ανάλυση Επιπτώσεων (Impact Analysis)

Το επόμενο σημαντικό στάδιο για τη μέτρηση του ύψους του κινδύνου είναι να προσδιοριστούν οι δυσμενείς επιπτώσεις που προκύπτουν από μια «επιτυχημένη» υλοποίηση απειλής. Πριν ξεκινήσουμε την ανάλυση των επιπτώσεων, είναι απαραίτητο, να διερευνήσουμε και να ενημερωθούμε σχετικά με ακόλουθα ([N01b], [N02]):

- την αποστολή του συστήματος (π.χ. τις διαδικασίες που εκτελούνται από το σύστημα),
- την κρισιμότητα του συστήματος και των δεδομένων (π.χ. το κόστος του συστήματος ή σημασία του για τον Οργανισμό),
- την ευαισθησία του συστήματος και των δεδομένων.

Οι πληροφορίες αυτές μπορεί να αντληθούν από υφιστάμενα έγγραφα τεκμηρίωσης του Οργανισμού όπως, εκθέσεις ανάλυσης επιπτώσεων στην εκπλήρωση της αποστολής του Οργανισμού, ή εκθέσεις εκτίμησης κρισιμότητας των περιουσιακών στοιχείων του Οργανισμού. Μια ανάλυση του αντίκτυπου στην εκπλήρωση της αποστολής του Οργανισμού (γνωστή και ως ανάλυση επιχειρηματικών επιπτώσεων), κατηγοριοποιεί τις επιπτώσεις που σχετίζονται με τα «πληροφοριακά» περιουσιακά στοιχεία ενός Οργανισμού βάσει μιας ποιοτικής ή ποσοτικής αξιολόγησης της ευαισθησίας και της κρισιμότητας των εν λόγω περιουσιακών στοιχείων. Μια εκτίμηση της κρισιμότητας των στοιχείων αυτών προσδιορίζει και προτεραιοποιεί τα ευαίσθητα και κρίσιμα περιουσιακά στοιχεία του Οργανισμού (π.χ. υλικό, λογισμικό, συστήματα, υπηρεσίες, και

συναφή τεχνολογικά περιουσιακά στοιχεία) που υποστηρίζουν κρίσιμα τμήματα της αποστολής του.

Αν δεν υπάρχει σχετικό υλικό τεκμηρίωσης ή δεν έχουν διεξαχθεί εκτιμήσεις (assessments) για τα IT περιουσιακά στοιχεία του Οργανισμού, η ευαισθησία του συστήματος και των δεδομένων μπορεί να προσδιοριστεί με βάση το επίπεδο προστασίας / ασφάλειας που απαιτείται για να επιτυγχάνεται η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα των δεδομένων και του συστήματος.

Ανεξάρτητα από τη μέθοδο που χρησιμοποιείται για τον προσδιορισμό του βαθμού ευαισθησίας ενός IT συστήματος και των δεδομένων του, οι «ιδιοκτήτες» του συστήματος και των πληροφοριών είναι αυτοί που φέρουν την ευθύνη για τη διαβάθμιση των επιπτώσεων σε επίπεδα, ξεχωριστά για κάθε σύστημα και τα δεδομένα του. Κατά συνέπεια, στην ανάλυση του αντίκτυπου, η καταλληλότερη προσέγγιση είναι να πάρουμε συνέντευξη από αυτούς.

Η αρνητική επίδραση ενός συμβάντος ασφάλειας μπορεί να περιγραφεί από την άποψη της απώλειας ή υποβάθμισης οποιουδήποτε συνδυασμού των ακόλουθων στόχων ασφάλειας: *ακεραιότητα*, *διαθεσιμότητα* και *εμπιστευτικότητα* ([SCL], [N02]). Παρακάτω παρουσιάζεται μια σύντομη περιγραφή καθενός από τους στόχους αυτούς και των επιπτώσεων αν ο εν λόγω στόχος δεν επιτυγχάνεται:

1. Απώλεια Ακεραιότητας. Η ακεραιότητα του συστήματος και των δεδομένων του αναφέρεται στην απαίτηση ότι οι πληροφορίες πρέπει να προστατεύονται από «καταχρηστική» τροποποίηση. Η ακεραιότητα χάνεται όταν μη εξουσιοδοτημένες αλλαγές γίνουν στα δεδομένα ή το ίδιο το σύστημα, από εκούσιες ή ακούσιες πράξεις. Εάν η απώλεια της ακεραιότητας συστήματος ή των δεδομένων δε διορθωθεί, τότε περαιτέρω χρήση του «μη ακέραιου» συστήματος ή των αλλοιωμένων δεδομένων θα μπορούσε να οδηγήσει σε ανακρίβειες, λανθασμένες αποφάσεις, ακόμη και σε απάτη. Επίσης, η παραβίαση της ακεραιότητας

μπορεί να αποτελεί το πρώτο βήμα σε μια επιτυχημένη επίθεση εναντίον της διαθεσιμότητας ή της εμπιστευτικότητας του συστήματος. Για όλους αυτούς τους λόγους, η απώλεια της ακεραιότητας μειώνει σημαντικά την ασφάλεια ενός IT συστήματος.

2. Απώλεια Διαθεσιμότητας. Αν ένα κρίσιμο για την αποστολή του Οργανισμού IT σύστημα σταματήσει να είναι διαθέσιμο στους τελικούς του χρήστες, η αποστολή του Οργανισμού μπορεί να επηρεαστεί δυσμενώς. Απώλεια της ορθής λειτουργίας και της επιχειρησιακής αποτελεσματικότητας ενός συστήματος, μπορεί να οδηγήσει σε απώλεια παραγωγικού χρόνου, μειώνοντας κατ' αυτόν τον τρόπο την παραγωγικότητα των τελικών χρηστών και τη συμβολή τους στην υποστήριξη της αποστολής του Οργανισμού.
3. Απώλεια Εμπιστευτικότητας. Η εμπιστευτικότητα του συστήματος και των δεδομένων του αναφέρεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη δημοσιοποίησή τους. Ο αντίκτυπος της παράνομης αποκάλυψης εμπιστευτικών πληροφοριών μπορεί να κυμαίνεται από ατομικό επίπεδο (π.χ. αποκάλυψη προσωπικών δεδομένων), μέχρι πολύ ευρύ και συλλογικό επίπεδο (π.χ. αποκάλυψη στοιχείων που θέτουν σε κίνδυνο την εθνική ασφάλεια). Αυθαίρετες, μη εξουσιοδοτημένες αποκαλύψεις, ακόμη και ακούσιες, θα μπορούσαν να οδηγήσουν σε απώλεια της εμπιστοσύνης του κοινού, ή ακόμη και σε νομική δράση κατά του Οργανισμού.

Ορισμένες από τις συνέπειες των παραπάνω προβληματικών καταστάσεων μπορούν να ποσοτικοποιηθούν με τη χρήση μετρήσιμων μεγεθών, όπως είναι η απώλεια εσόδων, ή το κόστος επισκευής του συστήματος. Άλλες επιπτώσεις (π.χ. απώλεια της εμπιστοσύνης του κοινού, απώλεια αξιοπιστίας) δεν μπορούν να μετρηθούν σε συγκεκριμένες μονάδες, αλλά μπορούν να ταξινομηθούν ανάλογα με τον αντίκτυπο σε πολύ υψηλής, υψηλής, μέτριας, χαμηλής και πολύ χαμηλής επίπτωσης. Μία τέτοια ποιοτική κατηγοριοποίηση απεικονίζεται στον Πίνακα 6.

Πίνακας 6: Διαβάθμιση Αντίκτυπου

ΔΙΑΒΑΘΜΙΣΗ ΑΝΤΙΚΤΥΠΟΥ	**ΟΡΙΣΜΟΣ ΑΝΤΙΚΤΥΠΟΥ**
Πολύ Υψηλός	Η πραγματοποίηση της απειλής μπορεί να οδηγήσει σε πολύ υψηλού κόστους απώλειες ιδιαίτερα σημαντικών περιουσιακών στοιχείων ή πόρων και να πλήξει σε πολύ μεγάλο βαθμό την αποστολή και τη φήμη του Οργανισμού. Ενίοτε, μπορεί να θέσει σε σημαντικό κίνδυνο ανθρώπινες ζωές.
Υψηλός	Η πραγματοποίηση της απειλής μπορεί να οδηγήσει σε υψηλού κόστους απώλειες σημαντικών περιουσιακών στοιχείων ή πόρων και να πλήξει σημαντικά την αποστολή και τη φήμη του Οργανισμού. Ενίοτε, μπορεί να θέσει σε κίνδυνο ανθρώπινες ζωές.
Μέτριος	Η πραγματοποίηση της απειλής μπορεί να οδηγήσει σε απώλειες περιουσιακών στοιχείων ή πόρων και να πλήξει σε ένα βαθμό την αποστολή και τη φήμη του Οργανισμού. Ενίοτε, μπορεί να οδηγήσει σε τραυματισμούς ανθρώπων.
Χαμηλός	Η πραγματοποίηση της απειλής μπορεί να οδηγήσει σε μικρές απώλειες περιουσιακών στοιχείων ή πόρων, δε μπορεί όμως να πλήξει ουσιαστικά την αποστολή και τη φήμη του Οργανισμού.
Πολύ Χαμηλός	Η πραγματοποίηση της απειλής μπορεί να οδηγήσει σε αμελητέες απώλειες περιουσιακών στοιχείων ή πόρων και δε μπορεί σε καμία περίπτωση να πλήξει την αποστολή και τη φήμη του Οργανισμού.

4.3.2.1. Ποιοτική έναντι Ποσοτικής Αξιολόγησης

Κατά τη διεξαγωγή του σταδίου ανάλυσης των επιπτώσεων, ιδιαίτερη προσοχή θα πρέπει να αποδίδεται στα πλεονεκτήματα και τα μειονεκτήματα των ποσοτικών έναντι των ποιοτικών αξιολογήσεων ([N02]). Το κύριο πλεονέκτημα μιας ποιοτικής ανάλυσης των επιπτώσεων είναι ότι προτεραιοποιεί τους κινδύνους και προσδιορίζει τους τομείς που χρίζουν άμεσων βελτιώσεων για τη βελτίωση των τρωτών σημείων. Το μειονέκτημα των ποιοτικών αναλύσεων είναι ότι δεν παρέχουν μετρήσεις των επιπτώσεων και κατά συνέπεια καθιστούν δύσκολη οποιαδήποτε ανάλυση κόστους-οφέλους των προτεινόμενων ενεργειών αντιμετώπισης του προβλήματος.

Από την άλλη, το σημαντικότερο πλεονέκτημα μιας ποσοτικής ανάλυσης του αντίκτυπου είναι ότι παρέχει «μετρήσιμα» μεγέθη που χαρακτηρίζουν το μέγεθος των επιπτώσεων και μπορούν κατά συνέπεια να χρησιμοποιηθούν σε οποιαδήποτε ανάλυση κόστους-οφέλους για την ενσωμάτωση νέων ελέγχων. Το μειονέκτημα είναι ότι, ανάλογα με τις αριθμητικές κλίμακες που χρησιμοποιούνται για να εκφράσουν τα υπό μέτρηση μεγέθη, η σημασία της ποσοτικής ανάλυσης ενδέχεται να καταστεί ασαφής, οδηγώντας τελικά στην αναγκαιότητα ερμηνείας του αποτελέσματος με «ποιοτικό» τρόπο. Πρόσθετοι παράγοντες πρέπει συχνά να λαμβάνονται υπόψη για τον καθορισμό του εύρους των επιπτώσεων. Αυτοί οι παράγοντες περιλαμβάνουν, αλλά δεν περιορίζονται στα ακόλουθα:

- μια εκτίμηση της συχνότητας υλοποίησης πηγών απειλής εντός μίας προκαθορισμένης χρονικής περιόδου (π.χ. 3 έτη),
- το κατά προσέγγιση κόστος που έχει προκύψει από τη μέχρι τώρα πραγματοποίηση κάθε πηγής απειλής,
- ένα σταθμισμένο συντελεστή που δείχνει τη βαρύτητα του σχετικού αντίκτυπου υλοποίησης μιας συγκεκριμένης πηγής απειλής.

Αποτέλεσμα Σταδίου 6. **Το μέγεθος του αντίκτυπου (Πολύ Υψηλό, Υψηλό, Μέτριο, Χαμηλό, Πολύ Χαμηλό).**

4.3.3. Στάδιο 7: Προσδιορισμός Κίνδυνων (Risk Determination)

Σκοπός αυτού του σταδίου είναι να αξιολογήσει το επίπεδο κινδύνου που διατρέχει ένα IT σύστημα. Ο προσδιορισμός του κινδύνου για ένα συγκεκριμένο ζεύγος απειλής / αδυναμίας μπορεί να εκφραστεί ως συνάρτηση τριών πραγμάτων ([N02]):

- της πιθανότητας μια συγκεκριμένη πηγή απειλής να πραγματοποιηθεί εκμεταλλευόμενη μια συγκεκριμένη αδυναμία του συστήματος,

- του μεγέθους των επιπτώσεων που θα προκύψουν αν μια συγκεκριμένη απειλή πραγματοποιηθεί, εκμεταλλευόμενη μια συγκεκριμένη αδυναμία του συστήματος και
- της επάρκειας των υφιστάμενων ελέγχων ασφαλείας για τη μείωση ή την εξάλειψη του εν λόγω κινδύνου.

Για τη μέτρηση του κινδύνου, μια κλίμακα κινδύνου και ένας πίνακας κλίμακας κινδύνων πρέπει να δημιουργηθούν, τα οποία περιγράφονται στις ενότητες που ακολουθούν.

4.3.3.1. Πίνακας Κλίμακας Κινδύνων

Ο τελικός προσδιορισμός του κινδύνου εκπλήρωσης της αποστολής ενός Οργανισμού, προκύπτει από το γινόμενο της πιθανότητας που αποδόθηκε στο ενδεχόμενο πραγματοποίησης μιας απειλής και τον αντίκτυπο που αυτή η απειλή θα έχει για τον Οργανισμό. Ο Πίνακας 7 δείχνει πώς η συνολική διαβάθμιση των κινδύνων θα μπορούσε να προσδιοριστεί βάσει της πιθανότητας πραγματοποίησης μιας απειλής και της κλίμακας των επιπτώσεων της απειλής αυτής. Πρόκειται για ένα πίνακα 5x5 που κωδικοποιεί σε πέντε επίπεδα την πιθανότητα κινδύνου (Πολύ Υψηλή, Υψηλή, Μέτρια, Χαμηλή, Πολύ Χαμηλή) και τον αντίκτυπο των απειλών (Πολύ Υψηλός, Υψηλός, Μέτριος, Χαμηλός, Πολύ Χαμηλός). Σε κάθε διαβάθμιση αντιστοιχίζουμε ένα score και σε κάθε συνδυασμό το γινόμενο των επιμέρους scores. Εν συνεχεία, σε κάθε συνδυασμό αποδίδεται και πάλι μία ποιοτική διαβάθμιση ανάλογα με το εύρος τιμών στο οποίο ανήκει το συνδυαστικό score με βάση ένα αριθμό ραντών (bands) που έχουμε προκαθορίσει. Ο Πίνακας 7 δείχνει πώς εξάγονται τα συνολικά επίπεδα κινδύνου (Πολύ Υψηλός, Υψηλός, Μέτριος, Χαμηλός, Πολύ Χαμηλός).

Πίνακας 7: Διαβάθμιση Κινδύνου

ΠΙΘΑΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	**ΑΝΤΙΚΤΥΠΟΣ**				
	ΠΟΛΥ ΥΨΗΛΟΣ (100)	***ΥΨΗΛΟΣ (50)***	***ΜΕΤΡΙΟΣ (10)***	***ΧΑΜΗΛΟΣ (1)***	***ΠΟΛΥ ΧΑΜΗΛΟΣ (0.1)***
ΠΟΛΥ ΥΨΗΛΗ (0.9)	*Πολύ Υψηλός (90)*	*Υψηλός (45)*	*Μέτριος (9)*	*Χαμηλός (0.9)*	*Πολύ Χαμηλός (0.09)*
ΥΨΗΛΗ (0.5)	*Υψηλός (50)*	*Υψηλός (25)*	*Μέτριος (5)*	*Χαμηλός (0.5)*	*Πολύ Χαμηλός (0.05)*
ΜΕΤΡΙΑ (0.2)	*Υψηλός (20)*	*Μέτριος (10)*	*Μέτριος (2)*	*Χαμηλός (0.2)*	*Πολύ Χαμηλός (0.02)*
ΧΑΜΗΛΗ (0.05)	*Μέτριος (5)*	*Μέτριος (2.5)*	*Χαμηλός (0.5)*	*Πολύ Χαμηλός (0.05)*	*Πολύ Χαμηλός (0.005)*
ΠΟΛΥ ΧΑΜΗΛΗ (0.01)	*Χαμηλός (1)*	*Χαμηλός (0.5)*	*Πολύ Χαμηλός (0.1)*	*Πολύ Χαμηλός (0.01)*	*Πολύ Χαμηλός (0.001)*

Διαβάθμιση Κινδύνου: *Πολύ Υψηλός:50+ έως 90, Υψηλός:10+ έως 50, Μέτριος: 1+ έως 10, Χαμηλός: 0.1+ έως 1, Πολύ Χαμηλός:0.001-0.1*

Ανάλογα με τις απαιτήσεις του Οργανισμού αλλά και τον επιθυμητό βαθμό ανάλυσης, κάποιοι Οργανισμοί μπορεί να χρησιμοποιήσουν μήτρες μικρότερων ή μεγαλύτερων διαστάσεων (π.χ. 3x3 ή 7x7). Αυτό σημαίνει ότι η χρησιμοποιούμενη κλίμακα μπορεί να εμπλουτιστεί και να συμπεριλάβει διαβαθμίσεις όπως «Πολύ Χαμηλή/ός», «Πολύ Υψηλή/ός», «Βέβαιη/ος», «Μηδενική/ός».

Θα πρέπει τέλος να αναφερθεί ότι ο καθορισμός αυτών των επιπέδων κινδύνου περιλαμβάνει και το υποκειμενικό στοιχείο. Για παράδειγμα, η πιθανότητα που μπορεί να αποδοθεί σε κάθε επίπεδο απειλής κινδύνου μπορεί να είναι 1 για το Υψηλό επίπεδο, 0,5 για το Μέτριο και 0,1 για το Χαμηλό. Αντίστοιχα, η τιμή για κάθε επίπεδο επίπτωσης θα μπορούσε να είναι 10 για το Υψηλό, 5 για το Μέτριο και 1 για το Χαμηλό.

4.3.3.2. Περιγραφή Κλίμακας Κινδύνων

Ο Πίνακας 8 περιγράφει τα επίπεδα κινδύνου που απεικονίζονται στην παραπάνω μήτρα. Αυτή η κλίμακα των κινδύνων, με διαβαθμίσεις «Πολύ Υψηλός», «Υψηλός», «Μέτριος», «Χαμηλός» και «Πολύ Χαμηλός», αναπαριστά το βαθμό ή το επίπεδο του κινδύνου στον οποίο ένα IT σύστημα, ή μια εγκατάσταση, ή μια διαδικασία θα μπορούσε να εκτεθεί, αν μια συγκεκριμένη απειλή πραγματοποιείτο. Η κλίμακα κινδύνου υποδεικνύει επίσης τις ενέργειες που τα ανώτερα διοικητικά στελέχη του Οργανισμού θα πρέπει να πραγματοποιήσουν για κάθε επίπεδο κινδύνου.

Πίνακας 8: Διαβάθμιση Κινδύνου και Προτεινόμενες Ενέργειες

ΔΙΑΒΑΘΜΙΣΗ ΚΙΝΔΥΝΟΥ	**ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΕΝΕΡΓΕΙΕΣ**
Πολύ Υψηλός	Η ανάγκη για λήψη διορθωτικών μέτρων είναι άμεση και επιτακτική. Εάν το σύστημα είναι ήδη σε λειτουργία θα πρέπει να διακοπεί η λειτουργία του, να σχεδιαστεί και να τεθεί άμεσα σε εφαρμογή πλάνο διορθωτικών ενεργειών.
Υψηλός	Η ανάγκη για λήψη διορθωτικών μέτρων είναι επιτακτική. Εάν το σύστημα είναι ήδη σε λειτουργία θα πρέπει να σχεδιαστεί και να τεθεί άμεσα σε εφαρμογή πλάνο διορθωτικών ενεργειών.
Μέτριος	Η ανάγκη για λήψη διορθωτικών μέτρων είναι απαραίτητη και θα πρέπει να σχεδιαστεί και εφαρμοστεί πλάνο διορθωτικών ενεργειών εντός εύλογου χρονικού διαστήματος.
Χαμηλός	Η λήψη διορθωτικών μέτρων είναι απαραίτητη, αλλά μπορεί να αποφασιστεί σε επόμενο στάδιο ή να γίνει αποδοχή του κινδύνου από τον Οργανισμό.
Πολύ Χαμηλός	Η λήψη διορθωτικών μέτρων δεν είναι απαραίτητη, μπορεί να αποφασιστεί σε επόμενο στάδιο ή να γίνει αποδοχή του κινδύνου από τον Οργανισμό.

Αποτέλεσμα Σταδίου 7. **Το επίπεδο κινδύνου (Πολύ Υψηλό, Υψηλό, Μέτριο, Χαμηλό, Πολύ Χαμηλό).**

4.4. Προτάσεις και Τεκμηρίωση

4.4.1. Στάδιο 8: Συστάσεις Ελέγχων (Control Recommendations)

Σε αυτό το στάδιο της διαδικασίας, προτείνονται οι έλεγχοι που θα μπορούσαν να μετριάσουν ή να εξαλείψουν τους κινδύνους που εντοπίστηκαν, ανάλογα με τις δραστηριότητες του Οργανισμού. Ο στόχος των προτεινόμενων ελέγχων είναι να μειώσουν τα επίπεδα κινδύνων για το IT σύστημα και τα δεδομένα του καθιστώντας τα αποδεκτά για τον Οργανισμό. Οι ακόλουθοι παράγοντες πρέπει να λαμβάνονται υπόψη για να είναι όσο το δυνατό πληρέστερη η πρόταση ελέγχων για την ελαχιστοποίηση ή την εξάλειψη των εντοπιζόμενων κινδύνων ([N02], [B01]):

- Εφικτότητα των προτεινόμενων επιλογών (π.χ. συμβατότητα του συστήματος).
- Νομοθεσία και κανονιστικές διατάξεις.
- Πολιτική του Οργανισμού.
- Λειτουργικές επιπτώσεις.
- Ασφάλεια και αξιοπιστία.

Οι συστάσεις ελέγχων είναι το αποτέλεσμα της διαδικασίας αξιολόγησης κινδύνων και αποτελούν πληροφορία / είσοδο για τη διαδικασία μείωσης των κινδύνων που παρουσιάζεται στην επόμενη Ενότητα, και κατά τη διάρκεια της οποίας οι προτεινόμενοι διαδικαστικοί και τεχνικοί έλεγχοι ασφαλείας αξιολογούνται, προτεραιοποιούνται και υλοποιούνται. Θα πρέπει να σημειωθεί ότι δεν είναι πάντα δυνατή η υλοποίηση όλων των προτεινόμενων ελέγχων. Για να προσδιορίσουμε ποιοι από αυτούς απαιτούνται και είναι κατάλληλοι για ένα συγκεκριμένο Οργανισμό, θα πρέπει να διεξαχθεί, όπως ήδη αναφέρθηκε, μια ανάλυση κόστους-οφέλους για να καταδείξει αν τελικά το κόστος υλοποίησης των ελέγχων που οδηγεί σε μείωση των επίπεδων κινδύνου είναι αποδεκτό από τον Οργανισμό. Επιπλέον, οι λειτουργικές επιπτώσεις (π.χ. επιπτώσεις στην

απόδοση του συστήματος) και η εφικτότητα (π.χ. τεχνικές προδιαγραφές, αποδοχή από τους χρήστες) εφαρμογής των προτεινόμενων επιλογών, πρέπει να αξιολογούνται προσεκτικά κατά τη διάρκεια της διαδικασίας μείωσης κινδύνων.

Αποτέλεσμα Σταδίου 8. **Σύσταση ελέγχων για τον περιορισμό των κινδύνων.**

4.4.2. Στάδιο 9: Τεκμηρίωση Αποτελεσμάτων (Results Documentation)

Αφού η αξιολόγηση κινδύνων έχει ολοκληρωθεί (προσδιορισμός πηγών απειλής και τρωτών σημείων, αξιολόγηση κινδύνων και πρόταση ελέγχων), τα αποτελέσματα της όλης διαδικασίας θα πρέπει να τεκμηριωθούν με κάποια επίσημη έκθεση ή ενημέρωση ([B01], [N02]).

Μια έκθεση αξιολόγησης κινδύνων είναι μια διοικητική έκθεση που βοηθά ανώτερα διευθυντικά στελέχη στη λήψη αποφάσεων σχετικά με την πολιτική, τις διαδικασίες, τον προϋπολογισμό και ενδεχόμενες αλλαγές στη λειτουργία των συστημάτων και του Οργανισμού. Αντίθετα από μία έκθεση ελέγχου (audit report) ή διερεύνησης (investigation report), οι οποίες ερευνούν «προβληματικές» ενέργειες, η έκθεση αξιολόγησης κινδύνων δε θα πρέπει να παρουσιάζεται με κατηγορηματικό τρόπο, αλλά ως μια συστηματική και αναλυτική προσέγγιση για την εκτίμηση κινδύνων, έτσι ώστε τα ανώτερα διοικητικά στελέχη να μπορούν να κατανοήσουν τους κινδύνους και να διαθέσουν τους απαραίτητους πόρους για τη μείωσή τους. Για το λόγο αυτό, κάποιοι προτιμούν να αναφέρουν τα ζεύγη απειλής / αδυναμίας ως παρατηρήσεις και όχι ως διαπιστώσεις στην έκθεση αξιολόγησης κινδύνων.

Αποτέλεσμα Σταδίου 9. **Έκθεση εκτίμησης κινδύνου που περιγράφει τις απειλές και τα τρωτά σημεία, μετρά τον κίνδυνο και παρέχει συστάσεις για την υλοποίηση ελέγχων.**

5. Ανάλυση και Διαχείριση Κινδύνων – Μέθοδοι

Ο περιορισμός του κινδύνου (risk mitigation), είναι ουσιαστικά η δεύτερη σημαντική ενότητα της διαδικασίας διαχείρισης κινδύνων ([JA05], [N02]). Σημαντικές εργασίες που εκτελούνται κατά τη διάρκεια της διαδικασίας περιορισμού κινδύνων είναι η προτεραιοποίηση, αξιολόγηση, και υλοποίηση των κατάλληλων ελέγχων μείωσης κινδύνου που έχουν προταθεί κατά τη διαδικασία εκτίμησης των κινδύνων (risk assessment) που προηγήθηκε. Δεδομένου ότι η εξάλειψη όλων των κινδύνων είναι συνήθως ανέφικτη, αποτελεί ευθύνη των ανώτερων διευθυντικών στελεχών να επιλέξουν, λαμβάνοντας υπόψη και το κόστος υλοποίησης, ποιοι είναι οι πλέον ενδεδειγμένοι έλεγχοι, η υλοποίηση των οποίων θα μειώσει τον κίνδυνο εκπλήρωσης της αποστολής του Οργανισμού σε αποδεκτό επίπεδο, με το ελάχιστο δυνατό κόστος. Ιδιαίτερα σημαντική είναι η πρόληψη περιπτώσεων απάτης (fraud), η οποία μπορεί σε σημαντικό βαθμό να υποβοηθηθεί από διαρκή παρακολούθηση των IT συστημάτων για εντοπισμό «ύποπτων» συμπεριφορών συστημάτων και προειδοποίηση των υπεύθυνων όταν εντοπίζονται τέτοιες συμπεριφορές ώστε να περιορίζονται τυχόν επιπτώσεις σε αρχικό στάδιο ([M09]).

Στην ενότητα αυτή περιγράφονται οι δυνατές επιλογές και η στρατηγική περιορισμού των κινδύνων, η μεθοδολογία με την οποία επιλέγονται οι έλεγχοι που θα υλοποιηθούν (cost-benefit analysis) και ο τρόπος εφαρμογής των επιλεχθέντων ελέγχων.

5.1. Περιορισμός - Εξάλειψη Κινδύνων (Risk Mitigation)

5.1.1. Επιλογές Περιορισμού Κινδύνων

Ο περιορισμός των κινδύνων είναι μια συστηματική μεθοδολογία που στοχεύει στη μείωση των κινδύνων που αντιμετωπίζει ένας Οργανισμός οι οποίοι μπορεί να έχουν αντίκτυπο στην εκπλήρωση της αποστολής του ([M09]). Η αντιμετώπιση και ο περιορισμός των κινδύνων αυτών, απαντάται συνήθως από ένα Οργανισμό με μία ή περισσότερες από τις παρακάτω επιλογές ([N02]):

1. Ανάληψη Κινδύνου. Αποδοχή του πιθανού κινδύνου και συνέχιση της λειτουργίας του IT συστήματος, ή μερική υλοποίηση ελέγχων ώστε να περιοριστεί ο κίνδυνος σε αποδεκτά επίπεδα.
2. Αποφυγή Κινδύνου. Αποφυγή κινδύνου με την εξάλειψη της αιτίας που τον προκαλεί ή / και των συνεπειών που έχει για τον Οργανισμό (π.χ. αναστολή ορισμένων λειτουργιών του IT συστήματος ή ακόμη και τερματισμό της λειτουργίας του όταν εντοπίζονται κίνδυνοι).
3. Περιορισμός του Κινδύνου. Περιορισμός του κίνδυνου με υλοποίηση των ελέγχων που ελαχιστοποιούν τις αρνητικές επιπτώσεις τυχόν πραγματοποίησης μιας απειλής (π.χ. χρήση υποστηρικτικών, ανασταλτικών και ανιχνευτικών ελέγχων).
4. Σχεδιασμός Πλάνου Περιορισμού του Κινδύνου. Ανάπτυξη ενός πλάνου περιορισμού των κινδύνων που προτεραιοποιεί, υλοποιεί και συντηρεί τους απαραίτητους ελέγχους.
5. Έρευνα και Αναγνώριση. Μείωση του κινδύνου με την αναγνώριση των αδυναμιών ή των τρωτών σημείων των IT συστημάτων και τη διερεύνηση ελέγχων που ισχυροποιούν τα ευπαθή σημεία.

6. Μετακύληση του Κινδύνου. Μετακύληση του κινδύνου, χρησιμοποιώντας άλλες επιλογές για την αντιστάθμιση τυχόν απωλειών, όπως για παράδειγμα την επιλογή ασφαλιστικής κάλυψης.

Οι στόχοι και η αποστολή του Οργανισμού θα πρέπει να λαμβάνονται υπόψη για την χρησιμοποίηση ή όχι οποιασδήποτε από τις παραπάνω επιλογές. Κατά κανόνα, δεν είναι πρακτικά εφικτό για ένα Οργανισμό να αντιμετωπίσει όλους τους κινδύνους που έχουν εντοπιστεί, επομένως πρέπει να δίνεται προτεραιότητα σε εκείνα τα ζεύγη απειλών / αδυναμιών που δυνητικά μπορούν να προκαλέσουν σημαντικές βλάβες και να έχουν σοβαρό αντίκτυπο στην επίτευξη της αποστολής του Οργανισμού. Επιπλέον, ανάλογα με το περιβάλλον και τους στόχους του κάθε Οργανισμού, οι επιλογές που γίνονται για τον περιορισμό του κινδύνου και οι μέθοδοι που χρησιμοποιούνται για την υλοποίηση των ελέγχων μπορεί να διαφέρουν. Η καλύτερη προσέγγιση του ζητήματος είναι να χρησιμοποιήσουμε ένα μείγμα εφαρμογών ασφαλείας που διατίθενται στην αγορά μαζί με τις κατάλληλες επιλογές περιορισμού κινδύνων αλλά ταυτόχρονα και τα απαραίτητα «μη τεχνικά», διοικητικά μέτρα.

5.1.2. Στρατηγικές Περιορισμού των Κινδύνων

Τα ανώτερα διευθυντικά στελέχη κάθε Οργανισμού, γνωρίζοντας τους δυνητικούς κινδύνους και τους προτεινόμενους ελέγχους, θα ήθελαν να είναι σε θέση να γνωρίζουν, πότε και υπό ποιες συνθήκες θα πρέπει να αναλάβουν δράση και πότε θα πρέπει να εφαρμόσουν τους προτεινόμενους ελέγχους ώστε να προστατεύσουν τον Οργανισμό.

Η στρατηγική περιορισμού των κινδύνων μπορεί να καταστεί περισσότερο πρακτική αν ακολουθηθούν οι παρακάτω εμπειρικοί κανόνες, οι οποίοι εστιάζουν κυρίως στην αντιμετώπιση εκούσιων ανθρώπινων απειλών ([N01b], [NG96]):

- Όταν υπάρχουν αδυναμίες και τρωτά σημεία σε ένα IT σύστημα, μπορούν να εφαρμοστούν τεχνικές οι οποίες μειώνουν την πιθανότητα κάποιος να επωφεληθεί από τα κενά αυτά.
- Αν παραμένουν τρωτά σημεία τα οποία μπορεί κάποιος να εκμεταλλευτεί, τότε θα μπορούσαν να αποδειχτούν χρήσιμες τεχνικές πολυεπίπεδης προστασίας, επανασχεδιασμού ενδεδειγμένης αρχιτεκτονικής συστημάτων, καθώς και διοικητικοί έλεγχοι ώστε να ελαχιστοποιηθεί ο κίνδυνος ή να αποτραπεί η εμφάνιση σχετικού περιστατικού.
- Όταν το κόστος για τον εισβολέα είναι μικρότερο από το ενδεχόμενο όφελος, μπορούν να εφαρμοστούν τεχνικές που περιορίζουν τα κίνητρα του εισβολέα αυξάνοντας το κόστος του (π.χ. εφαρμογή μηχανισμών, όπως ο περιορισμός των προσβάσεων των χρηστών μόνο σε ότι είναι απαραίτητο για τη δουλειά τους μπορεί να μειώσει σημαντικά τα δυνητικά οφέλη και επομένως τα κίνητρα του εισβολέα).
- Όταν οι δυνητικές απώλειες είναι πολύ μεγάλες, μπορούν να εφαρμοστούν οι κατάλληλες αρχές επανασχεδιασμού της αρχιτεκτονικής του IT συστήματος αλλά και «μη τεχνικοί» έλεγχοι οι οποίοι θα περιορίσουν την έκταση της επίθεσης, μειώνοντας έτσι το μέγεθος της δυνητικής ζημίας.

Οι τεχνικές που περιγράφονται ανωτέρω, με εξαίρεση την τρίτη (κόστος εισβολέα μικρότερο από το ενδεχόμενο όφελος), έχουν εφαρμογή και για τον περιορισμό των κινδύνων που απορρέουν από τις περιβαλλοντικές απειλές ή ακούσιες ανθρώπινες απειλές (π.χ. σφάλματα συστήματος ή χρηστών).

5.1.3. Τρόποι Υλοποίησης Ελέγχων

Όταν είναι πλέον η στιγμή να πραγματοποιηθούν ενέργειες / δράσεις υλοποίησης ελέγχων, θα πρέπει να επιδιώκεται ο εντοπισμός των μεγαλύτερων

κινδύνων και να καταβάλλεται προσπάθεια επαρκούς περιορισμού τους με το χαμηλότερο δυνατό κόστος και την ελάχιστη δυνατή επίδραση στην ομαλή εκτέλεση της αποστολής του Οργανισμού.

Σε ό,τι ακολουθεί, περιγράφεται η προτεινόμενη από το ([N02]) μεθοδολογία περιορισμού/ εξάλειψης των κινδύνων. Η μεθοδολογία περιλαμβάνει 7 στάδια:

1. *Στάδιο 1: Προτεραιοποίηση Ενεργειών/ Δράσεων.* Οι ενέργειες / δράσεις υλοποίησης πρέπει να προτεραιοποιούνται ανάλογα με τα επίπεδα κινδύνου που έχουν προκύψει από την έκθεση αξιολόγησης κινδύνων που έχει διενεργηθεί. Κατά την κατανομή των πόρων, πρώτη προτεραιότητα πρέπει να δίνεται στους ελέγχους με πολύ υψηλά επίπεδα κινδύνου. Τα ζεύγη αδυναμιών / απειλών που έχουν εντοπιστεί κατά τη φάση αξιολόγησης κινδύνων, απαιτούν άμεσα διορθωτικά μέτρα για την προστασία των συμφερόντων και την απρόσκοπτη εκτέλεση της αποστολής του Οργανισμού.

   Αποτέλεσμα Σταδίου 1: Διαβάθμιση προτεραιότητας ενεργειών / δράσεων.

2. *Στάδιο 2: Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων.* Οι έλεγχοι που προτείνονται από τη διαδικασία αξιολόγησης κινδύνων που έχει προηγηθεί, μπορεί να μην είναι οι πλέον ενδεδειγμένες και εφικτές επιλογές για κάθε επιμέρους διοικητική μονάδα ή σύστημα πληροφορικής του Οργανισμού. Κατά τη διάρκεια αυτού του σταδίου, αναλύεται η εφικτότητα (π.χ. συμβατότητα με υφιστάμενους ελέγχους και συστήματα, αποδοχή από τους χρήστες) και η αποτελεσματικότητα (π.χ. ο βαθμός προστασίας και το επίπεδο περιορισμού του κινδύνου) των προτεινόμενων επιλογών ελέγχου. Ο στόχος του σταδίου αυτού είναι να επιλεγούν οι πλέον ενδεδειγμένοι έλεγχοι για την ελαχιστοποίηση των κινδύνων.

Αποτέλεσμα Σταδίου 2: Κατάλογος εφικτών (feasible) ελέγχων.

3. *Στάδιο 3: Διεξαγωγή Ανάλυσης Κόστους – Οφέλους.* Η διεξαγωγή της εν λόγω ανάλυσης είναι απαραίτητη για την υποστήριξη της Διοίκησης του Οργανισμού στη λήψη αποφάσεων σχετικά με τους προτεινόμενους ελέγχους, αφού προσδιορίζει τη σχέση κόστους – οφέλους των ελέγχων που έχουν προταθεί κατά το risk assessment. Ο τρόπος διεξαγωγής της ανάλυσης αυτής περιγράφεται αναλυτικά στην Ενότητα 5.1.5.

Αποτέλεσμα Σταδίου 3: Ανάλυση κόστους-οφέλους που περιγράφει το κόστος και τα οφέλη από την εφαρμογή ή όχι των προτεινόμενων ελέγχων.

4. *Στάδιο 4: Επιλογή Ελέγχων.* Αξιοποιώντας τα αποτελέσματα της ανάλυσης κόστους-οφέλους, η Διοίκηση του Οργανισμού επιλέγει την εφαρμογή εκείνων των ελέγχων οι οποίοι είναι υψηλότερης αξίας με βάση την ανάλυση κόστους-οφέλους που έχει διενεργηθεί. Οι έλεγχοι που επιλέγονται θα πρέπει να συνδυάζουν τεχνικά, λειτουργικά και διοικητικά χαρακτηριστικά ώστε να διασφαλίζεται επαρκώς η ασφάλεια των IT συστημάτων και κατά συνέπεια του Οργανισμού.

Αποτέλεσμα Σταδίου 4: Επιλεγμένοι έλεγχοι

5. *Στάδιο 5: Ανάθεση Αρμοδιοτήτων.* Κατά το στάδιο αυτό, εντοπίζονται τα κατάλληλα άτομα (υπάλληλοι του Οργανισμού ή εξωτερικοί συνεργάτες) που έχουν την απαιτούμενη κατάρτιση, εμπειρία και τα απαραίτητα προσόντα για να υλοποιήσουν τους επιλεγμένους ελέγχους και τους ανατίθενται οι σχετικές αρμοδιότητες.

Αποτέλεσμα Σταδίου 5: Κατάλογος αρμοδίων

6. *Στάδιο 6: Ανάπτυξη Πλάνου Υλοποίησης Προστασίας.* Κατά τη διάρκεια αυτού του σταδίου, αναπτύσσεται ένα πλάνο υλοποίησης μηχανισμών προστασίας. Το πλάνο αυτό πρέπει, κατ' ελάχιστο, να περιλαμβάνει τα ακόλουθα:
    1. Ζεύγη αδυναμιών/ απειλών και τα επίπεδα κινδύνου που τους αντιστοιχούν και τα οποία έχουν προκύψει από την έκθεση αξιολόγησης κινδύνων.
    2. Προτεινόμενοι έλεγχοι, όπως αυτοί έχουν προκύψει από την έκθεση αξιολόγησης των κινδύνων.
    3. Προτεραιοποιημένες ενέργειες / δράσεις ειδικότερα για τα πολύ υψηλά και υψηλά επίπεδα κινδύνου.
    4. Επιλεγμένοι έλεγχοι προς υλοποίηση, όπως αυτοί έχουν καθοριστεί με βάση την σκοπιμότητα, την αποτελεσματικότητα, τα οφέλη και το κόστος.
    5. Απαιτούμενοι πόροι για την υλοποίηση των επιλεχθέντων ελέγχων.
    6. Κατάλογοι αρμοδίων και προσωπικού που εμπλέκεται στη διαδικασία υλοποίησης.
    7. Ημερομηνία έναρξης για την υλοποίησης των ελέγχων.
    8. Ημερομηνία - στόχος για την ολοκλήρωση της υλοποίησης των ελέγχων.
    9. Απαιτήσεις για «συντήρηση» των ελέγχων.

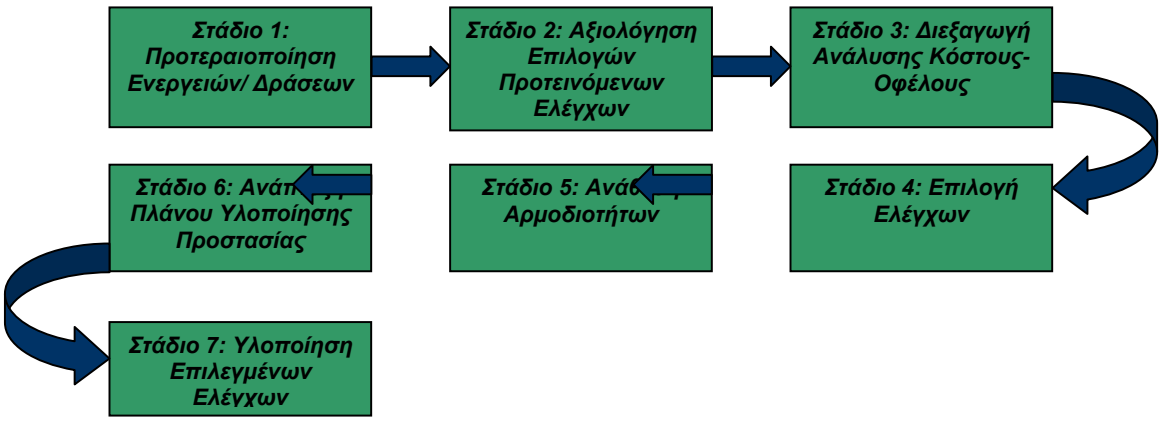
Το πλάνο υλοποίησης προστασίας προτεραιοποιεί, όπως φαίνεται παραπάνω τις ενέργειες / δράσεις και τα επιμέρους έργα που απαιτούνται και θέτει ημερομηνίες έναρξης και ολοκλήρωσης. Επιπλέον, επιταχύνει τη διαδικασία περιορισμού/ εξάλειψης των κινδύνων.

Αποτέλεσμα Σταδίου 6: Πλάνο υλοποίησης προστασίας

7. *Στάδιο 7: Υλοποίηση Επιλεγμένων Ελέγχων.* Ανάλογα με τις ιδιαιτερότητες του Οργανισμού, οι έλεγχοι που υλοποιούνται μειώνουν τα επίπεδα κινδύνου, αλλά σχεδόν ποτέ δεν εξαλείφουν πλήρως κάθε κίνδυνο. Οι κίνδυνοι που παραμένουν (residual risks) εξετάζονται στην Ενότητα 5.1.6.

Αποτέλεσμα Σταδίου 7: Εναπομείναντες Κίνδυνοι

Σχήμα 3: Στάδια Διαδικασίας Περιορισμού Κινδύνων



Τα παραπάνω στάδια της διαδικασίας περιορισμού των κινδύνων, παρουσιάζονται συνοπτικά στο Σχήμα 3.

5.1.4. Κατηγορίες Ελέγχων

Οι έλεγχοι ασφαλείας, όταν χρησιμοποιούνται με τον ενδεδειγμένο τρόπο, μπορεί να αποτρέψουν, ή να περιορίσουν τις απειλές και να συμβάλλουν στην απρόσκοπτη ολοκλήρωση της αποστολής του Οργανισμού. Κατά την υλοποίηση των προτεινόμενων ελέγχων για τον περιορισμό των κινδύνων, ένας

Οργανισμός πρέπει να εστιάσει σε τεχνικούς, διοικητικούς και λειτουργικούς ελέγχους ασφαλείας, ώστε να μεγιστοποιήσει την αποτελεσματικότητα των ελέγχων για τα IT συστήματα και τον Οργανισμό.

Ένα παράδειγμα το οποίο δείχνει τις διάφορες κατηγορίες ελέγχων που πρέπει να εξετάσει ένας Οργανισμός είναι η περίπτωση επιβολής χρήσης σύνθετων κωδικών πρόσβασης χρηστών ώστε να ελαχιστοποιηθεί ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης. Σε αυτή την περίπτωση, η ενσωμάτωση του σχετικού ελέγχου σε τεχνικό επίπεδο (λογισμικό ασφάλειας) μπορεί να είναι περισσότερο πολύπλοκη και δαπανηρή από ένα απλό διαδικαστικό έλεγχο, όμως ο τεχνικός έλεγχος είναι πιθανό να είναι αποτελεσματικότερος, επειδή η εκτέλεσή του είναι αυτοματοποιημένη και ελεγχόμενη από το σύστημα.

Ταυτόχρονα, ένας έλεγχος σε διαδικαστικό επίπεδο μπορεί να υλοποιηθεί με την απλή έκδοση ενός εγγράφου - υπομνήματος που αποτυπώνει τη διαδικασία, απευθύνεται σε όλο το εμπλεκόμενο προσωπικό και θέτει τις επιπλέον κατευθυντήριες γραμμές ασφάλειας για τον Οργανισμό. Είναι βέβαια προφανές ότι η διασφάλιση ότι οι χρήστες ακολουθούν με συνέπεια τις οδηγίες του υπομνήματος, είναι πρακτικά δύσκολη και προϋποθέτει την ευρεία ενημέρωση και ευαισθητοποίηση σε θέματα ασφάλειας, την εκπαίδευση του προσωπικού ([DR03]) και, τελικά, την αποδοχή των οδηγιών από τους τελικούς χρήστες.

Στις ενότητες που ακολουθούν παρατίθεται μια επισκόπηση των τεχνικών, διοικητικών και λειτουργικών ελέγχων. Αναλυτικότερα στοιχεία μπορεί κανείς να βρει στα ([N95]) και ([NF98]).

5.1.4.1. Τεχνικοί Έλεγχοι Ασφαλείας

Η εφαρμογή τεχνικών ελέγχων ασφαλείας για τον περιορισμό των κινδύνων

μπορεί να χρησιμοποιηθεί για την προστασία από συγκεκριμένους τύπους απειλών. Οι έλεγχοι αυτοί μπορεί να είναι απλοί ή σύνθετοι και συνήθως παραπέμπουν σε θέματα σχεδιασμού και αρχιτεκτονικής συστημάτων και εφαρμογές / προγράμματα ασφάλειας ([G04]). Συνήθως πρόκειται για ένα μείγμα παρεμβάσεων σε επίπεδο υλικού και λογισμικού συστημάτων και εφαρμογών. Τα μέτρα πρέπει να «δένουν» αρμονικά μεταξύ τους ώστε να διασφαλίζονται οι πληροφορίες και οι λειτουργίες των IT συστημάτων. Οι τεχνικοί έλεγχοι μπορούν να ομαδοποιηθούν στις ακόλουθες μεγάλες κατηγορίες, ανάλογα με το βασικό στόχο στον οποίο αποβλέπουν:

- *Υποστηρικτικοί.* Οι υποστηρικτικοί έλεγχοι είναι γενικοί και αποτελούν τη βάση για τις περισσότερες λειτουργίες ασφάλειας. Η ύπαρξη αυτής της κατηγορίας ελέγχων είναι απαραίτητη για την υλοποίηση άλλων ελέγχων.
- *Προληπτικοί*. Οι προληπτικοί έλεγχοι εστιάζουν στην πρόληψη εμφάνισης συμβάντων παραβίασης της ασφάλειας.
- *Ανιχνευτικοί και Διορθωτικοί.* Οι έλεγχοι εστιάζουν στην ανίχνευση συμβάντων παραβίασης και την αποκατάσταση λειτουργιών και δεδομένων μετά από τέτοιες παραβιάσεις.

5.1.4.1.1. Υποστηρικτικοί Τεχνικοί Έλεγχοι Ασφαλείας

Οι υποστηρικτικοί έλεγχοι είναι, από τη φύση τους, «εσωτερικοί» και αλληλένδετοι με πολλούς άλλους ελέγχους. Μια συνοπτική λίστα τέτοιων ελέγχων είναι η ακόλουθη:

- *Έλεγχοι Εντοπισμού.* Αυτή η κατηγορία ελέγχων παρέχει τη δυνατότητα ακριβούς προσδιορισμού των χρηστών, των διαδικασιών και των πηγών πληροφοριών και είναι ιδιαίτερα σημαντική για την υλοποίηση άλλων ελέγχων ασφαλείας (π.χ. έλεγχος διακριτής πρόσβασης, υποχρεωτικός έλεγχος πρόσβασης).

- *Κρυπτογράφηση.* Σημαντική υποδομή για μια ευρεία γκάμα ελέγχων αποτελεί η ύπαρξη μηχανισμών δημιουργίας και διαχείρισης κλειδιών κρυπτογράφησης. Η διαχείριση των κρυπτογραφικών κλειδιών περιλαμβάνει την παραγωγή, διανομή, αποθήκευση και συντήρηση κλειδιών.
- *Μηχανισμοί Διαχείρισης Ασφάλειας.* Τα χαρακτηριστικά ασφαλείας ενός IT συστήματος θα πρέπει να προσαρμόζονται και να παραμετροποιούνται με τον ενδεδειγμένο τρόπο ώστε να καλύπτουν τις εκάστοτε ανάγκες του και να είναι σε θέση να ενσωματώνουν τις αλλαγές που πραγματοποιούνται στο επιχειρησιακό περιβάλλον που υποστηρίζουν. Η ασφάλεια των συστημάτων μπορεί να υλοποιηθεί είτε σε επίπεδο λειτουργικού συστήματος, είτε σε επίπεδο εφαρμογής. Επιπλέον, διατίθεται στην αγορά ευρεία γκάμα προϊόντων υποστήριξης σε θέματα ασφάλειας.
- *Μηχανισμοί Προστασίας Συστήματος.* Σημαντική προϋπόθεση για την επαρκή υποστήριξη λειτουργικών δυνατοτήτων ασφάλειας αποτελεί πάντα η ποιότητα του σχεδιασμού και της υλοποίησης των μηχανισμών ασφαλείας σε τεχνικό επίπεδο. Ενδεικτικά αναφέρουμε κάποια παραδείγματα μηχανισμών προστασίας συστήματος, όπως είναι η προστασία από κινδύνους επαναχρησιμοποίησης πληροφοριών, ο διαχωρισμός των διαδικασιών, η τμηματοποίηση περιοχών των συστημάτων, κ.λπ.

5.1.4.1.2. Προληπτικοί Τεχνικοί Έλεγχοι Ασφαλείας

Πρόκειται για ελέγχους οι οποίοι εστιάζουν στην αποτροπή παραβιάσεων της πολιτικής ασφάλειας και περιλαμβάνουν τις εξής βασικές κατηγορίες:

- *Έλεγχοι Πιστοποίησης (Authentication).* Οι έλεγχοι πιστοποίησης αποτελούν μηχανισμούς εξακρίβωσης της ταυτότητας ενός χρήστη ώστε

να καταστεί εφικτή η πρόσβασή του στο σύστημα. Οι μηχανισμοί πιστοποίησης περιλαμβάνουν κωδικούς πρόσβασης (passwords), προσωπικούς αριθμούς αναγνώρισης (PINs), ενώ υπάρχει και ένας σημαντικός αριθμός νέων αναδυόμενων τεχνολογιών ελέγχου ταυτότητας όπως, έξυπνες κάρτες, ψηφιακά πιστοποιητικά, κωδικοί μιας χρήσης, κ.λπ.

- *Έλεγχοι Εξουσιοδότησης (Authorization).* Οι έλεγχοι εξουσιοδότησης επιτρέπουν τον καθορισμό και τη μελλοντική διαχείριση των δυνατοτήτων που παρέχει ένα σύστημα (π.χ. ο ιδιοκτήτης πληροφοριών και ο διαχειριστής της βάσης δεδομένων καθορίζει ποιοι χρήστες έχουν πρόσβαση σε μια συγκεκριμένη περιοχή πληροφοριών).
- *Επιβολή Ελέγχων Πρόσβασης.* Η ακεραιότητα και η εμπιστευτικότητα των δεδομένων επιβάλλεται μέσω της διαδικασίας επιβολής ελέγχων πρόσβασης. Όταν κάποιος χρήστης αποκτά πρόσβαση σε ένα σύστημα και μπορεί να εκτελέσει συγκεκριμένες λειτουργίες, είναι αναγκαίο να του επιβληθεί η προκαθορισμένη πολιτική ασφαλείας. Η επιβολή πολιτικών ασφαλείας πραγματοποιείται μέσω μηχανισμών ελέγχου πρόσβασης σε όλα τα επιμέρους τμήματα του IT συστήματος. Η αποτελεσματικότητα της εν λόγω διαδικασίας εξαρτάται από την ορθότητα των αποφάσεων ελέγχου πρόσβασης (π.χ. πώς έχουν παραμετροποιηθεί οι κανόνες ασφαλείας) καθώς επίσης και από το σχεδιασμό ασφάλειας σε επίπεδο λογισμικού και υλικού.
- *Υποχρεωτικότητα Αποστολής και Αποδοχής (Non-repudiation).* Η αξιοπιστία και εγκυρότητα ενός IT συστήματος εξαρτάται εν πολλοίς από την υποχρεωτικότητα αποστολής ή αποδοχής πληροφοριών. Οι έλεγχοι αυτοί εφαρμόζονται συνήθως στα σημεία αποστολής και λήψης πληροφοριών του συστήματος. Θα πρέπει να σημειώσουμε ότι παρόλο που ο εν λόγω μηχανισμός εστιάζει τόσο στην πρόληψη όσο και στην ανίχνευση, στην παρούσα εργασία έχει ενταχθεί κάτω από την ομπρέλα των μηχανισμών πρόληψης.

- *Προστασία Επικοινωνιών.* Σε κατανεμημένα (distributed) συστήματα, η εκπλήρωση των στόχων ασφαλείας εξαρτάται σε μεγάλο βαθμό από την ασφάλεια σε επίπεδο επικοινωνιών και δικτύων. Οι ασφαλείς επικοινωνίες χρησιμοποιούν μεθόδους κρυπτογράφησης δεδομένων και ειδικές τεχνολογίες κρυπτογράφησης (π.χ. Data Encryption Standard - DES, Triple DES, RAS, MD4, MD5, κλπ.) για την ελαχιστοποίηση δικτυακών απειλών.
- *Ιδιωτικότητα Συναλλαγών.* Απαραίτητη προϋπόθεση για την ορθή λειτουργία κάθε IT συστήματος, αποτελεί η προστασία της ιδιωτικότητας των συναλλαγών και των προσωπικών δεδομένων. Για το λόγο αυτό χρησιμοποιούνται ειδικοί μηχανισμοί οι οποίοι διασφαλίζουν την ιδιωτικότητα των συναλλαγών (π.χ. Secure Sockets Layer, Secure Shell).

5.1.4.1.3. Τεχνικοί Έλεγχοι Εντοπισμού και Αποκατάστασης Ασφάλειας

Οι έλεγχοι εντοπισμού ή ανίχνευσης μας προειδοποιούν για παραβιάσεις ή απόπειρες παραβίασης των πολιτικών ασφάλειας και περιλαμβάνουν ελέγχους όπως ιχνηλατήσεις (audit trails) και μεθόδους ανίχνευσης εισβολών. Οι μηχανισμοί αποκατάστασης μπορούν να χρησιμοποιηθούν για την αποκατάσταση χαμένων δεδομένων ή τμημάτων λογισμικού ή υλικού του συστήματος. Η ύπαρξή τους είναι αναγκαία για να συμπληρώσει τους υποστηρικτικούς και προληπτικούς τεχνικούς ελέγχους γιατί, ας μην ξεχνάμε, κανένας από τους ελέγχους των άλλων τομέων δε είναι τέλειος. Αναλυτικότερα, οι έλεγχοι εντοπισμού και αποκατάστασης, περιλαμβάνουν:

- *Επιθεωρήσεις – Έλεγχους Γεγονότων (Audits).* Οι έλεγχοι γεγονότων που σχετίζονται με ζητήματα ασφάλειας, καθώς και η παρακολούθηση και εντοπισμός «μη φυσιολογικών συμπεριφορών» του συστήματος είναι

τα βασικά στοιχεία για την ανίχνευση προβληματικών καταστάσεων και την αποκατάσταση των προβλημάτων μετά από παραβιάσεις ασφάλειας.

- *Ανιχνεύσεις και Περιορισμοί Εισβολών.* Είναι ιδιαίτερα σημαντικός ο άμεσος εντοπισμός παραβιάσεων ασφάλειας (π.χ. εισβολές στο δίκτυο, ύποπτες δραστηριότητες), έτσι ώστε να δρομολογούνται έγκαιρα οι απαιτούμενες διορθωτικές παρεμβάσεις. Από την άλλη, είναι μικρής αξίας η ανίχνευση κάποιας παραβίασης ασφάλειας, εάν δεν υπάρχει δυνατότητα άμεσης και αποτελεσματικής αντίδρασης.
- *Έλεγχοι Απόδειξης Πληρότητας και Ακεραιότητας.* Οι συγκεκριμένοι έλεγχοι αναλύουν την ακεραιότητα του συστήματος και τυχόν «μη φυσιολογικές συμπεριφορές» του και εντοπίζουν το βαθμό έκθεσης σε πιθανές απειλές. Οι έλεγχοι αυτοί δεν αποτρέπουν την παραβίαση πολιτικών ασφάλειας, αλλά εντοπίζουν τις παραβιάσεις και βοηθούν στον καθορισμό των απαιτούμενων διορθωτικών ενεργειών.
- *Επαναφορά σε Ασφαλή Κατάσταση.* Ο μηχανισμός αυτός επιτρέπει σε ένα σύστημα να επιστρέφει σε μια πρότερη κατάσταση που είναι γνωστό ότι είναι ασφαλής, στην περίπτωση που λάβει χώρα κάποια παραβίαση ασφάλειας.
- *Έλεγχοι Ανίχνευσης και Εξάλειψης Ιών.* Κατά κανόνα, η κατηγορία αυτών των ελέγχων υποστηρίζεται από λογισμικό ανίχνευσης και εξάλειψης ιών. Η εφαρμογή τους συμβάλλει σημαντικά στη διασφάλιση την ακεραιότητας του συστήματος και των δεδομένων.

5.1.4.2. Διοικητικοί Έλεγχοι Ασφαλείας

Οι διοικητικοί έλεγχοι ασφαλείας, εφαρμόζονται σε συνδυασμό με τους τεχνικούς και λειτουργικούς ελέγχους, για να διαχειριστούν αποτελεσματικά και, εν τέλει, να μειώσουν τους κινδύνους και να προστατέψουν την αποστολή ενός Οργανισμού. Οι διοικητικοί έλεγχοι επικεντρώνονται κυρίως στη διαμόρφωση πολιτικών για την προστασία των πληροφοριών, και στη συμμόρφωση με

κατευθυντήριες γραμμές και πρότυπα που πρέπει να ακολουθούνται βάσει των ισχυόντων επιχειρησιακών διαδικασιών. Οι τρεις κατηγορίες αυτών των ελέγχων (προληπτικοί, ανιχνευτικοί και αποκατάστασης), παρουσιάζονται αναλυτικά στις παρακάτω ενότητες.

5.1.4.2.1. Προληπτικοί Διοικητικοί Έλεγχοι Ασφαλείας

Η κατηγορία αυτή των ελέγχων περιλαμβάνει τα ακόλουθα:

- Ανάθεση αρμοδιοτήτων/ ευθυνών για ζητήματα ασφάλειας σε συγκεκριμένα άτομα, ώστε ανά πάσα στιγμή να διασφαλίζεται ότι υπάρχει ικανοποιητικός βαθμός ασφάλειας σε συστήματα που είναι κρίσιμα για την επίτευξη της αποστολής του Οργανισμού.
- Ανάπτυξη και ανανέωση των πλάνων ασφαλείας των συστημάτων τα οποία καταγράφουν τους υφιστάμενους ελέγχους και επισημαίνουν τους σχεδιαζόμενους ελέγχους.
- Υλοποίηση μηχανισμών ελέγχου ασφαλείας του προσωπικού. Οι έλεγχοι αυτοί πρέπει να στοχεύουν στη διασφάλιση αρχών όπως ο διαχωρισμός των καθηκόντων (segregation of duties), η εκχώρηση ή ακύρωση/ τερματισμός προσβάσεων, κ.λπ.
- Διεξαγωγή ενημερώσεων και τεχνικών εκπαιδεύσεων σε θέματα ασφάλειας ([DR03]), ώστε να διασφαλίζεται ότι οι τελικοί χρήστες και οι χρήστες υποστήριξης των συστημάτων γνωρίζουν τους κανόνες συμπεριφοράς και τις ευθύνες τους όσον αφορά στην προστασία της αποστολής του Οργανισμού.

5.1.4.2.2. Ανιχνευτικοί Διοικητικοί Έλεγχοι Ασφαλείας

Οι ανιχνευτικοί διοικητικοί έλεγχοι μπορεί να συνοψιστούν ως εξής:

- Υλοποίηση μηχανισμών ελέγχου ασφαλείας προσωπικού, όπως έλεγχος παρελθόντος, περιοδική αλλαγή καθηκόντων, κλπ.
- Διεξαγωγή περιοδικών επανεξετάσεων των ελέγχων ασφαλείας ώστε να διασφαλιστεί ότι παραμένουν αποτελεσματικοί.
- Εκτέλεση περιοδικών επιθεωρήσεων – ελέγχων συστήματος.
- Διεξαγωγή σε συνεχή βάση αξιολόγησης και διαχείρισης κινδύνων με στόχο το διαρκή περιορισμό τους.
- Απόφαση για συστημική αντιμετώπιση ενός τμήματος του εναπομένοντος κινδύνου και αποδοχή των υπολοίπων.

5.1.4.2.3. Διοικητικοί Έλεγχοι Αποκατάστασης Ασφαλείας

Οι έλεγχοι αυτοί συνίστανται στα ακόλουθα:

- Εξασφάλιση συνέχειας στην υποστήριξη ενός συστήματος καθώς επίσης και ανάπτυξη και συντήρηση πλάνου διασφάλισης της συνέχισης της λειτουργίας του Οργανισμού κατά τη διάρκεια έκτακτων αναγκών ή καταστροφών.
- Εγκαθίδρυση μηχανισμών και δομών αντίδρασης σε ανεπιθύμητα περιστατικά. Οι μηχανισμοί αυτοί πρέπει να περιλαμβάνουν προετοιμαστικές ενέργειες για ανεπιθύμητα συμβάντα, αναγνώριση των συμβάντων και αναφορά τους, αντιμετώπισή τους και την επιστροφή σε κατάσταση ομαλής λειτουργίας.

5.1.4.3. Λειτουργικοί Έλεγχοι Ασφαλείας

Η υλοποίηση και εφαρμογή λειτουργικών ελέγχων είναι απαραίτητη για τη διασφάλιση της ασφάλειας του Οργανισμού σε λειτουργικό επίπεδο. Για να

διασφαλιστεί η συνέπεια και η ομοιομορφία στις λειτουργίες ασφάλειας, πρέπει να ορίζονται σαφώς διαδικασίες και μέθοδοι για την σταδιακή υλοποίηση των λειτουργικών ελέγχων, καλά τεκμηριωμένες και τακτικά ενημερωμένες. Οι κύριες κατηγορίες λειτουργικών ελέγχων είναι οι προληπτικοί και οι ανιχνευτικοί και παρουσιάζονται στις ενότητες που ακολουθούν.

5.1.4.3.1. Προληπτικοί Λειτουργικοί Έλεγχοι Ασφαλείας

Οι προληπτικοί λειτουργικοί έλεγχοι περιλαμβάνουν τα εξής:

- Έλεγχο πρόσβασης και διάθεσης δεδομένων (π.χ. φυσικός έλεγχος πρόσβασης)
- Περιορισμό εξωτερικής διανομής των δεδομένων
- Έλεγχο για ιούς λογισμικού
- Εγκατάσταση μηχανισμών φύλαξης (π.χ. φύλακες, διαδικασίες πρόσβασης επισκεπτών, ηλεκτρονικές κάρτες πρόσβασης, έλεγχος βιομετρικών στοιχείων, κ.λπ.).
- Ασφαλείς χώρους φύλαξης της καλωδίωσης και του συναφούς εξοπλισμού.
- Δυνατότητα δημιουργίας αντιγράφων ασφαλείας (π.χ. διαδικασίες για την τακτική δημιουργία αντιγράφων ασφαλείας δεδομένων και συστήματος, διατήρηση των αρχείων που καταγράφουν τις δομικές αλλαγές στις βάσεις δεδομένων, κ.λπ.).
- Δημιουργία διαδικασιών αποθήκευσης και φύλαξης των αντιγράφων σε εξωτερικούς χώρους.
- Προστασία φορητών και προσωπικών υπολογιστών και σταθμών εργασίας.
- Προστασία εξοπλισμού ΙΤ από πυρκαγιά (π.χ. διαδικασίες για τη χρήση των πυροσβεστήρων, συστήματα αυτόματης κατάσβεσης, κ.λπ.).

- Εφεδρική παροχή ενέργειας (π.χ. απαιτήσεις αδιάλειπτης παροχής ενέργειας).
- Έλεγχο υγρασίας και θερμοκρασίας των εγκαταστάσεων (π.χ. λειτουργία κλιματιστικών).

5.1.4.3.2. Ανιχνευτικοί Λειτουργικοί Έλεγχοι Ασφαλείας

Οι ανιχνευτικοί λειτουργικοί έλεγχοι περιλαμβάνουν τα ακόλουθα:

- Παροχή φυσικής ασφάλειας (π.χ. χρήση ανιχνευτών κίνησης, κλειστά κυκλώματα παρακολούθησης, αισθητήρες, συναγερμοί, κ.λπ.).
- Διασφάλιση περιβαλλοντικής ασφάλειας (π.χ. χρήση ανιχνευτών καπνού και φωτιάς, αισθητήρων και συναγερμών).

5.1.5. Ανάλυση Κόστους - Οφέλους

Για την κατανομή των πόρων (υλικών και ανθρώπινων) και την υλοποίηση αποδοτικών και αποτελεσματικών ελέγχων, οι Οργανισμοί, μετά τον εντοπισμό όλων των δυνατών ελέγχων και την αξιολόγηση της εφικτότητας και της αποτελεσματικότητάς τους, θα πρέπει να προβαίνουν σε ανάλυση κόστους-οφέλους για κάθε προτεινόμενο έλεγχο για να καθορίσουν τελικά τους ελέγχους που θα υλοποιήσουν.

Η ανάλυση κόστους - οφέλους μπορεί να είναι ποιοτική ή ποσοτική. Στόχος της είναι να καταδείξει ότι το κόστος υλοποίησης των ελέγχων μπορεί να αιτιολογηθεί από τη μείωση του επιπέδου κινδύνου. Για παράδειγμα, είναι απόλυτα λογικό ένας Οργανισμός να μην επιθυμεί να ξοδέψει 10.000 Ευρώ για την υλοποίηση ενός ελέγχου, η εφαρμογή του οποίου θα οδηγήσει σε μείωση του κινδύνου η οποία αποτιμάται σε 1.000 Ευρώ. Μια ανάλυση κόστους-

οφέλους για τους προτεινόμενους νέους ελέγχους ή την ενίσχυση υφιστάμενων ελέγχων περιλαμβάνει τα ακόλουθα:

- Προσδιορισμό των επιπτώσεων της εφαρμογής των νέων ή των ενισχυμένων ελέγχων.
- Προσδιορισμό των επιπτώσεων της μη εφαρμογής των νέων ή των ενισχυμένων ελέγχων.
- Εκτίμηση του κόστους υλοποίησης. Το κόστος αυτό μπορεί να περιλαμβάνει επιμέρους κόστη, όπως:
    - Αγορά υλικού και λογισμικού.
    - Κόστη λόγω της επιδείνωσης της λειτουργικότητας και της επίδοσης του IT συστήματος λόγω των αυξημένων επιπέδων ασφάλειας.
    - Κόστος εφαρμογής συμπληρωματικών πολιτικών και διαδικασιών.
    - Κόστος πρόσληψης επιπλέον προσωπικού για την υλοποίηση των προτεινόμενων πολιτικών, διαδικασιών και υπηρεσιών.
    - Κόστη εκπαίδευσης.
    - Κόστη συντήρησης.
- Αξιολόγηση του κόστους υλοποίησης και των σχετικών επιπτώσεων καθώς επίσης και του οφέλους λαμβάνοντας υπόψη τη σημαντικότητα του συστήματος και την κρισιμότητα των δεδομένων για τον προσδιορισμό της αναγκαιότητας εφαρμογής των νέων ελέγχων για τον Οργανισμό.

Κάθε Οργανισμός θα πρέπει να αξιολογεί τα οφέλη των ελέγχων, πάντα σε σχέση με την αποστολή που έχει να επιτελέσει. Πρέπει να είναι σαφές για τον καθένα ότι, όπως ακριβώς υφίσταται ένα κόστος υλοποίησης ενός ελέγχου, έτσι υφίσταται και το αντίστοιχο κόστος μη υλοποίησής του. Συσχετίζοντας τα δυνητικά αποτελέσματα της μη εφαρμογής ενός ελέγχου με την αποστολή που ένας Οργανισμός έχει να επιτελέσει, οι Οργανισμοί μπορούν να εκτιμήσουν εάν

και κατά πόσο είναι εφικτό να συνεχίσουν να λειτουργούν χωρίς την υλοποίηση του ελέγχου αυτού.

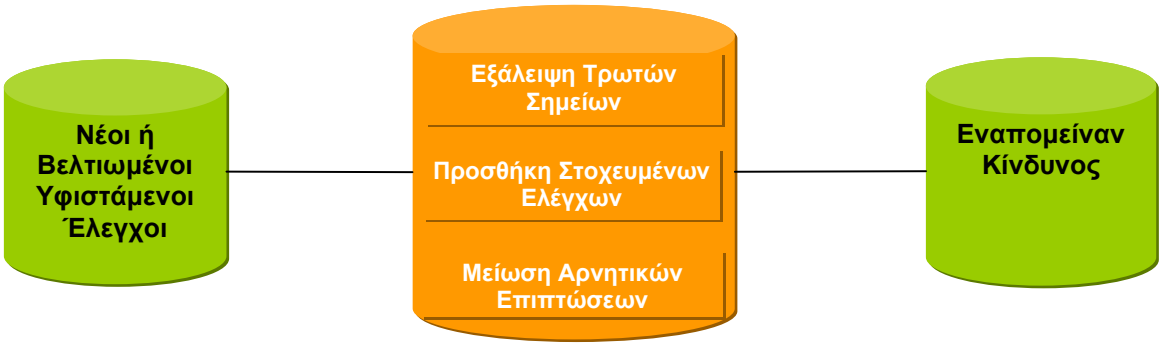
Ένα παράδειγμα ανάλυσης κόστους οφέλους παρατίθεται στη μελέτη περίπτωσης που ακολουθεί στην Ενότητα 7.

5.1.6. Εναπομείναντες Κίνδυνοι (Residual Risks)

Οι Οργανισμοί μπορούν να αναλύσουν την έκταση της μείωσης των κινδύνων που προκύπτει ως αποτέλεσμα της υλοποίησης νέων ή της βελτίωσης υφιστάμενων ελέγχων. Εν γένει, όπως ήδη έχουμε περιγράψει αναλυτικά στις προηγούμενες ενότητες, η εφαρμογή νέων και η βελτίωση των υφιστάμενων ελέγχων μπορεί να μετριάσει τον κίνδυνο μέσα από την:

- Εξάλειψη ορισμένων τρωτών σημείων του συστήματος, μειώνοντας έτσι τον αριθμό των δυνατών ζευγών πηγών απειλών/ αδυναμιών.
- Προσθήκη καλά στοχευμένων ελέγχων με στόχο τη μείωση της ικανότητας και των κινήτρων των πηγών απειλών. Για παράδειγμα, μια υπηρεσία του Οργανισμού εκτιμά ότι το κόστος για την εγκατάσταση και συντήρηση πρόσθετου λογισμικού ασφαλείας σε ένα PC, που αποθηκεύει ευαίσθητες πληροφορίες, είναι πολύ υψηλό, επομένως αντί αυτού θα πρέπει να υλοποιηθούν οι απαραίτητοι διαχειριστικοί και φυσικοί έλεγχοι για να καταστήσουν δυσκολότερη και περισσότερο ελεγχόμενη τη φυσική πρόσβαση σε αυτόν τον υπολογιστή (π.χ. αποθήκευση του PC σε ένα ασφαλέστερο χώρο, με αυστηρά ελεγχόμενη πρόσβαση).
- Μείωση του μεγέθους των αρνητικών επιπτώσεων.

Σχήμα 4: Υλοποιημένοι Έλεγχοι και Εναπομείναντες Κίνδυνοι



Η σχέση μεταξύ της υλοποίησης ελέγχων ([N02]) και των εναπομεινάντων κινδύνων παρουσιάζεται στο Σχήμα 4.

Ο κίνδυνος ο οποίος παραμένει μετά την υλοποίηση των νέων ή την ενίσχυση των υφιστάμενων ελέγχων είναι ο εναπομείναν κίνδυνος. Στην πράξη, κανένα πληροφοριακό σύστημα δεν είναι 100% ασφαλές και ακόμη και μετά την υλοποίηση των νέων ελέγχων δεν εξαλείφονται όλοι οι κίνδυνοι ασφάλειας ([S11]). Εάν μετά τις παρεμβάσεις περιορισμού των κινδύνων, ο εναπομείνας κίνδυνος δεν έχει μειωθεί σε αποδεκτό επίπεδο, ο κύκλος διαχείρισης των κινδύνων πρέπει να επαναληφθεί και να εντοπιστούν τρόποι περαιτέρω μείωσης του εναπομείναντος κινδύνου σε αποδεκτά επίπεδα.

6. Μελέτη Περίπτωσης – Διαχείριση IT Κινδύνων σε Τραπεζικό Οργανισμό

Στην Ενότητα αυτή παραθέτουμε μια μελέτη περίπτωσης για τη διαχείριση κινδύνων σε ένα Τραπεζικό Οργανισμό XYZ. Θα χρησιμοποιήσουμε τη μεθοδολογία που έχει προταθεί στην παρούσα εργασία, καταρχάς για να αξιολογήσουμε (assess) και εν συνεχεία για να περιορίσουμε (mitigate) τους κινδύνους. Τα βήματα που ακολουθούμε λοιπόν, σύμφωνα με την προτεινόμενη μεθοδολογία, είναι:

1. Αξιολόγηση Κινδύνων (Risk Assessment)
    - Χαρακτηρισμός Συστήματος
    - Προσδιορισμός Απειλών
    - Αναγνώριση Αδυναμιών
    - Ανάλυση Ελέγχων
    - Προσδιορισμός Πιθανοτήτων
    - Ανάλυση Επιπτώσεων
    - Προσδιορισμός των Κινδύνων
    - Συστάσεις Ελέγχων
    - Τεκμηρίωση Αποτελεσμάτων
2. Περιορισμός / Εξάλειψη Κινδύνων (Risk Mitigation)
    - Προτεραιοποίηση Ενεργειών / Δράσεων.
    - Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων.
    - Διεξαγωγή Ανάλυσης Κόστους – Οφέλους.
    - Επιλογή Ελέγχων.
    - Ανάθεση Αρμοδιοτήτων.
    - Ανάπτυξη Πλάνου Υλοποίησης Προστασίας.
    - Υλοποίηση Επιλεγμένων Ελέγχων.

Ακολουθεί αναλυτικά η περιγραφή του κάθε βήματος.

1. ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΩΝ

Στάδιο 1: Χαρακτηρισμός Συστήματος

Για να μπορέσουμε να διενεργήσουμε την αξιολόγηση κινδύνων στην Τράπεζα ΧΥΖ, καταρχάς διενεργήσαμε ένα αριθμό συνεντεύξεων, ανά σύστημα, ώστε να μπορέσουμε να αποκτήσουμε σημαντικές πληροφορίες για την τρέχουσα κατάσταση του Οργανισμού. Η Τράπεζα ΧΥΖ είχε 2 βασικά συστήματα Α και Β για τα οποία διενεργήθηκαν συνεντεύξεις. Οι ερωτήσεις των συνεντεύξεων και οι απαντήσεις ανά σύστημα μετά από την επεξεργασία ενός ικανοποιητικού αριθμού ερωτηματολογίων, παρατίθενται στον Πίνακα 9 που ακολουθεί.

Πίνακας 9:Ερωτηματολόγιο για τον χαρακτηρισμό συστημάτων της Τράπεζας ΧΨΖ

ΕΡΩΤΗΣΗ	**ΑΠΑΝΤΗΣΗ ΓΙΑ ΣΥΣΤΗΜΑ Α**	**ΑΠΑΝΤΗΣΗ ΓΙΑ ΣΥΣΤΗΜΑ Β**
1. Ποιοι είναι οι χρήστες του συστήματος;	Οι Διευθυντές και οι Υποδιευθυντές των καταστημάτων	Οι ταμίες των καταστημάτων
2. Ποια είναι η αποστολή των χρηστών μέσα στον Οργανισμό;	Παρακολούθηση στόχων και χαρτοφυλακίου καταστήματος, ανάπτυξη εργασιών	Διεκπεραίωση ταμειακών συναλλαγών
3.Ποιος είναι ο σκοπός του συστήματος σε σχέση με την αποστολή;	Υποστήριξη στοχοθεσίας και ανάπτυξης εργασιών	Εκτέλεση εγχρήματων συναλλαγών (καταθέσεις, αναλήψεις, μεταφορές, κ.α.)
4. Πόσο σημαντικό είναι το σύστημα με την αποστολή των χρηστών στον Οργανισμό;	Σημαντικό σε στρατηγικό και τακτικό επίπεδο	Πολύ σημαντικό σε λειτουργικό επίπεδο
5. Ποιες είναι οι απαιτήσεις για διαθεσιμότητα του συστήματος;	Τουλάχιστον 98%	Τουλάχιστον 99.5%
6. Ποιες είναι οι πληροφορίες (εισερχόμενες και εξερχόμενες) που απαιτούνται από τον Οργανισμό;	Πληροφορίες μεγεθών προϋπολογισμού και χαρτοφυλακίου καταστήματος, πληροφορίες	Πληροφορίες συναλλαγών (ημν/νία, ώρα, ποσό συναλλαγής, τύπος συναλλαγής, κ.α.)

	επαφών με πελάτες, κ.α.	
7. Τι πληροφορίες δημιουργούνται, καταναλώνονται, επεξεργάζονται, αποθηκεύονται και ανακτούνται από το σύστημα;	Προϋπολογισμός καταθέσεων, χορηγήσεων, δείκτες ποιότητας χαρτοφυλακίου	Υπόλοιπα λογαριασμών, καταθέσεις, αναλήψεις, μεταφορές, πληρωμές
8. Πόσο σημαντικές είναι οι πληροφορίες του συστήματος για την αποστολή του χρήστη στον Οργανισμό;	Πολύ σημαντικές	Πολύ σημαντικές
9. Ποιες είναι οι ροές των πληροφοριών του συστήματος;	Ανταλλάσει πληροφορίες με συστήματα planning και budgeting και με συστήματα contact management	Ανταλλάσει πληροφορίες με το κεντρικό τραπεζικό σύστημα
10. Τι είδους πληροφορίες επεξεργάζονται και αποθηκεύονται στο σύστημα (π.χ. Επιχειρησιακές και αν ναι για ποια επιχειρησιακή γραμμή, Οικονομικές, Προσωπικού);	Πληροφορίες προϋπολογισμού και παρακολούθησης και ανάπτυξης χαρτοφυλακίου καταστήματος	Τραπεζικές συναλλαγές πελατών
11. Πόσο ευαίσθητες είναι οι πληροφορίες και ποιο είναι το επίπεδο διαβάθμισης;	Ευαίσθητες και εμπιστευτικές (ισχύει το τραπεζικό απόρρητο)	Ευαίσθητες και εμπιστευτικές (ισχύει το τραπεζικό απόρρητο)
12. Ποιες από τις πληροφορίες που υπάρχουν στο σύστημα δεν πρέπει να γνωστοποιούνται και σε ποιον;	Προσωπικά δεδομένα πελατών σε άλλους πελάτες ή τρίτους, στοιχεία χαρτοφυλακίου σε υπαλλήλους του καταστήματος ή πελάτες	Στοιχεία τραπεζικών λογαριασμών και συναλλαγών σε οποιονδήποτε τρίτο
13. Που ακριβώς στο σύστημα επεξεργάζονται και αποθηκεύονται οι πληροφορίες;	Στην κατάλληλη για το σκοπό αυτό βάση δεδομένων	Στην κατάλληλη για το σκοπό αυτό βάση δεδομένων
14. Ποιος είναι ο πιθανός αντίκτυπος για τον Οργανισμό, αν οι πληροφορίες δημοσιοποιηθούν σε μη εξουσιοδοτημένο προσωπικό;	Σοβαρός (στοιχεία προϋπολογισμού στρατηγικής σημασίας και προσωπικά δεδομένα πελατών)	Πολύ σοβαρός (στοιχεία συναλλαγών που διέπονται από την προστασία τραπεζικού απορρήτου)
15. Ποιες είναι οι απαιτήσεις για τη διαθεσιμότητα και ακεραιότητα των πληροφοριών;	24 x 7 διαθεσιμότητα και πλήρη ακεραιότητα χωρίς προβλήματα	24 x 7 διαθεσιμότητα και πλήρη ακεραιότητα χωρίς προβλήματα
16. Ποια είναι η επίδραση στην αποστολή του	Τίθεται σε κίνδυνο η εφαρμογή της στρατηγικής	Τίθεται σε μεγάλο κίνδυνο η αξιοπιστία και η απρόσκοπτη

Οργανισμού, εάν το σύστημα ή πληροφορίες δεν είναι αξιόπιστες;	και η ανάπτυξη της τράπεζας	λειτουργία της Τράπεζας
17. Ποια είναι η μέγιστη «εκτός λειτουργίας» διάρκεια (downtime) του συστήματος που μπορεί να αντέξει ο Οργανισμός; Πώς συγκρίνεται αυτός ο χρόνος με το μέσο χρόνο επισκευής/ αποκατάστασης;	4ώρες. Είναι μικρότερος από το μέγιστο χρόνο αποκατάστασης (2 ώρες)	2 ώρες Είναι μικρότερος από το μέγιστο χρόνο αποκατάστασης (1.5 ώρες)
18. Σε τι άλλες λειτουργίες ή επιλογές επικοινωνίας έχουν πρόσβαση οι χρήστες;	Σε άλλες εφαρμογές εξυπηρέτησης πελατών, σε τηλεφωνικά δίκτυα και internet.	Σε καμία άλλη λειτουργία πλην τηλεφωνικής επικοινωνίας
19. Θα μπορούσε μια δυσλειτουργία ή μη διαθεσιμότητα του συστήματος να θέσει σε κίνδυνο ανθρώπινη ζωή;	Όχι	Όχι

Στάδιο 2: Προσδιορισμός Απειλών

Μετά τη συλλογή των στοιχείων με χρήση του ερωτηματολογίου στο Πίνακα 9, προχωρήσαμε στο Στάδιο 2, στο οποίο καταγράφηκαν οι απειλές. Η αναφορά απειλών (threat statement) παρατίθεται στον παρακάτω Πίνακα 10:

Πίνακας 10: Αναφορά απειλών της Τράπεζας ΧΨΖ

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΚΙΝΗΤΡΑ**	**ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ**
1. Εισβολείς (Hackers/ Crackers)	Πρόκληση, εγωισμός, αυτοεπιβεβαίωση	Επιθετική εισβολή (Hacking), Κοινωνική μηχανική (Social engineering), Παραβίαση συστήματος (System intrusion), Μη εξουσιοδοημένη πρόσβαση
2. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	Απόσπαση ή/και παράνομη δημοσιοποίηση πληροφοριών, Χρηματικό όφελος, Μη εξουσιοδοτημένη αλλοίωση δεδομένων	Ηλεκτρονικό έγκλημα, Απάτη (fraud), Πλαστογράφηση πληροφορίας, Παραβίαση συστήματος
3. Βιομηχανική κατασκοπία (εταιρίες,	Ανταγωνιστικό πλεονέκτημα, Οικονομική κατασκοπία	Οικονομική εκμετάλλευση, Κλοπή πληροφοριών, Παραβίαση προσωπικής ιδιοκτησίας, Κοινωνική μηχανική,

κυβερνήσεις, κλπ.)		Εισβολή στο σύστημα, Μη εξουσιοδοτημένη πρόσβαση
4. Εχθροί «εκ των έσω» (ελλιπώς εκπαιδευμένοι, δυσαρεστημένοι, εχθρικοί, απρόσεκτοι, δόλιοι, απολυμένοι)	Περιέργεια, Εγωισμός, Ευφυΐα, Οικονομικά οφέλη, Εκδίκηση, Ακούσια λάθη και παραλήψεις	Επίθεση σε εργαζόμενο, Εκβιασμός, Αναζήτηση περιουσιακών πληροφοριών, Παράνομη χρήση συστήματος, Απάτη, Κλοπή, Πλαστογράφηση πληροφοριών, Εισαγωγή ψευδών δεδομένων, Interception, Εχθρικά προγράμματα, Πώληση προσωπικών πληροφοριών, σφάλματα (bugs) συστήματος, Εισβολή στο σύστημα, σαμποτάζ, Μη εξουσιοδοτημένη πρόσβαση

Στάδιο 3: Αναγνώριση Αδυναμιών

Ο Πίνακας 11 παρουσιάζει τα ζεύγη αδυναμιών / απειλών ανά σύστημα που είναι το αποτέλεσμα αυτού του σταδίου.

Πίνακας 11: Απειλές/ Αδυναμίες της Τράπεζας ΧΨΖ ανά σύστημα

ΑΠΕΙΛΗ	**ΑΔΥΝΑΜΙΑ ΣΥΣΤΗΜΑΤΟΣ Α**	**ΑΔΥΝΑΜΙΑ ΣΥΣΤΗΜΑΤΟΣ Β**
1. Απολυμένοι εργαζόμενοι	Οι προσβάσεις απολυμένων εργαζόμενων δεν αφαιρούνται από το σύστημα	-
2. Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Κενά ασφάλειας στο σύστημα που έχουν εντοπιστεί αλλά δεν έχουν ακόμη επιλυθεί από τους προμηθευτές συστημάτων	Κενά ασφάλειας στο σύστημα που έχουν εντοπιστεί αλλά δεν έχουν ακόμη επιλυθεί από τους προμηθευτές συστημάτων
3. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	-	Κενά στη διαδικασία ελέγχου απάτης (έλεγχος πλαστογραφίας)

Στάδιο 4: Ανάλυση Ελέγχων

Κατά το στάδιο αυτό προέκυψε μια λίστα των υφιστάμενων ελέγχων που χρησιμοποιούνται ανά IT σύστημα, με στόχο την ελαχιστοποίηση των

πιθανοτήτων πραγματοποίησης μιας απειλής και τη μείωση των επιπτώσεων ενός τέτοιου δυσμενούς γεγονότος. Οι έλεγχοι αυτό παρατίθενται ανά σύστημα στους Πίνακες 12a και 12b.

Πίνακας 12a: Σύστημα Α - Έλεγχοι που ήδη εφαρμόζονται

ΥΦΙΣΤΑΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΟΣ Α
1. Απενεργοποίηση δυνατότητας πρόσβασης υπαλλήλων της Τράπεζας που δεν είναι Διευθυντές ή Υποδιευθυντές.
2. Υποχρεωτική αλλαγή κωδικών ασφαλείας από τους χρήστες κάθε 3 μήνες.
3. Πρόσβαση μόνο από σύστημα που ανήκει στο δίκτυο (intranet) της τράπεζας.
4. Έλεγχος προστασίας από ιούς.

Πίνακας 12b: Σύστημα Β - Έλεγχοι που ήδη εφαρμόζονται

ΥΦΙΣΤΑΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΟΣ Β
1. Απενεργοποίηση δυνατότητας πρόσβασης υπαλλήλων της Τράπεζας που δεν είναι ταμίες.
2. Υποχρεωτική αλλαγή κωδικών ασφαλείας από τους χρήστες κάθε 2 μήνες.
3. Πρόσβαση μόνο από σύστημα που ανήκει στο δίκτυο καταστημάτων της τράπεζας.
4. Έλεγχος προστασίας από ιούς.
5. Άμεση απενεργοποίηση κωδικών εργαζόμενων που παραιτούνται από την τράπεζα.

Στάδιο 5: Προσδιορισμός Πιθανοτήτων

Στο στάδιο αυτό χαρακτηρίστηκαν οι πιθανότητες ενεργοποίησης κάποιας απειλής. Ο χαρακτηρισμός έγινε για τα δύο συστήματα Α και Β και παρατίθεται στον Πίνακα 13.

Πίνακας 13: Προσδιορισμός πιθανοτήτων

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΔΙΑΒΑΘΜΙΣΗ ΠΙΘΑΝΟΤΗΤΑΣ ΣΥΣΤΗΜΑ Α**	**ΔΙΑΒΑΘΜΙΣΗ ΠΙΘΑΝΟΤΗΤΑΣ ΣΥΣΤΗΜΑ Β**
1. Απολυμένοι εργαζόμενοι	Υψηλή	-
2. Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Μέτρια	Υψηλή
3. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	-	Μέτρια

Στάδιο 6: Ανάλυση Επιπτώσεων

Στο στάδιο αυτό χαρακτηρίστηκαν οι επιπτώσεις ενεργοποίησης κάποιας απειλής. Ο χαρακτηρισμός έγινε για τα δύο συστήματα Α και Β και παρατίθεται στον Πίνακα 14.

Πίνακας 14: Διαβάθμιση Αντίκτυπου

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΔΙΑΒΑΘΜΙΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΥΣΤΗΜΑ Α**	**ΔΙΑΒΑΘΜΙΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΥΣΤΗΜΑ Β**
1. Απολυμένοι εργαζόμενοι	Χαμηλός	-
2. Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Μέτριος	Υψηλός
3. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	-	Υψηλός

Στάδιο 7: Προσδιορισμός των Κινδύνων

Στο στάδιο αυτό διαβαθμίστηκε ο κίνδυνος που προξενεί κάθε απειλή. Χρησιμοποιήθηκαν οι Πίνακες των Σταδίων 5 και 6 (Πίνακες 13 και 14) και ο Πίνακας 7 που συσχετίζει πιθανότητες – αντίκτυπο. Ο προσδιορισμός έγινε και για τα δύο συστήματα Α και Β και παρατίθεται στον Πίνακα 15.

Πίνακας 15: Διαβάθμιση Κινδύνου

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΔΙΑΒΑΘΜΙΣΗ ΚΙΝΔΥΝΟΥ ΣΥΣΤΗΜΑ Α**	**ΔΙΑΒΑΘΜΙΣΗ ΚΙΝΔΥΝΟΥ ΣΥΣΤΗΜΑ Β**
1. Απολυμένοι εργαζόμενοι	Χαμηλός (0.5)	-
2. Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Μέτριος (2)	Υψηλός (25)
3. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	-	Μέτριος (10)

Είναι σκόπιμο εδώ να σημειώσουμε ότι η τελική διαβάθμιση που προκύπτει είναι άμεση συνάρτηση των επιμέρους διαβαθμίσεων της πιθανότητας κινδύνου

και του αντίκτυπου των απειλών. Με βάση τις κλίμακες και τα scores που έχουν προταθεί στο κύριο μέρος της εργασίας, προκύπτει το score ανά κίνδυνο και ανά σύστημα (βαθμός εντός παρενθέσεως) και ο τελικός χαρακτηρισμός των κινδύνων τριών κινδύνων που εξετάζονται (Υψηλός, Μέτριος και Χαμηλός στη συγκεκριμένη περίπτωση).

Στάδιο 8: Συστάσεις Ελέγχων

Σε αυτό το στάδιο της διαδικασίας, προτάθηκαν οι έλεγχοι που θα μπορούσαν να μετριάσουν ή να εξαλείψουν τους κινδύνους που εντοπίστηκαν. Οι ακόλουθοι παράγοντες λήφθηκαν υπόψη για να είναι όσο το δυνατό πληρέστερη η πρόταση ελέγχων:

- Εφικτότητα των προτεινόμενων επιλογών (π.χ. συμβατότητα του συστήματος).
- Νομοθεσία και κανονιστικές διατάξεις.
- Πολιτική του Οργανισμού.
- Λειτουργικές επιπτώσεις.
- Ασφάλεια και αξιοπιστία.

Οι έλεγχοι αυτοί παρουσιάζονται στους Πίνακες 16a και 16b για τα συστήματα Α και Β αντίστοιχα.

Πίνακας 16a: Σύστημα Α - Προτεινόμενοι Έλεγχοι

ΠΡΟΤΕΙΝΟΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΟΣ Α
1. Απενεργοποίηση δυνατότητας πρόσβασης απολυμένων Διευθυντών και Υποδιευθυντών.
2. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).

Πίνακας 16b: Σύστημα Β - Προτεινόμενοι Έλεγχοι

ΠΡΟΤΕΙΝΟΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΟΣ Β
1. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).
2. Ενίσχυση διαδικασιών ανίχνευσης απάτης με έλεγχο επιβεβαίωσης υπογραφής από δύο υπαλλήλους όταν πρόκειται για συναλλαγές αξίας μεγαλύτερης των 1.500 Ευρώ

Στάδιο 9: Τεκμηρίωση Αποτελεσμάτων

Αφού η αξιολόγηση κινδύνων έχει ολοκληρωθεί (προσδιορισμός πηγών απειλής και τρωτών σημείων, αξιολόγηση κινδύνων και πρόταση ελέγχων), τα αποτελέσματα της όλης διαδικασίας τεκμηριώθηκαν σε μια επίσημη έκθεση αξιολόγησης κινδύνων ώστε να βοηθηθούν τα ανώτερα διευθυντικά στελέχη της Τράπεζας, στη λήψη αποφάσεων σχετικά με την πολιτική περιορισμού των κινδύνων που θα ακολουθήσουν. Η δομή της εν λόγω έκθεσης παρουσιάζεται στον Πίνακα 17.

Πίνακας 17: Δομή Έκθεσης Αξιολόγησης Κινδύνων

ΕΚΘΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΩΝ
Εκτελεστική Σύνοψη I. Εισαγωγή • Σκοπός • Πεδίο εφαρμογής/ εμβέλεια της αξιολόγησης κινδύνων II. Τρόπος/ Μεθοδολογία εκτίμησης κινδύνων • Οι συμμετέχοντες (π.χ. τα μέλη της ομάδας αξιολόγησης κίνδυνων) • Η τεχνικές που χρησιμοποιούνται για τη συλλογή πληροφοριών (π.χ. χρήση εργαλείων, ερωτηματολόγια) • Η ανάπτυξη και περιγραφή της κλίμακας κινδύνων. III. Χαρακτηρισμός Συστημάτων Χαρακτηρισμός συστήματων, συμπεριλαμβανομένου του υλικού, λογισμικού, διεπαφών, δεδομένων και χρηστών. IV. Αναφορά Απειλών Δημιουργία αναφοράς των δυνητικών απειλών και δράσεων που εφαρμόζονται στο υπό αξιολόγηση σύστημα. V. Αποτέλεσμα της διαδικασίας αξιολόγησης κινδύνων Κατάλογος παρατηρήσεων - ζευγών αδυναμίας / απειλής. Κάθε παρατήρηση πρέπει να περιλαμβάνει:

• Μια σύντομη περιγραφή της παρατήρησης
• Ένα σχολιασμό για κάθε ζεύγος αδυναμίας / απειλής
• Προσδιορισμό των υφισταμένων ελέγχων περιορισμού των κινδύνων
• Σχολιασμό και αποτίμηση πιθανοτήτων (υψηλή, μέτρια, χαμηλή πιθανότητα)
• Σχολιασμό και αποτίμηση των επιπτώσεων (υψηλή, μέτρια, χαμηλή)
• Διαβάθμιση Κινδύνου (υψηλός, μέτριος, χαμηλός)
• Προτεινόμενοι έλεγχοι ή εναλλακτικές επιλογές για τη μείωση του κινδύνου.

VI. Περίληψη

Συνοψίζονται οι παρατηρήσεις, τα αντίστοιχα επίπεδα κινδύνου, οι συστάσεις - προτάσεις και οποιαδήποτε τυχόν σχόλια διευκολύνουν την εφαρμογή των προτεινόμενων ελέγχων κατά τη διάρκεια της διαδικασίας περιορισμού των κινδύνων.

Συνοψίζοντας, αυτό που προκύπτει από την αξιολόγηση κινδύνου είναι ότι τα συστήματα Α και Β του Οργανισμού XYZ είναι εκτεθειμένα σε 3 κινδύνους, εκ των οποίων ο σημαντικότερος είναι η επίθεση από μη εξουσιοδοτημένους χρήστες (Μέτριος κίνδυνος για το Σύστημα Α και Υψηλός για το Σύστημα Β). Πέραν του ποιοτικού χαρακτηρισμού, παρέχεται και το score διαβάθμισης κάθε κινδύνου (10 και 25 αντίστοιχα για τα Συστήματα Α και Β για τον εν λόγω κίνδυνο). Επίσης, οι ηλεκτρονικοί εγκληματίες αποτελούν πηγή απειλής μόνο για το Σύστημα Β (Διαβάθμιση Κινδύνου: Μέτριος, score 10), ενώ οι απολυμένοι εργαζόμενοι αποτελούν κίνδυνο Χαμηλής διαβάθμισης (score 0.5) μόνο για το σύστημα Α. Μ' άλλα λόγια πρόκειται **για κινδύνους εισβολής στα συστήματα**, οι οποίοι μπορούν να θέσουν σε αμφισβήτηση τη δυνατότητα εκπλήρωσης της αποστολής του Οργανισμού.

Αξίζει να σημειωθεί ότι οι κίνδυνοι αυτοί καθώς επίσης και οι προτεινόμενοι για την αντιμετώπισή τους έλεγχοι, είναι τα βασικότερα σημεία του risk assessment που διενεργείται γιατί αποτελούν τη βάση για το επόμενο τμήμα της μεθόδου (risk mitigation) που περιγράφεται παρακάτω και στο οποίο τελικά αποφασίζονται και υλοποιούνται οι δράσεις περιορισμού/ εξάλειψης των κινδύνων εκείνων που αποτελούν σοβαρή απειλή για την εύρυθμη λειτουργία της Τράπεζας XYZ.

2. ΠΕΡΙΟΡΙΣΜΟΣ/ ΕΞΑΛΕΙΨΗ ΚΙΝΔΥΝΩΝ

Στάδιο 1: Προτεραιοποίηση Ενεργειών/ Δράσεων.

Στο στάδιο αυτό έγινε για την Τράπεζα ΧΨΖ η διαβάθμιση των προτεραιοτήτων των ενεργειών/ δράσεων με βάση το επίπεδο κινδύνου και τους πόρους που απαιτούνται για την υλοποίηση κάθε ελέγχου. Τα αποτελέσματα παρατίθενται, και για τα δύο συστήματα, στον Πίνακα 18.

Πίνακας 18: Διαβάθμιση Προτεραιότητας Ενεργειών/ Δράσεων

ΠΡΟΤΕΙΝΟΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΩΝ Α ΚΑΙ Β	**ΠΡΟΤΕΡΑΙΟΤΗΤΑ**
Α1. Απενεργοποίηση δυνατότητας πρόσβασης απολυμένων Διευθυντών και Υποδιευθυντών.	Χαμηλή
Α2. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Μέτρια
Β1. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Υψηλή
Β2. Ενίσχυση διαδικασιών ανίχνευσης απάτης με έλεγχο επιβεβαίωσης υπογραφής από δύο υπαλλήλους όταν πρόκειται για συναλλαγές αξίας μεγαλύτερης των 1.500 Ευρώ.	Υψηλή

Προκύπτει από το στάδιο αυτό, ότι η προτεραιότητα αντιμετώπισης των υφιστάμενων κινδύνων είναι Υψηλή για το Σύστημα Β και για τους δύο ελέγχους που έχουν προταθεί (Β1 και Β2) και Μέτρια ή Χαμηλή για το Σύστημα Α (Μέτρια για τον έλεγχο Α2 και Χαμηλή για τον Α1).

Στάδιο 2: Αξιολόγηση Επιλογών Προτεινόμενων Ελέγχων.

Κατά τη διάρκεια αυτού του σταδίου, αναλύθηκε η εφικτότητα (π.χ. συμβατότητα με υφιστάμενους ελέγχους και συστήματα, αποδοχή από τους χρήστες) και η αποτελεσματικότητα (π.χ. ο βαθμός προστασίας και το επίπεδο περιορισμού του κινδύνου) των προτεινόμενων επιλογών ελέγχου. Τα αποτελέσματα της αξιολόγησης παρατίθενται στον Πίνακα 19.

Πίνακας 19: Κατάλογος Εφικτών (Feasible) Ελέγχων.

ΠΡΟΤΕΙΝΟΜΕΝΟΙ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΩΝ Α ΚΑΙ Β	**ΕΦΙΚΤΟΤΗΤΑ**
Α1. Απενεργοποίηση δυνατότητας πρόσβασης απολυμένων Διευθυντών και Υποδιευθυντών.	Υψηλή
Α2. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Υψηλή
Β1. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Υψηλή
Β2. Ενίσχυση διαδικασιών ανίχνευσης απάτης με έλεγχο επιβεβαίωσης υπογραφής από δύο υπαλλήλους όταν πρόκειται για συναλλαγές αξίας μεγαλύτερης των 1.500 Ευρώ.	Χαμηλή

Στάδιο 3: Διεξαγωγή Ανάλυσης Κόστους – Οφέλους.

Στο στάδιο αυτό διεξάγουμε μια ανάλυση κόστους-οφέλους για τους προτεινόμενους ελέγχους της Τράπεζας XYZ. Τα αποτελέσματα της εν λόγω ανάλυσης παρατίθενται αναλυτικά για τον έλεγχο Α1 στον Πίνακα 20.

Πίνακας 20: Ανάλυση Κόστους – Οφέλους για τον Έλεγχο Α1.

Α1. Απενεργοποίηση δυνατότητας πρόσβασης απολυμένων Διευθυντών και Υποδιευθυντών.	
Αντίκτυπος υλοποίησης του ελέγχου	Η Διοίκηση του Οργανισμού θα έχει πλήρη έλεγχο στο ποιος έχει πρόσβαση σε στοιχεία κρίσιμα για τη στρατηγική και την ανάπτυξη της Τράπεζας και η διαρροή προς τρίτους περιορίζεται σημαντικά.
Αντίκτυπος μη υλοποίησης του ελέγχου	Η Διοίκηση του Οργανισμού δεν έχει τον πλήρη έλεγχο στο ποιος έχει πρόσβαση σε στοιχεία κρίσιμα για τη στρατηγική και την ανάπτυξη της Τράπεζας και η διαρροή προς τρίτους είναι πιθανή αν κάποιος πρώην Διευθυντής ή Υποδιευθυντής βρει τρόπο να εισχωρήσει στο σύστημα.
Εκτίμηση κόστους υλοποίησης του ελέγχου	• **500 Ευρώ:** Αγορά σχετικού υλικού και λογισμικού. • **5.000 Ευρώ ανά έτος:** Κόστος επιπλέον ενασχόλησης του προσωπικού για την υλοποίηση του εν λόγω ελέγχου.

	• **200 Ευρώ ανά έτος:** Κόστος συντήρησης του λογισμικού. ***Συνολικό Κόστος: 500 Ευρώ εφάπαξ και 5.200 Ευρώ ανά έτος***
Αντίκτυπος στην αποστολή της Τράπεζας	Ο έλεγχος είναι καλό να υπάρχει καθώς μειώνει σημαντικά το σχετικό ρίσκο, όμως δεν προσφέρει σημαντικά οφέλη στην Τράπεζα, καθώς ποτέ μέχρι τώρα δεν έχει δημιουργηθεί πρόβλημα, ενώ τα στοιχεία του συστήματος Α είναι μεν εμπιστευτικά, όχι όμως κρίσιμα για τη λειτουργία της Τράπεζας.

Η παραπάνω ανάλυση κόστους – οφέλους, πραγματοποιήθηκε και για τους άλλους τρεις ελέγχους που προτάθηκαν.

Στάδιο 4: Επιλογή Ελέγχων.

Αξιοποιώντας τα αποτελέσματα της ανάλυσης κόστους-οφέλους που διενεργήσαμε στο προηγούμενο στάδιο, η Διοίκηση της Τράπεζας ΧΥΖ επέλεξε την εφαρμογή εκείνων των ελέγχων οι οποίοι είναι υψηλότερης αξίας με βάση την ανάλυση κόστους-οφέλους που έχει διενεργηθεί. Οι έλεγχοι που επιλέχθηκαν παρατίθενται στον Πίνακα 21.

Πίνακας 21: Έλεγχοι προς Υλοποίηση.

ΠΡΟΣ ΥΛΟΠΟΙΗΣΗ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΩΝ Α ΚΑΙ Β
Α2. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).
Β1. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).
Β2. Ενίσχυση διαδικασιών ανίχνευσης απάτης με έλεγχο επιβεβαίωσης υπογραφής από δύο υπαλλήλους όταν πρόκειται για συναλλαγές αξίας μεγαλύτερης των 1.500 Ευρώ.

Στάδιο 5: Ανάθεση Αρμοδιοτήτων.

Κατά το στάδιο αυτό, εντοπίστηκαν τα κατάλληλα άτομα (υπάλληλοι του Οργανισμού ή εξωτερικοί συνεργάτες) που έχουν την απαιτούμενη κατάρτιση, εμπειρία και τα απαραίτητα προσόντα για να υλοποιήσουν τους επιλεγμένους ελέγχους και τους ανατέθηκαν οι σχετικές αρμοδιότητες. Στον Πίνακα 22 καταγράφεται ο κατάλογος των αρμοδίων.

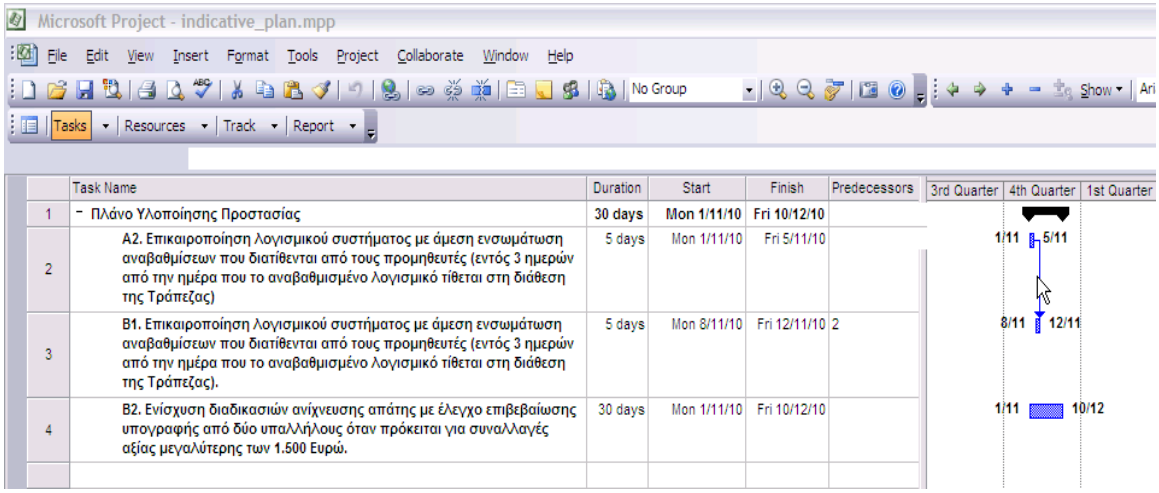
Πίνακας 22: Κατάλογος Αρμοδίων.

ΠΡΟΣ ΥΛΟΠΟΙΗΣΗ ΕΛΕΓΧΟΙ ΣΥΣΤΗΜΑΤΩΝ Α ΚΑΙ Β	**ΑΡΜΟΔΙΟΙ**
Α2. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Υπεύθυνος ενημερώσεων λογισμικού συστημάτων
Β1. Επικαιροποίηση λογισμικού συστήματος με άμεση ενσωμάτωση αναβαθμίσεων που διατίθενται από τους προμηθευτές (εντός 3 ημερών από την ημέρα που το αναβαθμισμένο λογισμικό τίθεται στη διάθεση της Τράπεζας).	Υπεύθυνος ενημερώσεων λογισμικού συστημάτων
Β2. Ενίσχυση διαδικασιών ανίχνευσης απάτης με έλεγχο επιβεβαίωσης υπογραφής από δύο υπαλλήλους όταν πρόκειται για συναλλαγές αξίας μεγαλύτερης των 1.500 Ευρώ.	Υπάλληλος Τμήματος Εσωτερικού Ελέγχου και Εξωτερικός Σύμβουλος

Στάδιο 6: Ανάπτυξη Πλάνου Υλοποίησης Προστασίας.

Κατά τη διάρκεια αυτού του σταδίου, αναπτύξαμε το πλάνο υλοποίησης μηχανισμών προστασίας, το οποίο προτεραιοποιεί τις ενέργειες/ δράσεις και τα επιμέρους έργα που απαιτούνται και θέτει ημερομηνίες έναρξης και ολοκλήρωσης. Το πλάνο αυτό παρατίθεται στο Σχήμα 5 και για τη δημιουργία του μπορούν να χρησιμοποιηθούν ειδικά εργαλεία διαχείρισης έργων (π.χ. MS Project).

Σχήμα 5: Πλάνο Υλοποίησης Προστασίας



Πρόκειται για 3 βασικά tasks, συγκεκριμένης χρονικής διάρκειας, με αρχική και τελική ημερομηνία εκτέλεσης του καθενός, και προαπαιτούμενα (predecessors) για κάθε task όπου υπάρχουν (π.χ. για να ξεκινήσει το B1 πρέπει να έχει ολοκληρωθεί το A2). Το προτεινόμενο Πλάνο Υλοποίησης Προστασίας, υλοποιεί το σχέδιο δράσης και τους επιμέρους ελέγχους που έχουν αποφασιστεί κατά τη διαδικασία του risk mitigation.

Στάδιο 7: Υλοποίηση Επιλεγμένων Ελέγχων.

Στο στάδιο αυτό υλοποιούνται οι προτεινόμενοι έλεγχοι. Οι κίνδυνοι που παραμένουν (residual risks) παρουσιάζονται στον Πίνακα 23.

Πίνακας 23: Εναπομείναντες Κίνδυνοι

ΠΗΓΗ ΑΠΕΙΛΗΣ	**ΣΥΣΤΗΜΑ Α**	**ΣΥΣΤΗΜΑ Β**
1. Απολυμένοι εργαζόμενοι	Χαμηλός (0.5)	-
2. Μη εξουσιοδοτημένοι χρήστες όπως εισβολείς (hackers), ευφυείς εργαζόμενοι, τρομοκράτες, ηλεκτρονικοί εγκληματίες	Χαμηλός (0.5)	Χαμηλός (1)
3. Ηλεκτρονικοί Εγκληματίες (Computer Criminals)	-	Χαμηλός (1)

Στον παραπάνω Πίνακα παρουσιάζεται η διαβάθμιση των κινδύνων ανά Σύστημα, μετά τις παρεμβάσεις που αποφασίστηκαν και υλοποιήθηκαν κατά τη διαδικασία του Risk Mitigation. Αξίζει να σημειώσουμε ότι οι έλεγχοι που υλοποιήθηκαν έχουν μειώσει σημαντικά τους κινδύνους εισβολής από μη εξουσιοδοτημένους χρήστες (score 0.5 και 1 αντίστοιχα για τα Συστήματα Α και

Β από 2 και 25 που ήταν αρχικά) και score 1 για τον κίνδυνο ηλεκτρονικού εγκλήματος για το Σύστημα Β από 10 που ήταν αρχικά. Παρ' όλα αυτά αξίζει να σημειωθεί ότι δεν έχουμε πλήρη εξάλειψη των κινδύνων αλλά σημαντική μείωσή τους.

Θα πρέπει με την ολοκλήρωση του case study να τονίσουμε για μια ακόμη φορά, πως **η διαχείριση κινδύνων είναι σημαντική και ωφέλιμη όταν συνδέεται άμεσα με την επιχειρησιακή διαδικασία του Οργανισμού**. Η προσέγγισή μας στην παρούσα μελέτη περίπτωσης ήταν τέτοια, ώστε ξεκινώντας από το business της Τράπεζας και από τις ανάγκες και τους κινδύνους των εργαζόμενων της πρώτης γραμμής (διευθυντές, ταμίες καταστημάτων), να καταλήξουμε στο πώς οι ανάγκες αυτές συνδέονται με IT κινδύνους. Επιπλέον, ανάλογα με τη φύση του κινδύνου αξιολογήσαμε τις πιθανότητες εμφάνισης συμβάντος αλλά και τις επιπτώσεις που αυτό θα είχε, όχι στο IT του Οργανισμού, αλλά στην επιχειρησιακή του συνέχεια και στην εκπλήρωση της αποστολής του. Με βάση την αξιολόγηση αυτή αποφασίστηκαν διορθωτικές ενέργειες και περιορίστηκαν τελικά οι δυνητικοί IT κίνδυνοι και κατά συνέπεια οι επιχειρηματικοί κίνδυνοι.

7. Ανοιχτά Ζητήματα και Μελλοντικές Κατευθύνσεις

Οι ευρύτεροι κίνδυνοι που αντιμετωπίζει ένας Οργανισμός και οι αβεβαιότητες που κυριαρχούν στο παγκόσμιο επιχειρηματικό περιβάλλον σε συνδυασμό με την ανάγκη για άμεση λήψη αποφάσεων και αντιμετώπιση κινδύνων, οδηγούν σταδιακά τον τομέα διαχείρισης των τεχνολογικών κινδύνων στην κατεύθυνση της ολοκληρωμένης «ευφυούς αντιμετώπισης κινδύνων» (risk intelligence). Ταυτόχρονα, η πρόοδος που συντελείται στον τομέα της διαχείρισης τεχνολογικών κινδύνων, είναι ιδιαίτερα σημαντική και κινείται προς δύο κατευθύνσεις:

1. Συνολική αντιμετώπιση του τεχνολογικού κινδύνου σε όλο το εύρος του Οργανισμού (επιμέρους κλάδοι, διευθύνσεις, υποκαταστήματα, θυγατρικές, κ.λπ.). Αυτό σημαίνει πως συγκεντρώνονται οι έλεγχοι σε κεντρικά σημεία και καλύπτουν σε όσο το δυνατό μεγαλύτερη έκταση τον Οργανισμό, επιτυγχάνοντας έτσι οικονομίες κλίμακας και περισσότερο πλήρεις και αποτελεσματικούς ελέγχους.
2. Συγκέντρωση ελέγχων που αναφέρονται σε πολλαπλούς και διαφορετικούς τύπους κινδύνου (τεχνολογικοί, οικονομικοί, νομικοί, κ.λπ.) σε κεντρικές εφαρμογές, οι οποίες καλύπτουν με ενιαίο τρόπο πολλούς επιμέρους τύπους κινδύνου ταυτόχρονα.

Μία άλλη σημαντική τάση, η οποία επίσης υποστηρίζεται από ανάπτυξη σύγχρονων εργαλείων και εφαρμογών, είναι η αναλυτική επεξεργασία και παραγωγή αναφορών (risk analytics and reporting). Για την υποστήριξη αυτών των δυνατοτήτων απαιτείται η επεξεργασία τεράστιου όγκου πληροφοριών και υπολογιστική ισχύς, ενώ ο βασικός στόχος της εν λόγω ανάλυσης είναι ο εντοπισμός πιθανών παραβιάσεων και ύποπτων συμπεριφορών. Οι εφαρμογές αυτές μπορούν να αποτελέσουν σημαντικά εργαλεία υποστήριξης αποφάσεων για τη Διοίκηση του Οργανισμού ή να ικανοποιήσουν αιτήματα πληροφόρησης των ελεγκτών του Οργανισμού (regulators). Μάλιστα η υφιστάμενη τεχνολογική ισχύς, επιτρέπει οι αναλύσεις αυτές να γίνονται ακόμη και σε πραγματικό χρόνο.

Ένας άλλος σημαντικός «ανοιχτός τομέας στον οποίο συντελείται πρόοδος, είναι η δημιουργία σε ολοένα και περισσότερους Οργανισμούς, ρόλων που έχουν τη γενική εποπτεία των πληροφοριών που χρησιμοποιούνται (Information governors ή data stewards). Πρόκειται προφανώς για παρέμβαση σε οργανωτικό και όχι σε τεχνολογικό επίπεδο, αν και το προσωπικό που θα αναλάβει το ρόλο αυτό πρέπει να έχει και τεχνολογικό υπόβαθρο ([LKA]). Ο «επόπτης πληροφοριών», επωμίζεται και μια σειρά από αρμοδιότητες που συμβάλλουν στην ευθυγράμμιση και ενοποίηση των συστημάτων του Οργανισμού, αυτοματοποιώντας και κεντροποιώντας ελέγχους.

Σε κάθε περίπτωση, γίνεται ολοένα και περισσότερο αντιληπτό, πως η ολοκληρωμένη διαχείριση IT κινδύνων δεν αποτελεί αμιγώς τεχνολογική εργασία και επομένως πρέπει να προσεγγίζεται από τους Οργανισμούς ευρύτερα ([N02]) και να αποτελεί μέρος της στρατηγικής τους.

8. Συμπεράσματα και Βέλτιστες Πρακτικές

Η Διαχείριση Κινδύνων διαδραματίζει έναν κρίσιμο ρόλο στην προστασία των πληροφοριών-περιουσιακών στοιχείων του Οργανισμού και ως εκ τούτου, η δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης κινδύνων αποτελεί σημαντική συνιστώσα ενός ολοκληρωμένου προγράμματος ασφαλείας σε επίπεδο IT. Επιπλέον, η διαδικασία διαχείρισης των κινδύνων δεν πρέπει να αντιμετωπίζεται ως μια «τεχνική» λειτουργία που διεξάγεται από ειδικούς του IT, αλλά ως μια βασική λειτουργία του Οργανισμού συνολικά.

Ο εντοπισμός και αξιολόγηση κινδύνων (risk assessment) είναι το πρώτο βήμα που ακολουθείται σε όλες σχεδόν τις μεθοδολογίες διαχείρισης κινδύνων. Κατά το βήμα αυτό, οι Οργανισμοί καθορίζουν το εύρος των δυνητικών απειλών για τα IT συστήματα και των κινδύνων που απορρέουν σε όλο τον Κύκλο Ζωής των συστημάτων. Το αποτέλεσμα αυτής της διαδικασίας βοηθά εν συνεχεία στον εντοπισμό κατάλληλων ελέγχων η εφαρμογή των οποίων θα οδηγήσει στη μείωση ή την εξάλειψη των κινδύνων αυτών (risk mitigation – elimination), διαδικασία η οποία αποτελεί επόμενο βήμα της προτεινόμενης μεθοδολογίας. Για να προσδιοριστεί η πιθανότητα ενός μελλοντικού ανεπιθύμητου γεγονότος, οι απειλές για ένα IT σύστημα θα πρέπει να αναλυθούν σε συνδυασμό με τις πιθανές αδυναμίες και τους ελέγχους που είναι εν ισχύ για το εν λόγω σύστημα.

Ο περιορισμός των κινδύνων (risk mitigation) είναι μια συστηματική μεθοδολογία που στοχεύει στη μείωση των κινδύνων που αντιμετωπίζει ένας Οργανισμός οι οποίοι μπορεί να έχουν αντίκτυπο στην εκπλήρωση της αποστολής του. Ο αντιμετώπιση και ο περιορισμός των κινδύνων αυτών, απαντάται συνήθως από ένα Οργανισμό με μία ή περισσότερες από επιλογές όπως ανάληψη, αποφυγή, περιορισμός ή μετακύληση κινδύνου. Οι στόχοι και η αποστολή του Οργανισμού θα πρέπει να λαμβάνονται υπόψη για την χρησιμοποίηση ή όχι οποιασδήποτε από τις παραπάνω επιλογές. Κατά κανόνα,

δεν είναι πρακτικά εφικτό για ένα Οργανισμό να αντιμετωπίσει όλους τους κινδύνους που έχουν εντοπιστεί, επομένως πρέπει να δίνεται προτεραιότητα σε εκείνα τα ζεύγη απειλών/ αδυναμιών που δυνητικά μπορούν να προκαλέσουν σημαντικές βλάβες και να έχουν σοβαρό αντίκτυπο στην επίτευξη της αποστολής του Οργανισμού.

Στους περισσότερους Οργανισμούς, τα δίκτυα επικοινωνιών επεκτείνονται και μεταβάλλονται διαρκώς και οι εφαρμογές λογισμικού αντικαθίστανται ή ενημερώνονται με νεώτερες εκδόσεις. Το προσωπικό αλλάζει, με αργούς ή γρήγορους ρυθμούς και οι πολιτικές ασφάλειας αλλάζουν κι αυτές με την πάροδο του χρόνου. Αυτές οι αλλαγές σημαίνουν ότι οι νέοι κίνδυνοι έρχονται στην επιφάνεια, ενώ οι κίνδυνοι που είχαν προηγουμένως περιοριστεί μπορεί και πάλι να αποτελέσουν πρόβλημα. Συνεπώς, η διαδικασία διαχείρισης κινδύνων πρέπει να είναι διαρκής και εξελισσόμενη. Για την αποτελεσματική υποστήριξη της διαδικασίας μπορεί να εφαρμοστεί μια σειρά καλών πρακτικών (best practices) ασφάλειας, όπως:

- Επανάληψη της διαδικασίας αξιολόγησης των κινδύνων ανά τακτά χρονικά διαστήματα (π.χ. 2 έτη).
- Ενσωμάτωση διαδικασιών αξιολόγησης και διαχείρισης κινδύνων στον Κύκλο Ζωής των IT συστημάτων.
- Εξέταση και περιορισμός κινδύνων εντός προκαθορισμένων συγκεκριμένων χρονοδιαγραμμάτων
- Ευέλικτες διαδικασίες ώστε να μπορούν να ενσωματώνονται άμεσα αλλαγές όταν αυτό επιβάλλεται, εξαιτίας μεγάλων αλλαγών στα IT συστήματα και το ευρύτερο περιβάλλον.

Για να είναι επιτυχημένο, ένα πρόγραμμα διαχείρισης κινδύνων πρέπει να στηρίζεται σε μια σειρά παραγόντων οι σημαντικότεροι εκ των οποίων είναι:

1. Η δέσμευση των ανώτερων διευθυντικών στελεχών.

2. Η ενεργή και συνεχής υποστήριξη και συμμετοχή του IT.
3. Η ικανότητα την Ομάδας που αξιολογεί τους κινδύνους. Τα μέλη της Ομάδας αυτής θα πρέπει να έχουν εμπειρία στην εφαρμογή της μεθοδολογίας αξιολόγησης κινδύνων από άλλους Οργανισμούς ή συστήματα, να εντοπίζουν τους κινδύνους στους οποίους είναι εκτεθειμένος ο Οργανισμός και να προτείνουν οικονομικά αποδοτικές λύσεις που ενισχύουν την ασφάλεια του Οργανισμού.
4. Η ενημέρωση, ευαισθητοποίηση και συνεργασία της κοινότητας των χρηστών, οι οποίοι πρέπει εν τέλει να ακολουθούν τις διαδικασίες και να συμμορφώνονται με τους εφαρμοζόμενους ελέγχους ώστε να διαφυλάσσεται η αποστολή του Οργανισμού.
5. Η συνεχής αξιολόγηση και εκτίμηση των IT κινδύνων που συνδέονται με την εκπλήρωση της αποστολής του Οργανισμού.

Εν κατακλείδι, θα μπορούσαμε να πούμε ότι τα πρότυπα ασφάλειας ενός Οργανισμού πρέπει να εμπεριέχουν ένα σύνολο ελέγχων και κατευθυντήριων γραμμών οι οποίοι να διασφαλίζουν ότι οι διαδικασίες ασφαλείας που διέπουν τη χρήση των IT συστημάτων και των πόρων του Οργανισμού, εφαρμόζονται ορθά και είναι ευθυγραμμισμένες με τους στόχους και την αποστολή του.

Βιβλιογραφία.

Αναφορές Αρθρογραφίας.

[ΚΓ04] Κάτσικας, Σ., Γκρίτζαλης, Δ., Γκρίτζαλης, Σ. Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών. 2004.

[A08] Anderson, R. Security Engineering. 2nd Edition, Wiley, 2008.

[B01] Barman, S. Writing Information Security Policies. Paperback. 2001.

[C06] Calder, A. Implementing Information Security Based on ISO 27001/ISO 17799: Best Practice. Paperback, 2006

[CBR] Cheswick, W., Bellovin, S., Rubin, A Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2003.

[DR03] Delamontagne, R. Reducing risk through training, Industrial Safety & HygieneNews, Vol. 37, Issue 2, pp. 1-2, 2003

[G04] Gilliam, D. Security risks: management and mitigation in the software life cycle. 13th IEEE International Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises - WET ICE, 2004.

[JA05] Jones, A., Ashenden D. Risk Management for Computer Security: Protecting Your Network & Information Assets. Elsevier, 2005.

[KPS] Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World. Prentice Hall, 2002.

[K10] Kissinger, B. Information Technology Compliance: Past, Present and Future. ISACA Journal, Vol. 1, 2010.

[LKA] Lawrie, G., Kalff, D and Andersen, H. Integrating Risk Management with Existing Methods of Strategic Control: Avoiding Duplication within the Corporate Governance Agenda. 6th International Conference on Corporate Governance and Board Leadership, Henley Management College, 2003.

[LC03] Lewis, M. Cause, consequence and control: Towards a theoretical and practical model of operational risk, Journal of Operations Management, Vol. 21, Issue 2, pp. 205-224, 2003.

[M09] Martin, A. Mitigating IT Vulnerabilities Provides Continual Fraud Prevention. ISACA Journal, Vol. 4, 2009.

[N95] NIST. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12, 1995.

[NG96] NIST, Guttman B. Generally Accepted Principles and Practices for Securing Information Technology Systems. Special Publication 800-14, 1996.

[NF98] NIST, FCSM Forum Working Group. Guide For Developing Security Plans for Information Technology Systems. Special Publication 800-18, 1998.

[N01a] NIST. Security Self-Assessment Guide for Information Technology Systems. Special Publication 800-26, 2001.

[N01b] NIST. Engineering Principles for IT Security. Special Publication 800-27, 2001.

[N02] NIST. Risk Management Guide for Information Technology Systems. Special Publication 800-30, 2002.

[SAA] Shahzad, B., Al-Ohali, Y. and Abdullah, A. Trivial model for mitigation of risks in software development life cycle. International Journal of the Physical Sciences Vol. 6(8), pp. 2072-2082, 2001.

[S11] Sharifrazi, F. Security Risk Mitigation and Residual Management in Distributed Educational Environment. 2011 Barcelona European Academic Conference, Spain, pp.766-770, 2011.

[SCL] Sherwood, J., Clark, A., Lynas, D. Enterprise Security Architecture: A Business-Driven Approach. CMP, 2005.

Αναφορές Διαδικτύου (Internet).

[I1]: www.securityfocus.com

[I2]: www.securitywatch.com

[I3]: www.securityportal.com

[I4]: www.SANS.org

[I5]: http://icat.nist.gov

Παράρτημα Ι

Στα πλαίσια της διπλωματικής εργασίας έχουμε αναπτύξει μια εφαρμογή η οποία αναφέρεται στον προσδιορισμό αδυναμιών, αντίκτυπων και λύσεων για την αντιμετώπιση των αδυναμιών, καθώς στην απόδοση βαρών για τα παραπάνω μεγέθη έτσι ώστε να είναι δυνατός ο υπολογισμός του κινδύνου που αναφέρεται στα παραπάνω. Αρχικά θα αναφερθούμε στα τεχνικά στοιχεία της εφαρμογής, στην συνέχεια θα δείξουμε τις δυνατότητές της και τέλος θα δούμε μελλοντικές βελτιώσεις της

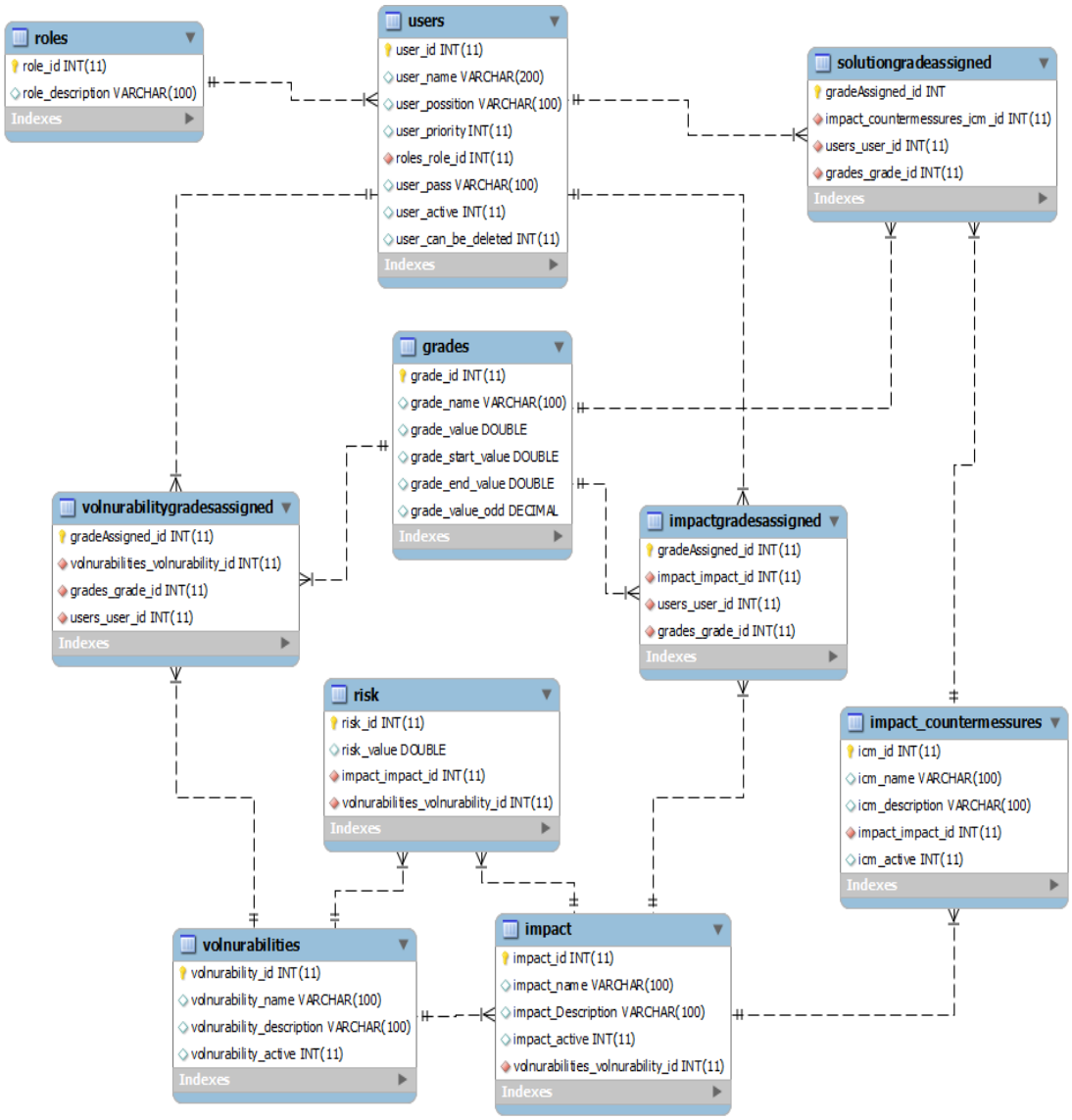
Π1. Τεχνικά Στοιχεία

Η εφαρμογή είναι γραμμένη σε C# .Net. Είναι μια Windows Forms εφαρμογή. Χρησιμοποιείται η τεχνολογία των Web Services για απομακρυσμένη πρόσβαση σε μια κεντρική βάση δεδομένων. Η βάση δεδομένων που επιλέχτηκε είναι η MySQL.

Η εφαρμογή χρησιμοποιεί σχεδιασμό τριών επιπέδων, όπου στο πρώτο επίπεδο έχουμε την βάση δεδομένων, στο δεύτερο επίπεδο το Web Service το οποίο επικοινωνεί με την βάση δεδομένων και στο τρίτο επίπεδο την εφαρμογή που επικοινωνεί με το Web Service.

Π1.1 Πρώτο Επίπεδο – Η Βάση Δεδομένων

Στο παρακάτω διάγραμμα δείχνουμε το σχεσιακό μοντέλο της βάσης δεδομένων.



Χρησιμοποιήθηκαν οι παρακάτω πίνακες:

volnurabilities	Αποτελεί τον πίνακα που αποθηκεύονται οι αδυναμίες
volnurabilitygradeassigned	Αποτελεί τον πίνακα που αποθηκεύεται το βάρος

	που έχει δοθεί από κάθε χρήστη για κάθε αδυναμία.
impact	Αποτελεί τον πίνακα που αποθηκεύονται οι αντίκτυποι
impactgradeassigned	Αποτελεί τον πίνακα που αποθηκεύεται το βάρος που έχει δοθεί από κάθε χρήστη για κάθε αντίκτυπο.
impact_countermessures	Αποτελεί τον πίνακα που αποθηκεύονται οι λύσεις που προτείνονται για κάθε αδυναμία
solutiongradeassigned	Αποτελεί τον πίνακα που αποθηκεύεται το βάρος που έχει δοθεί από κάθε χρήστη για κάθε λύση.
risk	Αποτελεί τον πίνακα των Κινδύνων.
grade	Αποτελεί πίνακα που τοποθετούνται τα βάρη.
users	Αποτελεί πίνακα με τους χρήστες του συστήματος
roles	Αποτελεί πίνακα που περιέχει τους ρόλους που μπορούν να έχουν οι χρήστες.

Ας δούμε περιγραφή των πινάκων.

volnurabilities	
volnurability_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αδυναμία
volnurability_name	Σύντομο όνομα αδυναμίας
volnurability_description	Περιγραφή αδυναμίας
volnurability_active	0: Δεν είναι ενεργή 1: Είναι ενεργή

volnurabilitygradeassigned	
gradeAssigned_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αντιστοίχιση
volnurabilities_volnurability_id	Το id που αντιστοιχεί την αδυναμία
grades_grade_id	Το βάρος που εισήχθη

users_user_id	Το id του χρήστη που εισήγαγε το βάρος

impact	
impact_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αντίκτυπο
impact_name	Σύντομο όνομα αντίκτυπου
impact_Description	Περιγραφή αντίκτυπου
impact_active	0: Δεν είναι ενεργός 1: Είναι ενεργός
volnurabilities_volnurability_id	Το id της αδυναμίας στην οποία αντιστοιχεί ο συγκεκριμένος αντίκτυπος.

impactgradeassigned	
gradeAssigned_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αντιστοίχιση
impact_impact_id	Το id που αντιστοιχεί τον αντίκτυπο
users_user_id	Το βάρος που εισήχθη
grades_grade_id	Το id του χρήστη που εισήγαγε το βάρος

impact_countermessures	
icm_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε λύση
icm_name	Σύντομο όνομα λύσης
icm_description	Περιγραφή λύσης
impact_impact_id	Το id του αντίκτυπου στον οποίο

	αντιστοιχεί η λύση.
icm_active	0: Δεν είναι ενεργή 1: Είναι ενεργή

solutiongradeassigned	
gradeAssigned_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αντιστοίχιση
impact_countermessures_icm_id	Το id που αντιστοιχεί στον αντίκτυπο
users_user_id	Το id του χρήστη που εισήγαγε το βάρος
grades_grade_id	Το βάρος που εισήχθη

risk	
risk_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε κίνδυνο
risk_value	Βαθμός του κινδύνου
impact_impact_id	Το id που αντιστοιχεί στον αντίκτυπο
volnurabilities_volnurability_id	Το id που αντιστοιχεί την αδυναμία

grade	
grade_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε βαθμό
grade_name	Σύντομο όνομα βαθμού
grade_value	Η τιμή του βαθμού
grade_start_value	Άνω όριο τιμών βαθμού
grade_end_value	Κάτω όριο τιμών βαθμού

grade_value_odd	Τιμή Πιθανότητας βαθμού

users	
user_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε χρήστη.
user_name	Όνομα χρήστη
user_possition	Περιγραφή θέσης χρήστη στον οργανισμό
user_priority	Προτεραιότητα χρήστη. Αριθμός που αναφέρεται στο ‘βάρος της γνώμης’ του χρήστη.
roles_role_id	Το id του ρόλου του χρήστη
user_pass	Το συνθηματικό εισόδου του χρήστη
user_active	0: Ο χρήστης δεν είναι στο σύστημα 1: Ο χρήστης είναι στο σύστημα
user_can_be_deleted	0: Ο χρήστης δεν μπορεί να διαγραφεί 1: Ο χρήστης μπορεί να διαγραφεί

roles	
role_id	Μοναδικός αριθμός που αντιστοιχεί σε κάθε αδυναμία
role_description	Σύντομο όνομα ρόλου

Η βάση δεδομένων είναι κεντρική και βρίσκεται στον DB Server του οργανισμού. Αυτό διευκολύνει τις διαχειριστικές λειτουργίες της βάσης και επιτρέπει την ταυτόχρονη ενημέρωση όλων των χρηστών της εφαρμογής για αλλαγές που τους ενδιαφέρουν.

Στο συνοδευτικό CD υπάρχει το αρχείο DB/RiskManagementApp.mwb με το οποίο μπορούμε να φτιάξουμε στην MySQL τους πίνακες της βάσης.

Π1.2 Δεύτερο Επίπεδο – Το Web Service

Το Web Service βρίσκεται στον Application Server ή στον Web Server του οργανισμού. Η δουλειά του είναι να επικοινωνεί με την βάση δεδομένων.

Έχει γραφεί με τεχνολογία .Net 4 (WCF) και ειδικά σε γλώσσα προγραμματισμού C#. Παραθέτουμε παρακάτω μια λίστα με τις λειτουργίες που μπορεί να πραγματοποιήσει.

getUsers	Επιστρέφει όλους τους χρήστες που είναι εγγεγραμμένοι
getUserByUsernameAndPassword	Επιστρέφει όλους τους χρήστες στους οποίους αντιστοιχούν δοθέντα όνομα χρήστη και συνθηματικό χρήστη
deleteUser	Διαγράφει έναν χρήστη από την βάση δεδομένων
insertUser	Εισάγει έναν χρήστη στην βάση δεδομένων
setUserActive	Αλλάζει το πεδίο user_active της βάσης δεδομένων για δοθέντα χρήστη σε 1
setUserInactive	Αλλάζει το πεδίο user_active της βάσης δεδομένων για δοθέντα χρήστη σε 0
updateUserPassword	Αλλάζει το συνθηματικό χρήστη για δοθέντα χρήστη
updateUser	Αλλάζει τα στοιχεία του χρήστη για δοθέντα χρήστη
getRoles	Επιστρέφονται όλοι οι ρόλοι που

	υπάρχουν στην βάση δεδομένων
getGrades	Επιστρέφονται όλοι οι βαθμοί που υπάρχουν στην βάση δεδομένων
insertVolnurability	Γίνεται εισαγωγή μιας αδυναμίας στην βάση δεδομένων
setVolnurabilityInactive	Αλλάζει το πεδίο volnurability_active της βάσης δεδομένων για δοθείσα αδυναμία σε 0
setVolnurabilityActive	Αλλάζει το πεδίο volnurability_active της βάσης δεδομένων για δοθείσα αδυναμία σε 1
insertGradeToVol	Εισάγεται ένα καινούριο βάρος για συγκεκριμένη αδυναμία
insertImpact	Γίνεται εισαγωγή ενός αντίκτυπου στην βάση δεδομένων
setImpactInactive	Αλλάζει το πεδίο impact_active της βάσης δεδομένων για δοθέντα αντίκτυπο σε 0
setImpactActive	Αλλάζει το πεδίο impact_active της βάσης δεδομένων για δοθέντα αντίκτυπο σε 1
insertGradeToImp	Εισάγεται ένα καινούριο βάρος για συγκεκριμένο αντίκτυπο
insertSolution	Γίνεται εισαγωγή μιας λύσης στην βάση δεδομένων
setSolutionInactive	Αλλάζει το πεδίο icm_active της βάσης δεδομένων για δοθείσα λύση σε 0
setSolutionActive	Αλλάζει το πεδίο icm_active της βάσης δεδομένων για δοθείσα λύση

	σε 1
insertGradeToSol	Εισάγεται ένα καινούριο βάρος για συγκεκριμένη λύση
getAllVolnurabilities	Επιστρέφει όλες τις αδυναμίες που είναι ορισμένες στην βάση δεδομένων
getAllImpacts	Επιστρέφει όλους τους αντίκτυπους που είναι ορισμένοι στην βάση δεδομένων
getAllSolutions	Επιστρέφει όλες τις λύσεις που είναι ορισμένες στην βάση δεδομένων

Παρακάτω θα περιγράψουμε τις μεταβλητές εισόδου και τις επιστρεφόμενες μεταβλητές των παραπάνω μεθόδων.

getUsers	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των χρηστών.

getUserByUsernameAndPassword	
Είσοδος	
username	Το όνομα χρήστη
password	Το συνθηματικό χρήστη
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των χρηστών.

deleteUser	
Είσοδος	
userID	Το id του χρήστη
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

insertUser	
Είσοδος	
userName	Το όνομα χρήστη
userPossition	Η θέση του χρήστη στον οργανισμό
userPriority	Η προτεραιότητα του χρήστη (βλέπε παραπάνω)
userRole	Ο ρόλος του χρήστη
userPass	Το συνθηματικό χρήστη
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

setUserActive	
Είσοδος	
userID	Το id του χρήστη
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

setUserInactive	
Είσοδος	
userID	Το id του χρήστη
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

updateUserPassword	
Είσοδος	
userID	Το id του χρήστη
newPassword	Το νέο συνθηματικό του χρήστη
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

updateUser	
Είσοδος	
userID	Το id του χρήστη
userPossition	Η θέση του χρήστη στον οργανισμό
userPriority	Η προτεραιότητα του χρήστη (βλέπε παραπάνω)
userRole	Ο ρόλος του χρήστη
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

getRoles	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των ρόλων.

getGrades	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των βαθμών.

insertVolnurability	
Είσοδος	
volName	Το όνομα της αδυναμίας
volDescr	Η περιγραφή της αδυναμίας
volActive	Εναργή ή όχι αδυναμία
userID	Το id του χρήστη που εισήγαγε την αδυναμία
gradeID	Το βάρος που έβαλε ο χρήστης για την αδυναμία
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

setVolnurabilityInactive	
Είσοδος	
volID	Το id της αδυναμίας
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

setVolnurabilityActive	
Είσοδος	
volID	Το id της αδυναμίας
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

insertGradeToVol	
Είσοδος	
volID	Το id της αδυναμίας
gradeID	Το id του βαθμού
userID	Το id του χρήστη που τον εισήγαγε
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

insertImpact	
Είσοδος	
impName	Το όνομα της του αντίκτυπου
impDescr	Η περιγραφή του αντίκτυπου
impActive	Ενεργός ή όχι αντίκτυπος

volID	Το id της αδυναμίας που αντιστοιχεί στον αντίκτυπο
userID	Το id του χρήστη που εισήγαγε τον αντίκτυπο
gradeID	Το id του βαθμού του αντίκτυπου
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία
setImpactInactive	
Είσοδος	
impID	Το id του αντίκτυπου
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

setImpactActive	
Είσοδος	
impID	Το id του αντίκτυπου
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

insertGradeToImp	
Είσοδος	
impID	Το id του αντίκτυποι
gradeID	Το id του βαθμού
userID	Το id του χρήστη που τον εισήγαγε
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

insertSolution	
Είσοδος	
solName	Το όνομα της λύσης
solDescr	Η περιγραφή της λύσης
solActive	Ενεργή ή όχι λύση
impID	Το id του αντίκτυποι που αντιστοιχεί στην λύση
userID	Το id του χρήστη που εισήγαγε τον αντίκτυπο
gradeID	Το id του βαθμού του αντίκτυπού
Έξοδος	
Integer	> 0: Επιτυχής Λειτουργία -1: Ανεπιτυχής Λειτουργία

setSolutionInactive	
Είσοδος	
solID	Το id της λύσης
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

setSolutionActive	
Είσοδος	
solID	Το id της λύσης
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

insertGradeToSol	
Είσοδος	
solID	Το id της λύσης
gradeID	Το id του βαθμού
userID	Το id του χρήστη που τον εισήγαγε
Έξοδος	
Boolean	true: Επιτυχής Λειτουργία false: Ανεπιτυχής Λειτουργία

getAllVolnurabilities	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των αδυναμιών.

getAllImpacts	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των αντίκτυπων.

getAllSolutions	
Είσοδος	
-	
Έξοδος	
DataSet ds	Ένα .Net dataset το οποίο περιέχει όλα τα δεδομένα των λύσεων.

Εδώ είναι σημαντικό να σημειωθεί ότι το Web Service είναι σχεδιασμένο ώστε να παράγει log αρχείο για όλες τις ενέργειες που πραγματοποιεί.
Στον φάκελο WebService του συνοδευτικού CD μπορείτε να βρείτε τον πηγαίο κώδικα του Web Service.

Π1.3 Τρίτο Επίπεδο – Η Εφαρμογη

Η εφαρμογή που έχει αναπτυχθεί είναι γραμμένη στην γλώσσα προγραμματισμού C# .Net και έχει χρησιμοποιηθεί .Net Framework 4. Χρησιμοποιεί το παραπάνω Web Service για να συνδεθεί με την βάση δεδομένων και να λάβει ή να αλλάξει δεδομένα στην βάση δεδομένων.
Κάθε client τοποθετείται στον προσωπικό υπολογιστή του χρήστη. Από εκεί μπορεί ο χρήστης, ανάλογα και με τον ρόλο που του έχει αποδοθεί, να έχει έλεγχο στις λειτουργίες που θα δούμε στο παρακάτω κεφάλαιο του παραρτήματος.

Π1.3.1 Περιγραφή Εφαρμογής

Στο τμήμα αυτό θα παρουσιάσουμε την εφαρμογή που υλοποιήθηκε στα πλαίσια της διπλωματικής εργασίας. Μετά το τέλος της παρουσίασης αυτής θα αναφέρουμε τρόπους βελτίωσης των λειτουργιών καθώς και επέκτασης των.

Π1.3.1.1 Γενικά

Η εφαρμογή έχει σαν βασικό της ρόλο την αντιμετώπιση ενός σημαντικού προβλήματος κυρίως μεγάλων οργανισμών. Μια διαδικασία πολύ σημαντική όπως αυτή του εντοπισμού κινδύνων και διαχείρισής τους γίνεται μόνο στο ανώτερο ή ανώτατο επίπεδο διοίκησης του οργανισμού. Συχνά, λόγω της παραπάνω παρατήρησης, υπάρχει δυστοκία στην άμεση και διεξοδική αντιμετώπιση των καθημερινών προβλημάτων που μπορεί να παρουσιαστούν στον οργανισμό και που είναι πιθανό να αποτελούν κινδύνους που χρίζουν άμεσης αντιμετώπισης. Επιπλέον έχει αξία σε αυτή την διαδικασία να συμμετέχουν όλοι οι χρήστες που μπορεί να έχουν γνώμη για συγκεκριμένα

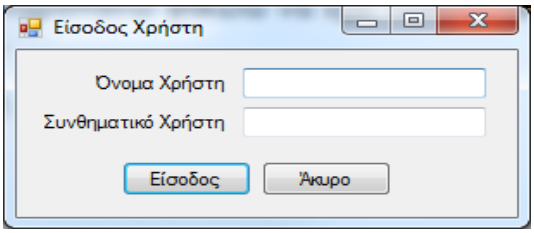
ζητήματα, έτσι ώστε η ανώτερη διοίκηση να έχει άμεση άποψη πάνω στα διάφορα προβλήματα και ζητήματα.
Η συγκεκριμένη εφαρμογή προσπαθεί να καλύψει τα παραπάνω θέματα με τρόπο άμεσο και αποτελεσματικό, φτηνό για τον οργανισμό, αλλά πολύτιμο διότι διαχέεται η πληροφορία σε όλους τους ενδιαφερόμενους άμεσα και κυρίως εύκολα αναγνώσιμη και διαχειρίσιμη.
Οι χρήστες μπορούν ανάλογα με τις θέσεις που κατέχουν στον οργανισμό, αλλά και με τις γενικές γνώσεις και δεξιότητές τους να λάβουν συγκεκριμένη προτεραιότητα/βάρος ως προς τις καταχωρίσεις τους. Αυτές δε μπορούν άμεσα να πραγματοποιούνται με την βοήθεια της εφαρμογής έτσι ώστε οποιοδήποτε πρόβλημα μπορεί να παρουσιαστεί και να αποτελέσει κίνδυνο για την λειτουργία ή τους στόχους του οργανισμού να γνωστοποιείται, να μηχανογραφείται και να διαχέεται σε όλους τους ενδιαφερόμενους.
Τέλος το πρόγραμμα μπορεί να παράγει και να ταξινομεί τους κινδύνους που αναφέρονται στις καταχωρίσεις των χρηστών.

Π1.3.1.2 Εγκατάσταση

Έχει προβλεφθεί η εφαρμογή να έχει ένα πρόγραμμα εγκατάστασης το οποίο θα τοποθετεί το εκτελέσιμο αρχείο στον δίσκο του υπολογιστή μας. Είναι σημαντικό να σημειώσουμε ότι στον υπολογιστή μας πρέπει να έχουμε εγκατεστημένο το .Net Framework 4 το οποίο μπορείτε να κατεβάσετε από την παρακάτω ηλεκτρονική διεύθυνση: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17851.
Μετά την εγκατάσταση του .Net Framework 4 είμαστε έτοιμοι να εκκινήσουμε το πρόγραμμα εγκατάστασης της εφαρμογής μας. Θα το βρούμε στον φάκελο Risk Management Application του συνοδευτικού CD. Το αρχείο είναι το setup.exe. Αν στον υπολογιστή σας ήδη υπάρχει εγκατεστημένη η εφαρμογή δεν θα μπορέσετε να την επανεγκαταστήσετε. Θα πρέπει να κάνετε απεγκατάσταση και επανεγκατάσταση.
Το προκαθορισμένο σημείο τοποθέτησης της εφαρμογής είναι το:
C:\Program Files\Panepistimio Peiraia\Risk Management Application

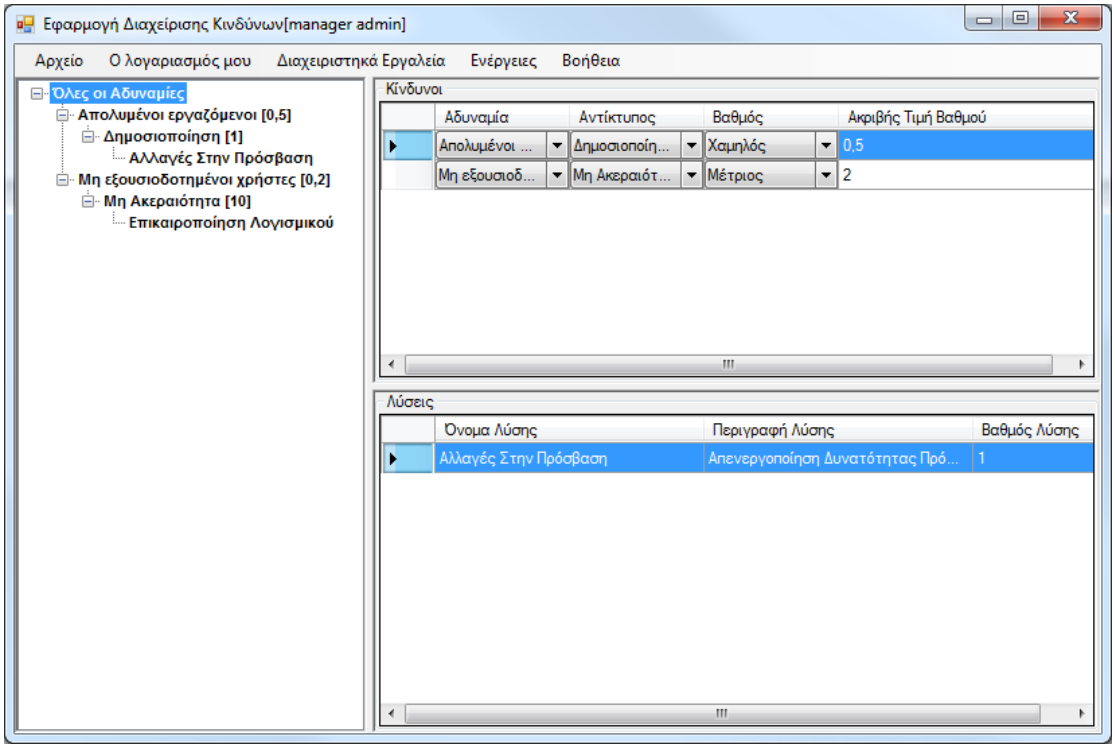
όπου και μπορείτε να βρείτε το εκτελέσιμο αρχείο RiskManagementApplication.exe.
Έχει προβλεφθεί στον παραπάνω φάκελο να έχει τοποθετηθεί και ο πηγαίος κώδικας της εφαρμογής.

Π1.3.1.3 Είσοδος στην εφαρμογή



Παραπάνω δείχνουμε την οθόνη εισόδου στην εφαρμογή. Το όνομα χρήστη και συνθηματικό του προκαθορισμένου χρήστη είναι admin/admin. Πατάμε ‘Είσοδος’ για να εισέλθουμε.

Π1.3.1.4 Η κεντρική οθόνη της εφαρμογής



Η παραπάνω εικόνα δείχνει την κεντρική οθόνη της εφαρμογής. Παρατηρούμε 4 βασικά στοιχεία:

- Το μενού επιλογών
- Το δέντρο αδυναμιών
- Τον πίνακα κινδύνων
- Τον πίνακα λύσεων

Π1.3.1.4.1 Το μενού επιλογών

Στους παρακάτω πίνακες θα αναλύσουμε όλες τις δυνατότητες που έχει κάποιος χρήστης με ρόλο διαχειριστή του συστήματος.

Αρχείο	
Έξοδος	Πραγματοποιείται αποσύνδεση του χρήστη από την εφαρμογή

Ο λογαριασμός μου	
Αλλαγή κωδικού πρόσβασης	Εμφανίζεται παράθυρο αλλαγής κωδικού πρόσβασης.
Αποσύνδεση	Πραγματοποιείται αποσύνδεση του χρήστη απο την εφαρμογή

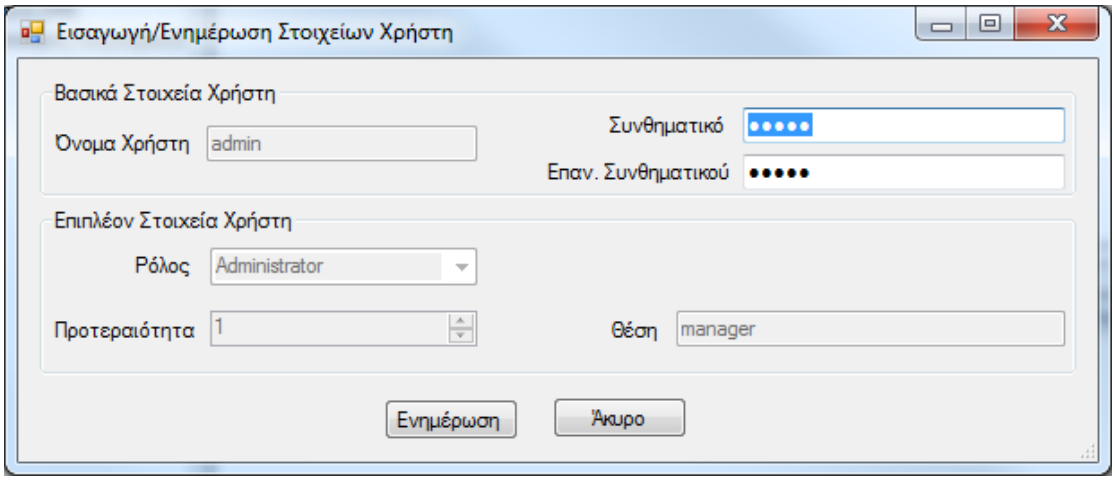
Διαχειριστικά Εργαλεία	
Διαχείριση Χρηστών	Εμφανίζεται παράθυρο διαχείρισης χρηστών.
Διαχείριση Ρόλων	Εμφανίζεται παράθυρο διαχείρισης ρόλων.
Διαχείριση Βαθμών Πιθανοτήτων	Εμφανίζεται παράθυρο διαχείρισης βαθμών πιθανοτήτων.

Ενέργειες	
Ενημέρωση Δέντρου Αδυναμιών	Ενημερώνονται τα δεδομένα που παρουσιάζονται από την βάση δεδομένων.

Βοήθεια	
Σχετικά	Παράθυρο διαλόγου με γενικές πληροφορίες για την εφαρμογή.

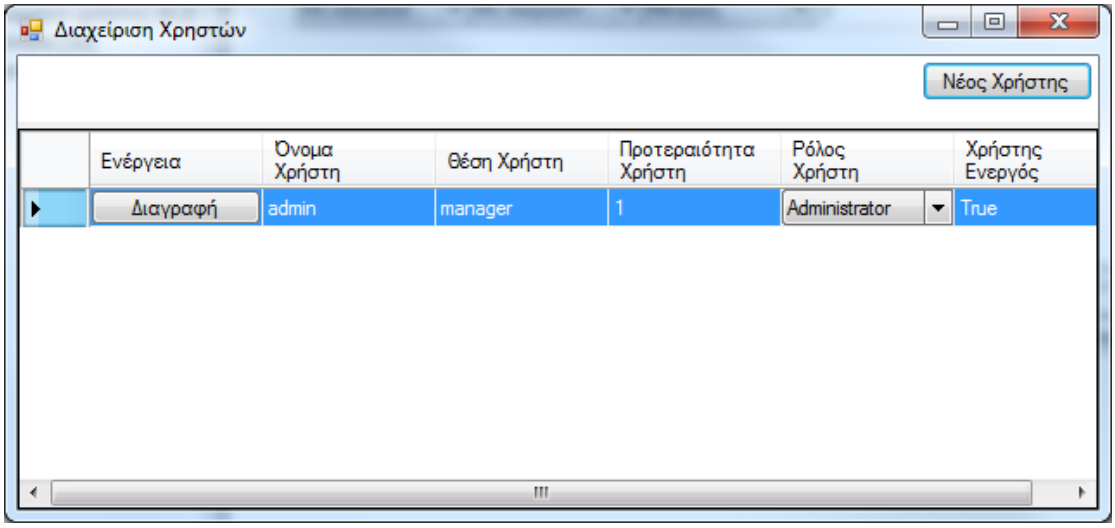
Παρακάτω θα δούμε μια προς μία τις παραπάνω λειτουργίες.

Π1.3.1.4.1.1 Αλλαγή κωδικού πρόσβασης



Όπως βλέπουμε στην παραπάνω εικόνα, εδώ ο χρήστης μπορεί να αλλάξει τον κωδικό πρόσβασής του και πατά ενημέρωση.

Π1.3.1.4.1.2 Διαχείριση Χρηστών

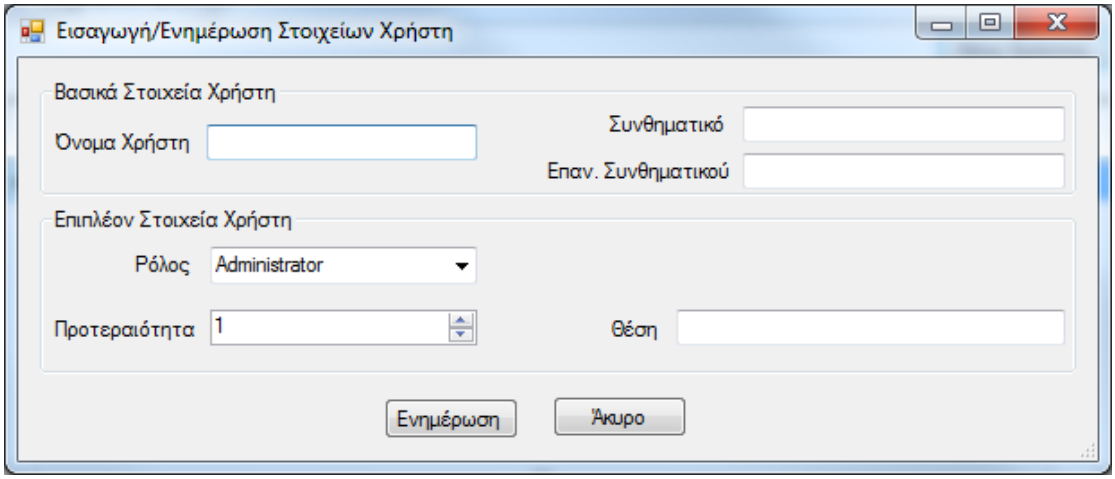


Η παραπάνω εικόνα δείχνει το παράθυρο διαχείρισης χρηστών.

Όπως βλέπουμε ο διαχειριστής μπορεί να πραγματοποιήσει 2 ενέργειες.

- Διαγραφή Χρήστη
- Εισαγωγή Χρήστη

Εισαγωγή χρήστη

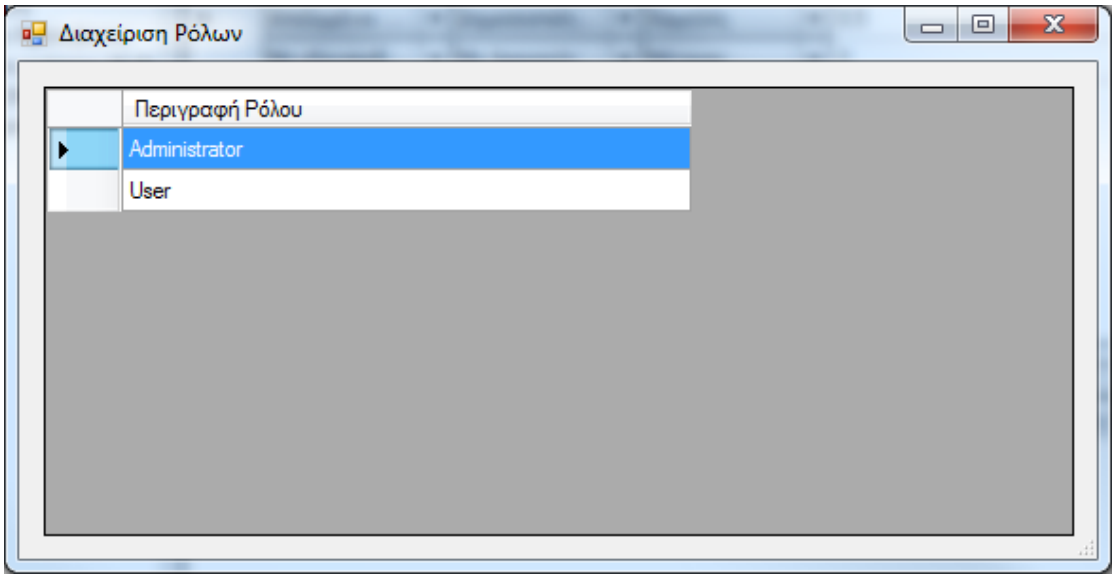


Η παραπάνω εικόνα δείχνει το παράθυρο εισαγωγής χρήστη. Ο διαχειριστής μπορεί να δηλώσει όλα τα απαραίτητα στοιχεία και να πατήσει ‘Ενημέρωση’.

Διαγραφή χρήστη

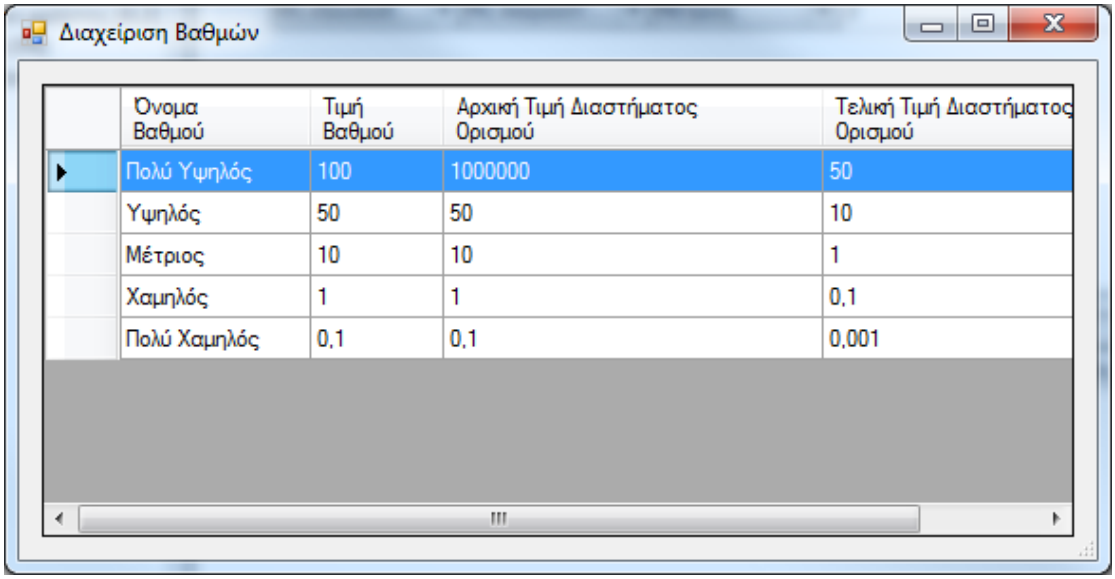
Με το πάτημα του κουμπιού ‘Διαγραφή’ και μετά από μήνυμα επιβεβαίωσης ο χρήστης διαγράφετε (ακόμη και αν είναι ενεργός). Ο χρήστης admin δεν μπορεί να διαγραφεί.

Π1.3.1.4.1.3 Διαχείριση ρόλων



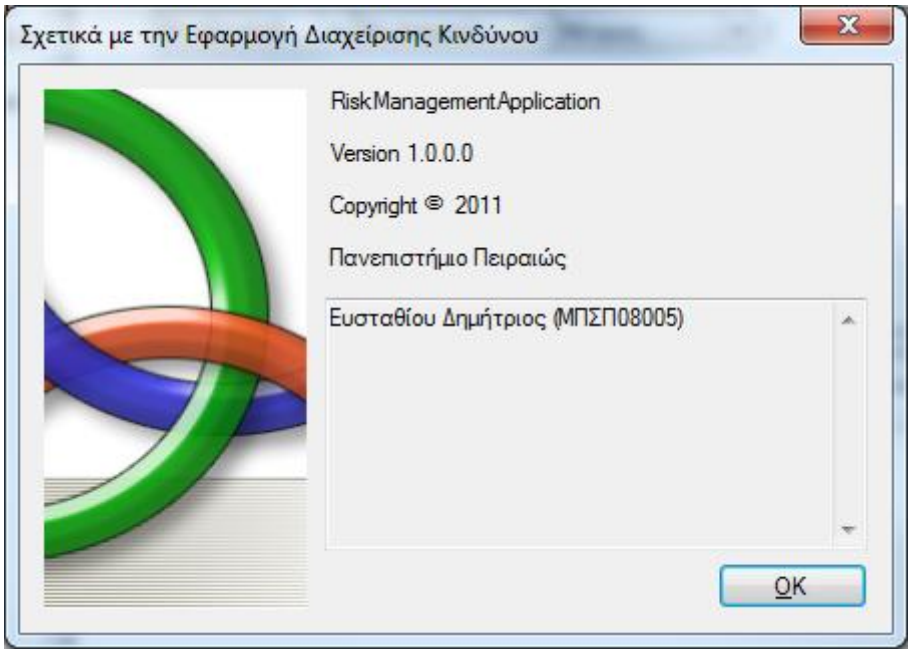
Παραπάνω φαίνεται το παράθυρο διαχείρισης ρόλων της εφαρμογής. Στην παρούσα έκδοση της εφαρμογής απλά παρουσιάζονται οι υπάρχοντες ρόλοι, χωρίς να μπορούν να γίνουν αλλαγές.

Π1.3.1.4.1.4 Διαχείριση Βαθμών

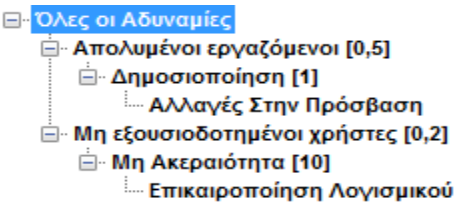


Παραπάνω φαίνεται το παράθυρο διαχείρισης βαθμών. Όπως και με τους ρόλους, στην παρούσα έκδοση έχουμε την δυνατότητα να δούμε όλα τα δεδομένα των βαθμών αλλά όχι να τα αλλάξουμε.

Π1.3.1.4.1.5 Σχετικά



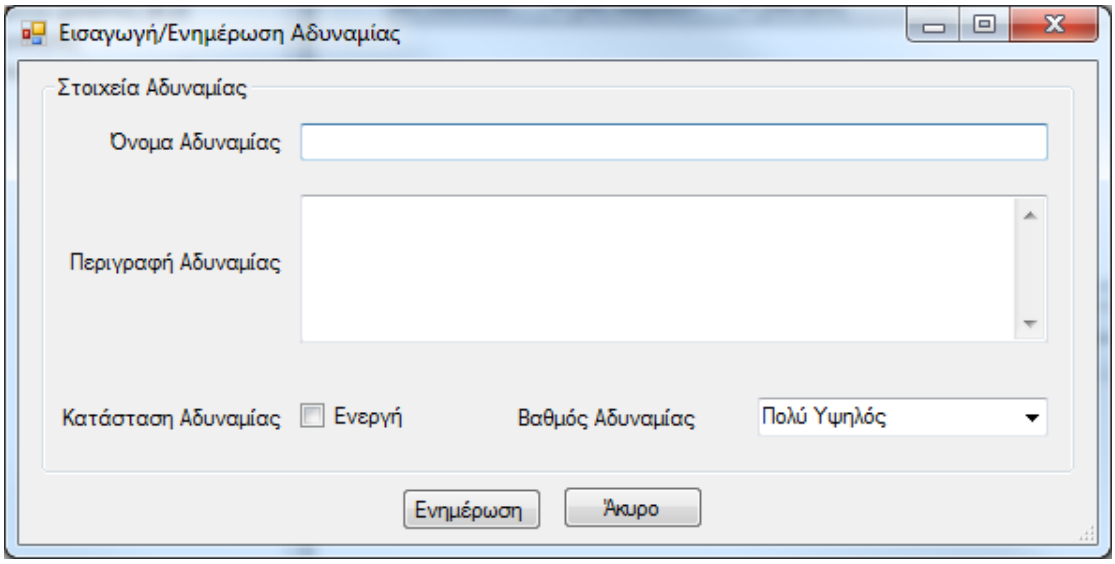
Π1.3.1.4.2 Το δέντρο αδυναμιών



Παραπάνω βλέπουμε ένα τυπικό δέντρο αδυναμιών. Το πρώτο επίπεδο αντιστοιχεί στις αδυναμίες, το δεύτερο επίπεδο στους αντίκτυπους και το τρίτο επίπεδο στις λύσεις. Κάθε ένα από τα επίπεδα αυτά έχει διαφορετικές ενέργειες που ο χρήστης μπορεί να πραγματοποιήσει.

Π1.3.1.4.2.1 Προσθήκη αδυναμίας

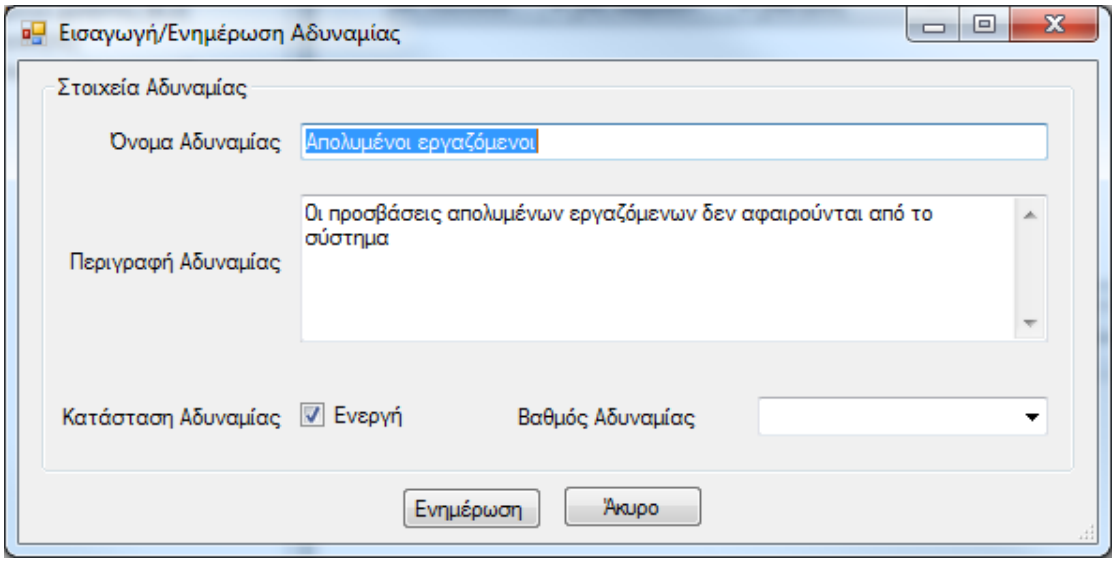
Στον κόμβο ‘’Όλες οι αδυναμίες’ του δέντρου ο χρήστης μπορεί να κάνει δεξί κλικ και να εμφανιστεί η επιλογή ‘Προσθήκη Αδυναμίας’. Το παράθυρο της προσθήκης φαίνεται στη παρακάτω εικόνα.



Εδώ ο χρήστης μπορεί να εισάγει μια καινούρια αδυναμία και να ορίσει βαθμό (βάρος) για αυτήν.

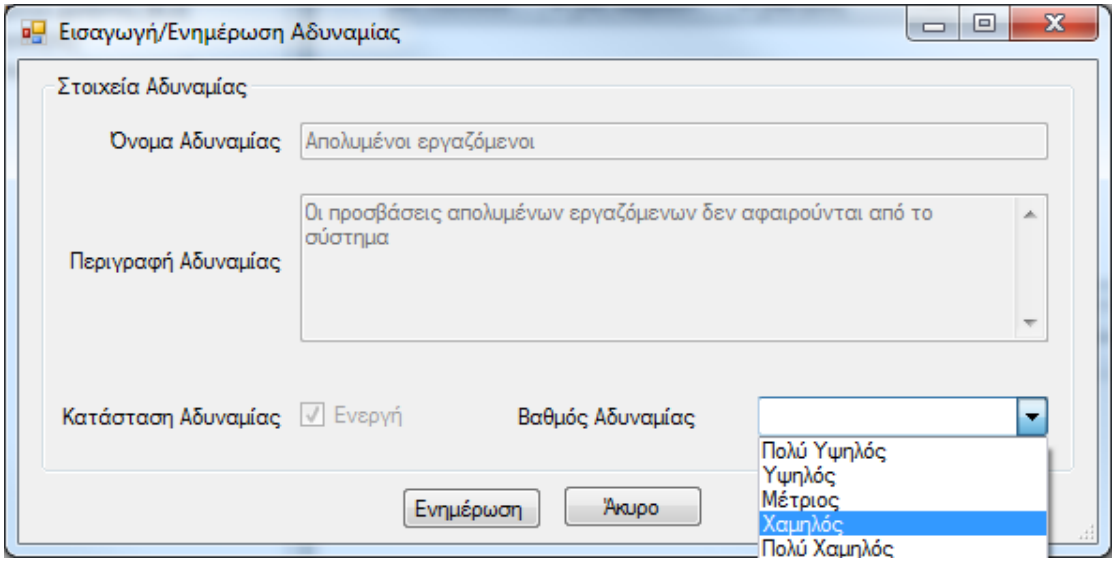
Π1.3.1.4.2.2 Εμφάνιση αδυναμίας

Ο χρήστης μπορεί να δει και να αλλάξει τα δεδομένα μιας αδυναμίας αν κάνει δεξί κλικ πάνω σε μια αδυναμία και επιλέξει ‘Εμφάνιση Αδυναμίας’.



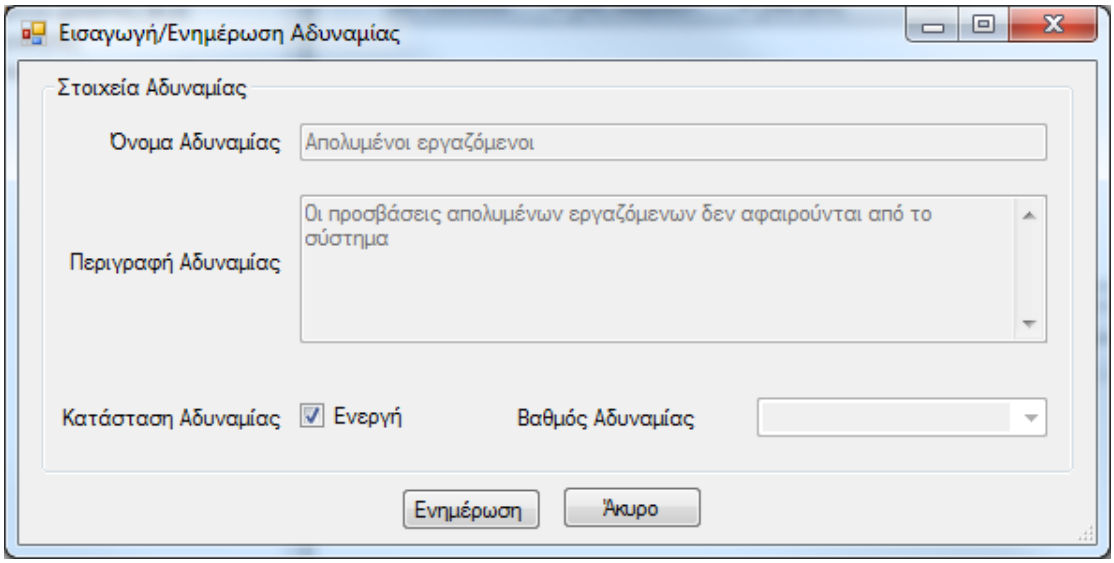
Παραπάνω βλέπουμε το παράθυρο που δίνει αυτές τις δυνατότητες στον χρήστη.

Π1.3.1.4.2.3 Προσθήκη Βαθμού



Κάθε χρήστης μπορεί να προσθέσει τον βαθμό αδυναμίας που από την σκοπιά του αντιστοιχεί σε αυτή την αδυναμία. Ο βαθμός της αδυναμίας δεν αλλάζει, αλλά προστίθεται, με τρόπο που θα δούμε αργότερα, στην αδυναμία.

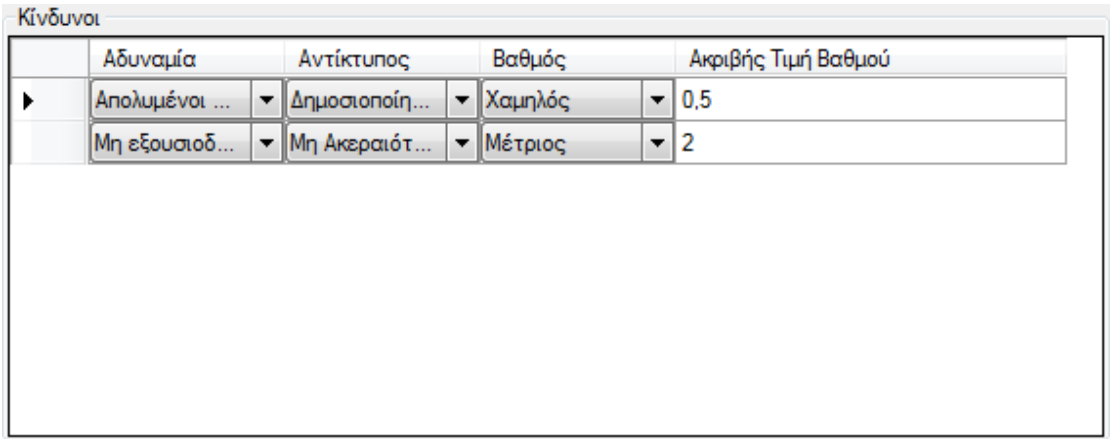
Π1.3.1.4.2.4 Αλλαγή κατάστασης αδυναμίας



Κάθε χρήστης μπορεί να μεταβάλλει την κατάσταση κάποιας αδυναμίας από ενεργή σε ανενεργή και ανάποδα. Με αυτόν τον τρόπο η αδυναμία αυτή δεν συμμετέχει στην παραγωγή κινδύνου. Στην συγκεκριμένη έκδοση αυτή η λειτουργία δεν έχει υλοποιηθεί.

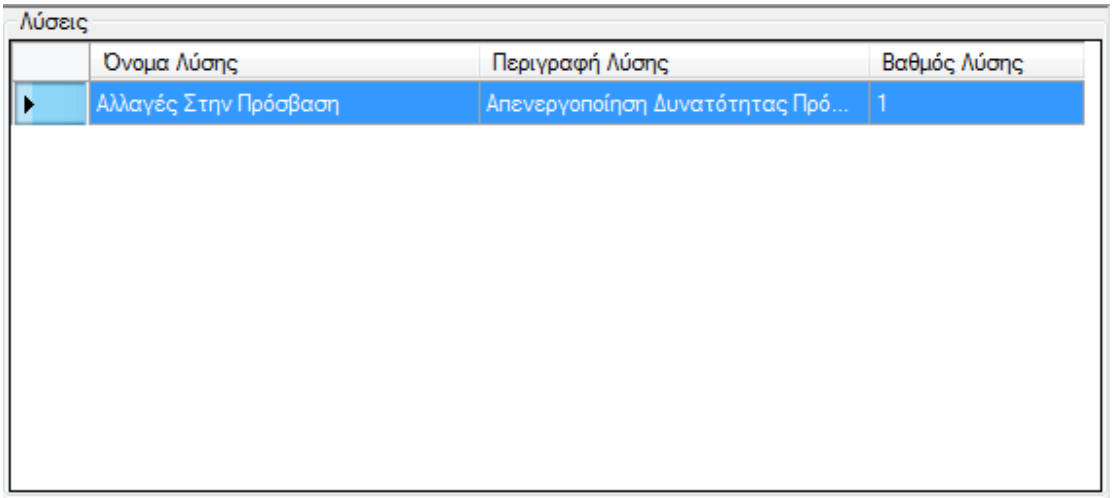
Επίσης μπορεί να γίνει προσθήκη αντίκτυπου, λειτουργία που το παράθυρό της είναι παρόμοιο με αυτό της προσθήκης αδυναμίας. Όλες οι λειτουργίες για τους αντίκτυπους και τις λύσεις, τα άλλα στοιχεία του δέντρου αδυναμιών είναι παρόμοιες με αυτές των κόμβων αδυναμιών.

Π1.3.1.4.3 Ο πίνακας κινδύνων



Στον πίνακα κινδύνων μπορεί ο χρήστης να δει τους κινδύνους που παράγονται από το δέντρο αδυναμιών. Οι κίνδυνοι αποτελούν ζεύγη αδυναμίας/αντίκτυπού και ο βαθμός του κινδύνου παράγεται με τον τρόπο που έχει αναλυθεί στο κύριο σώμα της παρούσας διπλωματικής εργασίας. Οι κίνδυνοι είναι ταξινομημένοι κατά αύξουσα σειρά επικινδυνότητας.

Π1.3.1.4.4 Ο πίνακας λύσεων



Με την επιλογή κάποιου κινδύνου μπορούμε να δούμε και τις προτεινόμενες λύσεις που σχετίζονται με τον συγκεκριμένο κίνδυνο. Όσο μεγαλύτερος είναι ο βαθμός της λύσης, τόσο περισσότερο προκρίνεται σαν λύση του προβλήματος.

Π1.3.1.5 Υπολογισμός Βαθμών.

Στην συγκεκριμένη εφαρμογή έχουμε αναπτύξει τον παρακάτω τρόπο υπολογισμού των βαθμών των διαφόρων στοιχείων.
Παίρνουμε όλους τους βαθμούς που έχουν ορίσει οι χρήστες για το συγκεκριμένο αντικείμενο (αδυναμία, αντίκτυπο ή λύση).
Πολλαπλασιάζουμε τον την τιμή του βαθμού με την προτεραιότητα του χρήστη που έχει ορίσει τον βαθμό.
Προσθέτουμε τα γινόμενα για όλους τους βαθμούς που έχουν οριστεί για το συγκεκριμένο αντικείμενο.
Διαιρούμε το άθροισμα με τον αριθμό των βαθμών που έχουν οριστεί για το συγκεκριμένο αντικείμενο.
Με την παραπάνω μέθοδο παράγεται ένας αριθμός που αποτελεί τον βαθμό κάθε αντικειμένου.
Οι τρέχοντες βαθμοί κάθε αντικειμένου φαίνονται στο δέντρο αδυναμιών, δίπλα από το όνομα κάθε αντικειμένου (εκτός από τις λύσεις, των οποίων οι βαθμοί παρουσιάζονται στον πίνακα λύσεων.

Π1.3.2 Βελτιώσεις – Προσθήκες.

Στο τμήμα αυτό καλούμαστε να εξετάσουμε όλα εκείνα που θα θέλαμε να προστεθούν στην συγκεκριμένη εφαρμογή ώστε να βελτιώσει τις δυνατότητές της.
Ως προς τα λειτουργικά της κομμάτια:

- Δυνατότητα διαχείρισης Ρόλων.
- Δυνατότητα διαχείρισης Βαθμών Πιθανοτήτων.
- Δυνατότητα ενεργοποίησης – απενεργοποίησης αντικειμένων του δέντρου αδυναμιών.

- Διαφοροποίηση των δυνατοτήτων των χρηστών ανά ρόλους.
- Δυνατότητα αυτόματης ενημέρωσης δέντρου αδυναμιών μετά από οποιαδήποτε αλλαγή από οποιονδήποτε χρήστη.
- Δυνατότητα παραγωγής χρονικά προσδιορισμένων αναφορών προορισμένων για την ανώτερη και ανώτατη διοίκηση του οργανισμού.
- Δυνατότητα προσδιορισμού πολλαπλών 'Θεμάτων' το καθένα από τα οποία θα έχει ένα δέντρο αδυναμιών (διαφορετικό από τα άλλα θέματα), καθώς και διαφορετικό σύνολο χρηστών με διαφορετικά δικαιώματα και προτεραιότητες ανά 'Θέμα'.

Ως πρός τα κομμάτια που αναφέρονται σε επέκταση της εφαρμογής

- Δημιουργία βάσης γνώσης και χρησιμοποίησή της για αυτοματοποιημένες προτάσεις πάνω σε συγκεκριμένα προβλήματα.
- Αυτοματοποιημένο εντοπισμό γνωστών λύσεων στο Διαδίκτυο συσχετιζόμενες με τα δοθέντα στην εφαρμογή προβλήματα.