ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

«Συνεργατική πολυκριτηριακή διαχείριση ασφάλειας Πληροφοριακών Συστημάτων»

«Θεόδωρος Ν. Ντούσκας»

Επιβλέπουσα: Επίκουρος Καθηγήτρια Δ. Πολέμη

Πειραιάς, Σεπτέμβριος 2012

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

«Συνεργατική πολυκριτηριακή διαχείριση ασφάλειας Πληροφοριακών Συστημάτων»

«Θεόδωρος Ν. Ντούσκας»

Συμβουλευτική Επιτροπή : Δέσποινα Πολέμη

Χρήστος Δουληγέρης

Βασίλειος Χρυσικόπουλος

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 19η Σεπτεμβρίου 2012.

.....	.....	.....
Δέσποινα Πολέμη	Χρήστος Δουληγέρης	Βασίλειος Χρυσικόπουλος
Επ. Καθηγήτρια	Καθηγητής Πανεπιστημίου	Καθηγητής Ιονίου
Πανεπιστημίου Πειραιώς	Πειραιώς	Πανεπιστημίου
.....	.....	.....
Δημήτριος Γκρίτζαλης	Ιωάννης Χ. Παναγιωτόπουλος	Ιωάννης Σίσκος
Καθηγητής Οικονομικού	Καθηγητής Πανεπιστημίου	Καθηγητής Πανεπιστημίου
Πανεπιστημίου Αθηνών	Πειραιώς	Πειραιώς

.....

Ιωάννης Ψαρράς

Καθηγητής ΕΜΠ

Πειραιάς, Σεπτέμβριος 2012

.....

Θεόδωρος Ν. Ντούσκας

Διδάκτωρ Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς

Αφιερώνεται στους γονείς μου

Ευχαριστίες

Αρχικά θα ήθελα να εκφράσω ένα μεγάλο ευχαριστώ στην επιβλέπουσα καθηγήτριά μου κ. Δέσποινα Πολέμη για την καθοδήγηση και το ενδιαφέρον της καθώς επίσης και για την τεράστια υπομονή και υποστήριξή της. Επίσης ευχαριστώ τους καθηγητές κ. Χρήστο Δουληγέρη και κ. Βασίλη Χρυσικόπουλο για τις πολύτιμες συμβουλές τους καθ' όλη την διάρκεια της διατριβής. Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή κ. Ιωάννη Σίσκο για την επιστημονική του καθοδήγηση, καθώς επίσης και τα υπόλοιπα μέλη της επταμελούς μου επιτροπής, τους καθηγητές κ. Δημήτρη Γκρίτζαλη, κ Ιωάννη Χ. Παναγιωτόπουλο και κ. Ιωάννη Ψαρρά. Οι παρατηρήσεις και τα σχόλια όλης της επταμελούς επιτροπής καθόρισαν σε πολύ μεγάλο βαθμό την αρτιότητα της διατριβής και με βοήθησαν να την βελτιώνω συνέχεια μέχρι την τελική μορφή της.

Κατά την εκπόνηση της διατριβής υπήρξαν αρκετοί φίλοι και συνάδελφοι που με στήριξαν σε δύσκολες στιγμές. Ο διδάκτορας Αθανάσιος Καραντζιάς, ο λέκτορας Παναγιώτης Κοτζανικολάου και ο διδάκτορας Σπύρος Παπαστεργίου ήταν από εκείνους τους ανθρώπους που βρίσκονταν από την αρχή στο πλευρό μου τόσο για να μου δώσουν συμβουλές για την διατριβή αλλά κυρίως ως φίλοι για να με βοηθήσουν με όποιο τρόπο μπορούσαν. Θα ήθελα να τους ευχαριστήσω ολόψυχα για τη συμπαράσταση και την υποστήριξή τους.

Σημαντικοί για μένα άνθρωποι με τους οποίους μπορούσα να μοιραστώ τις ανησυχίες, τις σκέψεις και τους προβληματισμούς μου και που θα ήθελα επίσης να ευχαριστήσω για την συμπαράστασή τους είναι ο Ανδρέας Ζαπάντης, ο Γρηγόρης Ζαπάντης, ο Δημήτρης Παπανίκας, ο Κλεάνθης Δέλλιος, ο Κώστας Παπαμιχαήλ, ο Γιώργος Πενταφρόνιμος, ο Διονύσης Σκούρας και ο Πάνος Χατζηνικολάου, όλοι πολύ καλοί φίλοι που αγαπώ πολύ.

Επίσης, θέλω να ευχαριστήσω ολόψυχα την Χριστίνα Ζυγούρη η οποία ήταν στο πλευρό μου από την αρχή έως το τέλος τη δύσκολης αυτής πορείας και μου έδινε κουράγιο και ψυχολογική υποστήριξη στο να συνεχίσω και να πετύχω τους στόχους μου.

Τέλος, ευχαριστώ την οικογένειά μου η οποία έχει παίξει ίσως τον σημαντικότερο ρόλο στο να μάθω να θέτω και να πραγματοποιώ στόχους στη ζωή μου και να προσπαθώ να βελτιώνομαι όσο μπορώ. Ελπίζω να τους έχω κάνει περήφανους.

Σεπτέμβριος, 2012

Θεόδωρος Ν. Ντούσκας

Επιτελική Σύνοψη

Η διαχείριση ασφάλειας του Πληροφοριακού Συστήματος (ΠΣ) ενός οργανισμού αποτελεί απαραίτητο συστατικό για την εύρυθμη λειτουργία του φορέα και την αδιάλειπτη παροχή υπηρεσιών.

Τα σημερινά πληροφοριακά συστήματα χαρακτηρίζονται από πολυπλοκότητα (πολύπλοκες αρχιτεκτονικές, κατανεμημένα σε πολλές διαφορετικές τοποθεσίες), αλληλεξαρτώνται από ΠΣ συνεργαζόμενων φορέων και καλούνται να εξυπηρετήσουν ταυτόχρονα πολλούς χρήστες (εσωτερικούς χρήστες, συνεργάτες, πελάτες) έχοντας να αντιμετωπίσουν τον υψηλό ανταγωνισμό και την οικονομική κρίση. Από την άλλη, οι μικρές και μικρομεσαίες επιχειρήσεις (ΜΜΕ) όπου ο αντίκτυπος της οικονομικής κρίσης είναι ορατός, μη έχοντας τους οικονομικούς πόρους αλλά ούτε και την απαραίτητη τεχνογνωσία, αδιαφορούν για την εναρμόνισή τους με τα πρότυπα ασφάλειας, με αποτέλεσμα να αποτελούν αδύναμο κρίκο τόσο για την εγχώρια όσο και για την παγκόσμια οικονομία.

Οι υφιστάμενες μεθοδολογίες και τα υπάρχοντα εργαλεία ανάλυσης και διαχείρισης κινδύνου δεν είναι σε θέση να ανταποκριθούν στις ανάγκες της σημερινής πραγματικότητας. Συγκεκριμένα, δεν μπορούν να καλύψουν τις αυξανόμενες ανάγκες των σημερινών πολύπλοκων και κατανεμημένων ΠΣ των μεγάλων οργανισμών αλλά ούτε και να ανταπεξέλθουν και να προσαρμοστούν στις ιδιαίτερες ανάγκες (χαμηλός προϋπολογισμός, έλλειψη τεχνογνωσίας) των ΠΣ των ΜΜΕ. Το γεγονός αυτό προκύπτει από το ότι οι υπάρχουσες μεθοδολογίες:

- ✓ είναι γενικές και δεν προσαρμόζονται εύκολα στις ανάγκες των διαφορετικής φύσεως οργανισμών,
- ✓ δεν υποστηρίζουν την συνεργατικότητα, δηλαδή δεν εμπλέκουν όλους τους χρήστες των ΠΣ, με αποτέλεσμα να μην συλλέγουν την απαραίτητη γνώση και να οδηγούνται σε μη αντικειμενικά αποτελέσματα,
- ✓ βασίζονται σε χρονοβόρα ερωτηματολόγια και συνεντεύξεις με τους ειδικούς πάνω σε θέματα ασφάλειας, και
- ✓ τα εργαλεία τα οποία τις υλοποιούν είναι συνήθως δύσχρηστα και απαιτούν εξειδικευμένη γνώση και πόρους (ανθρωποώρες, υψηλό κόστος), που στις περισσότερες περιπτώσεις (π.χ. στην περίπτωση των ΜΜΕ) δεν υπάρχει.

Επομένως, είναι επιτακτική ανάγκη η ύπαρξη αναβαθμισμένων μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας οι οποίες θα είναι σε θέση να αντιμετωπίσουν την σημερινή πραγματικότητα της διαχείρισης ασφάλειας ΠΣ, ενώ ταυτόχρονα θα συνοδεύονται από εύχρηστα

εργαλεία τα οποία θα μπορούν να αποτελέσουν σημαντικό εφόδιο για τις διοικήσεις τόσο των κρίσιμων υποδομών όσο και των ΜΜΕ.

Η παρούσα διατριβή, κατανοώντας τις αδυναμίες αυτές, αντιμετωπίζει το πρόβλημα της ανάλυσης και διαχείρισης επικινδυνότητας ως ένα πολυκριτηριακό πρόβλημα όπου συμμετέχουν πολλοί χρήστες (διαχειριστές, μέλη της διοίκησης, μέλη της ομάδας ασφάλειας και τελικοί χρήστες), οι οποίοι καλούνται να λύσουν τα εξής προβλήματα:

- ✓ εντοπισμός και αξιολόγηση των επιπτώσεων από την απώλεια ασφάλειας (απώλεια εμπιστευτικότητας, διαθεσιμότητας, ακεραιότητας) των αγαθών του ΠΣ του οργανισμού τους,
- ✓ εντοπισμός και αξιολόγηση των απειλών και αδυναμιών των αγαθών του ΠΣ του οργανισμού τους, και
- ✓ αξιολόγηση και επιλογή των κατάλληλων μέτρων προστασίας για την εξασφάλιση της ομαλής λειτουργίας του ΠΣ,

λαμβάνοντας υπόψη τα δικά τους κριτήρια (τεχνολογικά, επιχειρησιακά, νομικά) βασιζόμενοι στην εμπειρία και την τεχνογνωσία τους.

Συγκεκριμένα, συνδυάζοντας τις πολυκριτηριακές μεθοδολογίες ομαδικής λήψης αποφάσεων προτείνεται μια συνεργατική, πολυκριτηριακή μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας (STORM-RM) η οποία έχει ως στόχο την συλλογή της γνώσης (η οποία είναι διασκορπισμένη στους χρήστες των ΠΣ των οργανισμών), την ελάττωση των χρονοβόρων ερωτηματολογίων και συνεντεύξεων και την εξοικονόμηση πόρων.

Ταυτόχρονα, κάνοντας χρήση των προηγμένων τεχνολογιών Web 2.0 και άλλων ανοιχτού κώδικα επιλογών, προτείνεται ένα ασφαλές συνεργατικό περιβάλλον (STORM) το οποίο παρέχει την μεθοδολογία ως ηλεκτρονική υπηρεσία και συνδυάζοντας μια ομάδα συνεργατικών υπηρεσιών στοχεύει στην ολιστική, οικονομική και αποτελεσματική διαχείριση ασφάλειας των ΠΣ.

Τέλος, η παρούσα διατριβή, με στόχο να καλύψει τις ανάγκες διαφορετικής φύσεως ΠΣ, εξέτασε την εφαρμογή του συνεργατικού περιβάλλοντος και των υπηρεσιών του στα περιβάλλοντα των ΠΣ των εμπορικών λιμένων (τα οποία αποτελούν μεγάλης κλίμακας κρίσιμες υποδομές) καθώς και των ΜΜΕ.

Λέξεις - κλειδιά: συνεργατικότητα, πολυκριτηριακή ανάλυση αποφάσεων, ανάλυση επικινδυνότητας, διαχείριση επικινδυνότητας, διαχείριση ασφάλειας.

Abstract

Information Security Management is an important governance and administration procedure aiming at the protection of an organization from internal and external risks that could negatively affect the achievement of its operational objectives.

Current Information and Communication Systems (ICS) are characterized by growing complexity, distribution, interference and dependency with other ICS and by the plethora of the hosted electronic services. They are called to serve simultaneously several users (internal users, partners and customers), having to face the fierce competition, the economic crisis, and a growing number of different types of spatial and temporal attacks. On the other hand, small and medium sized enterprises (SMEs), where the impacts of the economic crisis are more visible, not having the financial resources and the necessary expertise to become harmonized with security standards, become the weak links for the domestic and the global economy.

The existing risk management methodologies and tools are not capable to meet the needs of today's reality. They can neither meet the growing needs of today's complex and distributed ICS nor can they cope and address these specific needs (low budget, lack of knowledge) of the SMEs, since the existing methodologies:

- ✓ are too generic and not tailored to the needs of organizations of different culture,
- ✓ do not support collaboration, i.e. they do not involve all the users of ICS (managers, administrators, members of the security team, end users) in order to collect the necessary knowledge leading to non-objective results,
- ✓ are based on time-consuming questionnaires and interviews with experts on security issues, and
- ✓ the tools which implement them are often difficult to use and require specialized knowledge and resources (man-hours, high cost), which in most cases (e.g. in the case of SMEs) are not available.

Therefore, it is essential to enhance the risk management methodologies in order to meet the security needs of today's ICS, implemented in automated, collaborative tools, making them an important asset for their governance.

Realizing these weaknesses and needs, this Ph.D. thesis proposes to view the problem of analyzing and managing risk as a multicriteria decision making problem involving many users (managers, administrators, members of the security team and end users) who are asked to solve the following complex decision problems:

- ✓ categorise the importance for the organisation (impact level) of its ICS assets, i.e., physical infrastructure (data centres, computer rooms and buildings), networks, servers, software, services and ICS participants,
- ✓ prioritise the ICS threats (potential causes of unwanted incidents which may result in harm to ICS,
- ✓ prioritise vulnerabilities (weaknesses of an ICS asset(s) that may be exploited by a threat(s),
- ✓ estimate the threat and vulnerability levels, and
- ✓ select the appropriate countermeasures.

Each of the above decision problems involves multiple criteria and objectives of conflicting nature including security (integrity, availability and confidentiality), business, cost, technological and legal with respect to all the ICS participants' experiences and preferences.

Specifically, by combining multi-criteria group decision-making methodologies a collaborative, multi-criteria risk management methodology (STORM-RM) is proposed, which aims to gather knowledge (which is dispersed among organization users), reducing the time-consuming questionnaires and interviews and saving resources.

Additionally, with the use of advanced Web 2.0 technologies and other open source solutions, a secure collaborative environment (STORM) is proposed, which provides the risk management methodology as an online service (each phase of STORM -RM methodology has been implemented as a distinct module in the STORM environment) and aims at holistic, effective and efficient ICS security management by combining a group of collaborative services.

Finally, the PhD candidate implemented the collaborative environment STORM and its services in the complex ports' ICS (which are large-scale critical information infrastructures) and the SMEs in order to meet the needs of these different type infrastructures.

Key - words: collaboration, multicriteria decision making, risk analysis, risk management, security management.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Εισαγωγή 23
1.1 Αντικείμενο και στόχος της διατριβής 24
1.2 Δομή της διατριβής 26
1.3 Βασικοί ορισμοί - Συντομογραφίες 28
2 Πρότυπα και μεθοδολογίες Ανάλυσης και Διαχείρισης Ασφάλειας ΠΣ 31
2.1 Εισαγωγή 31
2.2 Πρότυπα Διαχείρισης Ασφάλειας 31
2.2.1 Το πρότυπο ISO / IEC 27001:2005 31
2.2.2 Το πρότυπο ISO / IEC 27005:2008 32
2.2.3 Το πρότυπο ISO / IEC 27002:2005 33
2.2.4 Το πρότυπο AS / NZS 4360 33
2.2.5 Το πρότυπο NIST SP 800-30 35
2.3 Μεθοδολογίες Ανάλυσης και Διαχείρισης Επικινδυνότητας 37
2.3.1 CRAMM 37
2.3.2 EBIOS 38
2.3.3 OCTAVE 39
2.3.4 MEHARI 40
2.3.5 MAGERIT 41
2.4 Ανοιχτά προβλήματα - Συνεισφορά διατριβής 43
2.5 Βιβλιογραφία 2ου Κεφαλαίου 46
3 Η Ανάλυση και Διαχείριση Επικινδυνότητας ως πολυκριτηριακό πρόβλημα 49
3.1 Εισαγωγή 49
3.2 Πολυκριτηριακή λήψη αποφάσεων 50
3.3 Υπάρχουσες πολυκριτηριακές μέθοδοι λήψης αποφάσεων 53
3.4 Analytical Hierarchy Process (AHP) 56
3.5 Συμπεράσματα Κεφαλαίου 64
3.6 Βιβλιογραφία 3ου Κεφαλαίου 65
4 Συνεργατική Μεθοδολογία Ανάλυσης και Διαχείρισης Επικινδυνότητας (STORM-RM) 67
4.1 Εισαγωγή 67

4.2 Πεδίο εφαρμογής και στόχοι 67
4.3 Απαιτήσεις και χαρακτηριστικά της STORM-RM 68
4.3.1 Απαιτήσεις της STORM-RM 68
4.3.2 Χαρακτηριστικά της STORM-RM 69
4.4 Αναλυτική περιγραφή της μεθοδολογίας STORM-RM 71
4.4.1 Φάση 1: Χαρτογράφηση 71
4.4.1.1 Βήμα 1.1: Προσδιορισμός κρίσιμων η-υπηρεσιών 73
4.4.1.2 Βήμα 1.2: Καταγραφή αγαθών 75
4.4.1.3 Βήμα 1.3: Αλληλεξαρτήσεις αγαθών 77
4.4.1.4 Βήμα 1.4: Υπάρχοντα μέτρα προστασίας / διαδικασίες ασφάλειας 78
4.4.2 Φάση 2: Αποτίμηση Επιπτώσεων Ασφάλειας 78
4.4.2.1 Κατηγορίες επιπτώσεων 78
4.4.2.2 Κλίμακα επιπτώσεων 80
4.4.2.3 Βήμα 2.1: Ατομική αποτίμηση 80
4.4.2.4 Βήμα 2.2: Ομαδική αποτίμηση 85
4.4.2.5 Βήμα 2.3: Συνολική αποτίμηση 85
4.4.3 Φάση 3: Αποτίμηση Απειλών 90
4.4.3.1 Βήμα 3.1: Προσδιορισμός Απειλών 90
4.4.3.2 Βήμα 3.2: Αποτίμηση απειλών 91
4.4.4 Φάση 4: Αποτίμηση αδυναμιών 94
4.4.4.1 Βήμα 4.1: Προσδιορισμός αδυναμιών 94
4.4.4.2 Βήμα 4.2: Θεωρητική Αποτίμηση Αδυναμιών 95
4.4.4.3 Βήμα 4.3: Πρακτική Αποτίμηση Αδυναμιών 97
4.4.4.4 Βήμα 4.4: Συνολική Αποτίμηση Αδυναμιών 103
4.4.5 Φάση 5: Αποτίμηση επικινδυνότητας 104
4.4.5.1 Βήμα 5.1: Υπολογισμός επιπέδων κινδύνου 104
4.4.5.2 Βήμα 5.2: Προσδιορισμός Επικινδυνότητας 106
4.4.6 Φάση 6: Μέτρα προστασίας - Σχέδιο Ασφάλειας 107
4.4.6.1 Βήμα 6.1: Προτεινόμενα μέτρα ασφάλειας 107
4.4.6.2 Βήμα 6.2: Επιλογή κατάλληλων μέτρων ασφάλειας 107
4.4.7 Φάση 7: Αναφορές Ανάλυσης Επικινδυνότητας 108

4.5 Συμπεράσματα κεφαλαίου 110
4.6 Βιβλιογραφία 4ου Κεφαλαίου 111
5 Συνεργατικό περιβάλλον διαχείρισης ασφάλειας (STORM) 113
5.1 Εισαγωγή 113
5.2 Συνεργατική Διαχείριση Κινδύνων (ΔΚ) 115
5.3 Απαιτήσεις συνεργατικού περιβάλλοντος STORM 115
5.3.1 Ασφάλεια 115
5.3.2 Επεκτασιμότητα 116
5.3.3 Διαλειτουργικότητα 116
5.3.4 Απλότητα στην χρήση 116
5.3.5 Εικονοποίηση 117
5.3.6 Αισθητική 117
5.3.7 Ευκολία στην εκμάθηση 117
5.3.8 Αποφυγή σύγχυσης του χρήστη 117
5.3.9 Δυνατότητα αποφυγής λαθών και εύκολης διαχείρισης λαθών 117
5.4 Αρχιτεκτονική και Τεχνολογίες του STORM 118
5.4.1 Κύρια Πλατφόρμα 119
5.4.1.1 Δικτυακό-Διαδραστικό Επίπεδο (Web Interactive Tier) 119
5.4.1.2 Επιχειρησιακό Επίπεδο (Enterprise Tier) 121
5.4.1.3 Επίπεδο Βάσης Δεδομένων (Database Tier) 125
5.4.2 Συστήματα STORM 126
5.4.2.1 Δίαυλος Επιχειρησιακών Υπηρεσιών 126
5.4.2.2 Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών 127
5.4.2.3 Σύστημα Διαχείρισης Ταυτοτήτων 129
5.5 Ομάδες Χρηστών STORM 130
5.6 Υπηρεσίες STORM 133
5.6.1 Υπηρεσίες ανάλυσης και διαχείρισης επικινδυνότητας - STORM-RM 133
5.6.1.1 Υπηρεσία Χαρτογράφησης 133
5.6.1.2 Υπηρεσία Αποτίμησης Επιπτώσεων Ασφάλειας 139
5.6.1.3 Υπηρεσία Αποτίμησης Απειλών 143
5.6.1.4 Υπηρεσία Αποτίμησης Αδυναμιών 146

5.6.1.5 Υπηρεσία Αποτίμησης Επικινδυνότητας 149
5.6.1.6 Υπηρεσίες Διαχείρισης Επικινδυνότητας 150
5.6.2 Υπηρεσία Διαχείρισης Εγγράφων Ασφάλειας 152
5.6.3 Συνεργατικές Υπηρεσίες STORM 154
5.6.3.1 Forum 155
5.6.3.2 Wiki 156
5.6.3.3 Chat rooms 157
5.6.3.4 Blog 159
5.6.3.5 Ηλεκτρονική Βιβλιοθήκη 160
5.7 Συμπεράσματα - Ανοιχτά θέματα 163
5.8 Βιβλιογραφία 5ου Κεφαλαίου 165
6 Μελέτες περίπτωσης 167
6.1 Εισαγωγή 167
6.2 Συνεργατική ΔΑ των ΠΣ εμπορικών λιμένων 167
6.2.1 ΠΣ εμπορικών λιμένων 167
6.2.2 Υφιστάμενη κατάσταση στη διαχείριση ασφάλειας ΠΣ εμπορικών λιμένων 171
6.2.3 Ανοιχτά θέματα - Συνεισφορά διατριβής 173
6.2.4 S-PORT: συνεργατικό περιβάλλον ΔΑ των ΠΣ εμπορικών λιμένων 175
6.2.5 Συμπεράσματα – Ανοιχτά θέματα 180
6.3 Μελέτη περίπτωσης στα ΠΣ μικρών, μεσαίων και πολύ μικρών επιχειρήσεων (ΜΜΕ) 181
6.3.1 ΜΜΕ 181
6.3.2 Υφιστάμενη κατάσταση στη διαχείριση ασφάλειας ΠΣ ΜΜΕ 183
6.3.2.1 Πρότυπα Διαχείρισης Ασφάλειας ΠΣ ΜΜΕ 183
6.3.2.2 Μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας 184
6.3.2.3 Προσεγγίσεις και εργαλεία πρακτικής ανάλυσης Αδυναμιών 186
6.3.3 Ανοιχτά θέματα - Συνεισφορά διατριβής 187
6.3.4 Συνεργατικό εργαλείο για την διαχείριση ασφάλειας των ΠΣ ΜΜΕ 189
6.3.5 Συμπεράσματα – Ανοιχτά θέματα 192
6.4 Βιβλιογραφία 6ου Κεφαλαίου 194
7 Επίλογος - Μελλοντικές ερευνητικές κατευθύνσεις 201
8 Παραρτήματα 205

8.1 Παράρτημα Ι: Ερωτηματολόγια μεθοδολογίας 205
8.1.1 Ερωτηματολόγια αποτίμησης επιπτώσεων 205
8.1.2 Ερωτηματολόγια αποτίμησης απειλών 213
8.1.3 Ερωτηματολόγια αποτίμησης αδυναμιών 213
8.2 Παράρτημα ΙΙ: Πίνακες αντιστοίχισης αγαθών / απειλών / αδυναμιών 214
8.3 Παράρτημα ΙΙΙ: Ταξονομία STORM 282
8.4 Παράρτημα IV: Πρότυπο αναπαράστασης υπηρεσιών 283
8.5 Παράρτημα V: Υπόδειγμα αναφορών μεθοδολογίας STORM-RM 286
8.5.1 Λίστα αγαθών και αλληλεξαρτήσεων 286
8.5.2 Αναφορά Ανάλυσης Επικινδυνότητας 287
8.5.3 Αναφορά κατάλληλων μέτρων προστασίας 293

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

Εικόνα 1: Βασικά βήματα του AS/NZS 4360....34
Εικόνα 2: Στάδια λήψης απόφασης....51
Εικόνα 3: Ιεραρχική Δομή Προβλήματος....57
Εικόνα 4: Ιεραρχική δομή του προβλήματος επιλογής μέτρου ασφάλειας....61
Εικόνα 5: Φάσεις Μεθοδολογίας STORM-RM....71
Εικόνα 6: Βασικά Βήματα της Φάσης Χαρτογράφησης....72
Εικόνα 7: Δένδρο απόφασης AHP για την κρισιμότητα των η-υπηρεσιών....74
Εικόνα 8: Μοντέλο Ομάδων χρηστών (User Group Model)....76
Εικόνα 9: Δένδρο αλληλεξαρτήσεων (Asset Group Model)....77
Εικόνα 10: Δένδρο Απόφασης για τον υπολογισμό των βαρών συμμετοχής στην αποτίμηση Δεδομένων....81
Εικόνα 11: Δένδρο Απόφασης για τον υπολογισμό των βαρών συμμετοχής στην αποτίμηση Συστημάτων..83
Εικόνα 12: Δένδρο Απόφασης-Ομαδικής Αποτίμησης Απειλών....92
Εικόνα 13: Ομαδική Θεωρητική Αποτίμηση Αδυναμιών....96
Εικόνα 14: Δένδρο Απόφασης AHP για την επιλογή των μέτρων προς υλοποίηση....107
Εικόνα 15: Αρχιτεκτονική συνεργατικού περιβάλλοντος STORM....118
Εικόνα 16: Δικτυακό - Διαδραστικό Επίπεδο....119
Εικόνα 17: Επιχειρησιακό Επίπεδο....122
Εικόνα 18: Ανταλλαγή μηνυμάτων αυθεντικοποίησης χρηστών....124
Εικόνα 19: Επικοινωνία Κύριας Πλατφόρμας - Δίαυλος Επ. Υπηρεσιών - Σύστημα Δ. Επ. Διαδικασιών..129
Εικόνα 20: Σύστημα Διαχείρισης Ταυτοτήτων....130
Εικόνα 21: Υπηρεσίες συνεργατικού περιβάλλοντος STORM....133
Εικόνα 22: Καταγραφή των υπηρεσιών από τον Νόμιμο Εκπρόσωπο....135
Εικόνα 23: Καταγραφή των εμπλεκόμενων χρηστών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους....136
Εικόνα 24: Καταγραφή των δεδομένων και των συστημάτων ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Α'τρόπος)....137
Εικόνα 25: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Β' τρόπος)....138
Εικόνα 26: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διαχειριστές....139
Εικόνα 27: Αποτίμηση των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας ασφάλειας και τα μέλη της Διοίκησης....140
Εικόνα 28: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης....141
Εικόνα 29: Αποτίμηση των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες....142

Εικόνα 30: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες....143
Εικόνα 31: Αποτίμηση των απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης....144
Εικόνα 32: Προβολή αποτελεσμάτων αποτίμησης απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης....145
Εικόνα 33: Αποτίμηση των απειλών από τους Διαχειριστές και τους Τελικούς Χρήστες....146
Εικόνα 34: Αποτίμηση των αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης..147
Εικόνα 35: Προβολή αποτελεσμάτων αποτίμησης αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης....148
Εικόνα 36: Αποτίμηση των αδυναμιών από τους Διαχειριστές και τους Τελικούς Χρήστες....149
Εικόνα 37: Προβολή των αποτελεσμάτων επικινδυνότητας από τον Νόμιμο Εκπρόσωπο, τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης....150
Εικόνα 38: Προβολή και επιλογή τελικών μέτρων ασφάλειας από τον Υπεύθυνο Ασφάλειας....152
Εικόνα 39: Δημιουργία της πολιτικής ασφάλειας από τον Υπεύθυνο Ασφάλειας....153
Εικόνα 40: Προβολή της πολιτικής ασφάλειας από όλες τις ομάδες χρηστών....154
Εικόνα 41: Δημιουργία Θέματος από όλες τις ομάδες χρηστών....155
Εικόνα 42: Απάντηση σε Θέμα του Forum από όλες τις ομάδες χρηστών....156
Εικόνα 43: Συνεισφορά στο wiki από όλες τις ομάδες χρηστών....157
Εικόνα 44: Συζήτηση με ανταλλαγή μηνυμάτων σε πραγματικό χρόνο από όλες τις ομάδες χρηστών....158
Εικόνα 45: Δημιουργία δημοσίευσης από τους Διαχειριστές και τα μέλη της Ομάδας ασφάλειας....159
Εικόνα 46: Απάντηση σε Δημοσίευση του Blog από όλες τις ομάδες χρηστών....160
Εικόνα 47: Ανάρτηση εγγράφου στην η-βιβλιοθήκη....161
Εικόνα 48: Αναζήτηση εγγράφου στην η-βιβλιοθήκη....162
Εικόνα 49: Περιβάλλον ναυτιλίας....168
Εικόνα 50: Ασφάλεια (security) και Φυσική ασφάλεια (safety)....170
Εικόνα 51: Ηλεκτρονικό ερωτηματολόγιο αποτίμησης επιπτώσεων....176
Εικόνα 52: Απεικόνιση αποτελεσμάτων αποτίμησης επιπτώσεων....177
Εικόνα 53: Ηλεκτρονικό ερωτηματολόγιο αποτίμησης αδυναμιών....177
Εικόνα 54: Απεικόνιση αποτελεσμάτων ανάλυσης επικινδυνότητας....178
Εικόνα 55: Επιλογή μέτρων ασφάλειας προς υλοποίηση....178
Εικόνα 56: Ηλεκτρονική φόρμα δημιουργίας της πολιτικής ασφάλειας του ΠΣ λιμένα....179
Εικόνα 57: Ηλεκτρονική βιβλιοθήκη του S-PORT....179
Εικόνα 58: Περιβάλλον STORM....189
Εικόνα 59: Υπηρεσίες STORM προσανατολισμένες σε χρήστες MME....190

Εικόνα 60: Απεικόνιση αποτελεσμάτων Ανάλυσης Επικινδυνότητας από τους κατάλληλους χρήστες των ΜΜΕ....191
Εικόνα 61: Διαχείριση Απειλών από τους συμβούλους ασφάλειας....192

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

Πίνακας 1: Υπάρχουσες μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας....43
Πίνακας 2: Αριθμητική Κλίμακα σημαντικότητας Saaty [13][14]....57
Πίνακας 3: Πίνακας Συγκρίσεων AHP....58
Πίνακας 4: Παράδειγμα Πίνακας Συγκρίσεων AHP....58
Πίνακας 5: Πίνακας Τυχαίων Δεικτών (Random Consistency Index)....59
Πίνακας 6: Υπολογισμός Προτεραιοτήτων....60
Πίνακας 7: Πίνακας Συγκρίσεων 1ου επιπέδου....61
Πίνακας 8: Πίνακας Προτεραιοτήτων 1ου Επιπέδου....62
Πίνακας 9: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κόστος Αγοράς....62
Πίνακας 10: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κόστος Συντήρησης....62
Πίνακας 11: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Αξιοπιστία....63
Πίνακας 12: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Αποτελεσματικότητα....63
Πίνακας 13: Τελικές Προτεραιότητες Εναλλακτικών....63
Πίνακας 14: Κλίμακα Αποτίμησης Επιπτώσεων....80
Πίνακας 15: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Επιχειρησιακών Στόχων....82
Πίνακας 16: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Επιχειρησιακών Κινδύνων....82
Πίνακας 17: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κατανόηση Επιχειρησιακής Αξίας των Δεδομένων....82
Πίνακας 18: Βάρη συμμετοχής στην αποτίμηση των Δεδομένων....82
Πίνακας 19: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Πληροφοριακών Στόχων....83
Πίνακας 20: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Πληροφοριακών Κινδύνων....83
Πίνακας 21: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κατανόηση Επιχειρησιακής Αξίας των Συστημάτων....84
Πίνακας 22: Βάρη συμμετοχής στην αποτίμηση των Συστημάτων....84
Πίνακας 23: Αποτελέσματα Αποτίμησης Επιπτώσεων....86
Πίνακας 24: Υπολογισμός των βαθμών αποτίμησης επιπτώσεων ενός αγαθού A_i....89
Πίνακας 25: Αντιστοίχιση Αγαθών -Απειλών....91
Πίνακας 26: Κλίμακα αποτίμησης Απειλών....91
Πίνακας 27: Ατομική αποτίμηση απειλών (χρήστης P_2)....92

Πίνακας 28: Ομαδικά Αποτελέσματα 93
Πίνακας 29: Υπολογισμός επιπέδου απειλής για το αγαθό A_1 93
Πίνακας 30: Παράδειγμα αντιστοίχισης Είδους αγαθού/Απειλών/Αδυναμιών 94
Πίνακας 31: Κλίμακα Αποτίμησης Αδυναμιών 95
Πίνακας 32: Ομαδική Θεωρητική Αποτίμηση Αδυναμιών 96
Πίνακας 33: Πίνακας Επικινδυνότητας (Risk Level Evaluation Matrix) 105
Πίνακας 34: Κλίμακα Αποτίμησης Επικινδυνότητας 106
Πίνακας 35: Πίνακας Επικινδυνότητας (Risk Level Evaluation Matrix) 106
Πίνακας 36: Νέα Αντικείμενα Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών 128
Πίνακας 37: Υπάρχουσες μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας 184

Κεφάλαιο 1ο

1 Εισαγωγή

Τα πιο κρίσιμα και ευαίσθητα δεδομένα των οργανισμών φιλοξενούνται στα Πληροφοριακά τους Συστήματα (ΠΣ). Πιθανή υποβάθμιση, δυσλειτουργία ή διακοπή των ΠΣ έχει σημαντικές επιπτώσεις στην ασφάλεια, στην απώλεια δεδομένων, στην απώλεια φήμης και στην απώλεια διαθεσιμότητας των υπηρεσιών με αποτέλεσμα η ασφάλεια ενός ΠΣ να είναι ένα από τα πιο σημαντικά θέματα που πρέπει να λάβουν υπόψη τους οι οργανισμοί. Το γεγονός ότι τα σημερινά ΠΣ χαρακτηρίζονται πλέον από:

- ✓ αυξανόμενη πολυπλοκότητα,
- ✓ κατανεμημένη φύση και διασπορά όλων των συστατικών τους (δίκτυα, λογισμικό, υλικό, εφαρμογές, υπηρεσίες και ανθρώπινο δυναμικό),
- ✓ πληθώρα και διαφορετικής φύσης ηλεκτρονικές υπηρεσίες που προσφέρουν,
- ✓ αλληλεπίδραση - αλληλεξάρτηση με ΠΣ άλλων οργανισμών,
- ✓ απαίτηση των χρηστών για ασφαλείς, έμπιστες η-υπηρεσίες, με σεβασμό της ιδιωτικότητας τους,

δημιουργούν στη διαχείριση ασφάλειας μια μεγάλη πρόκληση.

Με τον όρο Διαχείριση Ασφάλειας ενός ΠΣ[1] εννοούμε την αποτελεσματική εφαρμογή, δημιουργία, αξιολόγηση, παρακολούθηση, βελτίωση και έλεγχο της ασφάλειας των ΠΣ. Η διαχείριση της ασφάλειας ΠΣ απαιτεί συνεχή και συστηματική διαδικασία προσδιορισμού, ανάλυσης, μετριασμού και ελέγχου των τεχνικών, λειτουργικών και άλλων τύπων κινδύνων, καθώς και την εφαρμογή των ενδεδειγμένων μέτρων ασφάλειας και ελέγχων για την σωστή εφαρμογή τους.

Οι υπάρχουσες μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας, καθώς και τα εργαλεία που τις υλοποιούν δεν είναι σε θέση να καλύψουν τις αυξανόμενες ανάγκες των σημερινών κατανεμημένων, πολύπλοκων και πολυδιάστατων οργανισμών αφού απαιτούν μια πληθώρα συνεντεύξεων με τους διαχειριστές των συστημάτων οι οποίες είναι χρονοβόρες, κοστίζουν στην διοίκηση και δεν έχουν τη δυνατότητα να λάβουν υπόψη τους την συλλογική γνώση όλων των

[1] Σωκρ. Κάτσικας - Δ. Γκρίτζαλης - Στεφ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», ISBN: 960-8105-57-9, Εκδόσεις Νέων Τεχνολογιών, Έκδοση: 1η 2004.

χρηστών του οργανισμού, με αποτέλεσμα να οδηγούμαστε σε περιορισμένα και μονόπλευρα συμπεράσματα.

Ταυτόχρονα, δεν υπάρχουν αυτοματοποιημένα συνεργατικά εργαλεία τα οποία να ενσωματώνουν πρότυπα ασφάλειας, μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας και οδηγίες για τους χρήστες των οργανισμών ώστε να είναι σε θέση:

- ✓ να προσδιορίζουν, αξιολογούν και κατηγοριοποιούν τις περιοχές επικινδυνότητας του οργανισμού,
- ✓ να αναγνωρίζουν τις επιπτώσεις που θα έχει ένα σοβαρό περιστατικό στην λειτουργία των οργανισμών,
- ✓ να διεξάγουν πρακτική ανάλυση αδυναμιών,
- ✓ να επιλέγουν κατάλληλα και αξιόπιστα μέτρα προστασίας ώστε να επιτυγχάνεται η διαθεσιμότητα και η ακεραιότητα των δεδομένων,
- ✓ να καθορίζουν μία επίσημη διαδικασία που θα ακολουθηθεί σε περίπτωση καταστροφής,
- ✓ να αναπτύσσουν μία αποτελεσματική στρατηγική τήρησης αντιγράφων ασφαλείας και ανάκτησης δεδομένων ώστε να ελαχιστοποιείται η επίπτωση τυχόν καταστροφών,
- ✓ να έχουν την δυνατότητα συνεχούς ενημέρωσης των σχεδίων Επιχειρησιακής Συνέχειας και Αποκατάστασης Καταστροφών και της Πολιτικής Ασφάλειας του οργανισμού τους, και
- ✓ να ενημερώνονται για τους νέους νόμους και πρότυπα που θα πρέπει να ακολουθεί η πολιτική ασφάλειας του οργανισμού τους.

1.1 Αντικείμενο και στόχος της διατριβής

Στόχος της παρούσας διατριβής είναι να συνεισφέρει στους παραπάνω δύο άξονες. Συγκεκριμένα, προτείνει μία νέα συνεργατική μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας, την STORM-RM (Secure Tool for Risk Management – Risk management Methodology), η οποία εμπλέκει όλους τους χρήστες του υπό εξέταση οργανισμού στις διαδικασίες και τα βήματα της ανάλυσης και διαχείρισης επικινδυνότητας. Η προτεινόμενη μεθοδολογία προτείνει έναν νέο τρόπο χαρτογράφησης των αγαθών ενός ΠΣ ο οποίος στοχεύει στην αποτύπωση των αλληλεξαρτήσεων των υπηρεσιών αλλά και των ίδιων των οργανισμών από τυχόν συνεργαζόμενους φορείς. Παράλληλα, με τον τρόπο με τον οποίο γίνεται η χαρτογράφηση στην STORM-RM απλοποιείται σε μεγάλο βαθμό ο αριθμός των ερωτηματολογίων και των συνεντεύξεων, καθώς οι συμμετέχοντες χρήστες συνδέονται ανάλογα με τον ρόλο τους στον οργανισμό με τις υπηρεσίες και τα αγαθά τα οποία χρησιμοποιούν ή είναι υπεύθυνοι.

Ταυτόχρονα, η προτεινόμενη μεθοδολογία αντιμετωπίζει την ανάλυση και διαχείριση επικινδυνότητας ως πολυκριτηριακό πρόβλημα όπου εμπλέκονται πολλοί συμμετέχοντες (τα μέλη της διοίκησης, οι διαχειριστές, τα μέλη της ομάδας ασφάλειας και οι τελικοί χρήστες των ΠΣ), έχοντας διαφορετικές απόψεις και εκτιμήσεις, ο καθένας από την δική του οπτική γωνία (επιχειρηματική / νομική / τεχνική), βασισμένοι στις γνώσεις και τις εμπειρίες τους. Στον αλγόριθμο υπολογισμού της προτεινόμενης μεθοδολογίας, χρησιμοποιείται η πολυκριτηριακή μεθοδολογία «Μέθοδος της Αναλυτικής Ιεράρχησης» (Analytical Hierarchy Process, AHP). Πιο αναλυτικά, χρησιμοποιούνται βάρη συμμετοχής των διαφόρων ομάδων χρηστών που παίρνουν μέρος στην διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας και με αυτόν τον τρόπο λαμβάνονται υπόψη οι διαφορετικές γνώμες των συμμετεχόντων και οδηγούμαστε σε πιο αντικειμενικά αποτελέσματα.

Τέλος, ένα ακόμα καινοτόμο σημείο της μεθοδολογίας είναι ο τρόπος επιλογής των προτεινόμενων μέτρων προστασίας. Στην φάση επιλογής των προτεινόμενων μέτρων η STORM-RM εμπλέκει τις κατάλληλες ομάδες χρηστών, όπου ο καθένας βάζει τα δικά του κριτήρια αξιολόγησης για την σύγκριση της αποτελεσματικότητας των μέτρων προστασίας τους ΠΣ του οργανισμού τους. Έτσι επιτυγχάνεται ο προσδιορισμός και η τελική επιλογή των πιο αναγκαίων μέτρων προστασίας τα οποία θα είναι σε θέση να καλύψουν τις τεχνολογικές, οικονομικές και επιχειρησιακές ανάγκες του οργανισμού.

Η δεύτερη συνεισφορά της διατριβής είναι η ανάπτυξη ενός συνεργατικού περιβάλλοντος, το οποίο θα βοηθήσει στην ολιστική διαχείριση της ασφάλειας των ΠΣ των οργανισμών. Κάνοντας χρήση των συνεργατικών τεχνολογιών Web 2.0 καθώς και άλλων σύγχρονων αυτοματοποιημένων, ανοιχτών, διαδραστικών και αξιόπιστων τεχνολογικών εργαλείων, αναπτύχθηκε το συνεργατικό περιβάλλον STORM (Secure Tool for Risk Management). Οι βασικοί στόχοι του προτεινόμενου περιβάλλοντος είναι η *συλλογή της γνώσης όλων των χρηστών* και η *συνεργατική διαχείριση της ασφάλειας* του ΠΣ του οργανισμού. Για την επίτευξη των στόχων αυτών, το περιβάλλον STORM ενσωματώνει την προτεινόμενη μεθοδολογία, η οποία παρέχεται ως υπηρεσία. Αποτέλεσμα αυτής της προσέγγισης είναι η αυτοματοποιημένη ανάλυση και διαχείριση επικινδυνότητας με φιλικό και εύχρηστο τρόπο, μέσα από τις διαδραστικές οθόνες του εργαλείου. Συγκεκριμένα, όλες οι φάσεις τις μεθοδολογίας έχουν υλοποιηθεί ως ανεξάρτητα υποσυστήματα τα οποία συλλέγουν την απαραίτητη πληροφορία με την βοήθεια ηλεκτρονικών φορμών, επεξεργάζονται τα δεδομένα εισόδου σύμφωνα με τον αλγόριθμο STORM-RM και παρουσιάζουν τα αποτελέσματα στους χρήστες με διάφορους τρόπους, όπως με τη βοήθεια γραφημάτων, με την μορφή εγγράφων PDF κτλ.

Σημαντική υπηρεσία του περιβάλλοντος STORM είναι η διαχείριση εγγράφων ασφαλείας. Με την συγκεκριμένη υπηρεσία, οι κατάλληλοι χρήστες του οργανισμού (τα μέλη της διοίκησης, τα

μέλη της ομάδας ασφάλειας και οι διαχειριστές) είναι σε θέση να σχεδιάζουν και να αποτυπώνουν τις διαδικασίες της πολιτικής ασφάλειας, καθώς επίσης και να προσδιορίζουν και να καταγράφουν τις απαραίτητες φάσεις ανάκαμψης των Σχεδίων Αποκατάστασης Καταστροφών και Επιχειρησιακής Συνέχειας, με την βοήθεια ειδικά διαμορφωμένων ηλεκτρονικών φορμών. Με αυτό τον τρόπο, είναι σε θέση να δημιουργούν, να ανανεώνουν και να επικαιροποιούν τα έγγραφα ασφάλειας, ενώ οι τοπικοί χρήστες του οργανισμού έχουν την δυνατότητα να γνωρίζουν ανά πάσα στιγμή την επικαιροποημένη πολιτική ασφάλειας του ΠΣ το οποίο χρησιμοποιούν ενώ αντίστοιχα να γνωρίζουν τους ρόλους και τις αρμοδιότητές τους σε περίπτωση που ενεργοποιηθούν τα Σχέδια Αποκατάστασης Καταστροφών και Επιχειρησιακής Συνέχειας.

Ταυτόχρονα, το προτεινόμενο περιβάλλον είναι εφοδιασμένο με μια ομάδα Web 2.0 υπηρεσιών όπως Forum, Blog, Wiki, Chat room και Ηλεκτρονική Βιβλιοθήκη, οι οποίες έχουν στόχο την ενημέρωση και την εκπαίδευση των χρηστών πάνω σε θέματα ασφάλειας, ενώ παράλληλα μπορούν να χρησιμοποιηθούν για την άμεση εύρεση λύσης και ανταπόκρισης σε περίπτωση κάποιου κακόβουλου περιστατικού ασφάλειας.

Για την καλύτερη αποτύπωση της ανάγκης ύπαρξης μιας νέας συνεργατικής μεθοδολογίας ανάλυσης και διαχείρισης επικινδυνότητας, αλλά και ενός περιβάλλοντος το οποίο θα παρέχει την μεθοδολογία σαν υπηρεσία και θα πλαισιώνεται από ένα σύνολο υπηρεσιών, παρουσιάζονται δύο μελέτες περίπτωσης χρήσης. Συγκεκριμένα, εξετάζεται και παρουσιάζεται η εφαρμογή του συνεργατικού περιβάλλοντος και των υπηρεσιών του στα ΠΣ εμπορικών λιμένων (αντιπροσωπευτικό παράδειγμα κρίσιμων υποδομών μεταφορών) και στα ΠΣ μικρών, μεσαίων και μικρομεσαίων επιχειρήσεων (οι οποίες είναι μικρής κλίμακας εμπορικές υποδομές πληροφορικής) και αποδεικνύεται ότι η ύπαρξη συνεργατικότητας στην διαχείριση της ασφάλειας είναι πλέον επιτακτική ανάγκη τόσο σε μικρής όσο και σε μεγάλης κλίμακας ΠΣ. Στην μεν πρώτη κατηγορία ΠΣ, η ανάγκη συνεργατικότητας πηγάζει από το μεγάλο πλήθος των χρηστών που η συλλογική τους γνώση συνεισφέρει στην αντικειμενικότερη αξιολόγηση των πληροφοριακών κινδύνων. Στη δεύτερη κατηγορία η ανάγκη για συνεργατικότητα πηγάζει από την απόκτηση γνώσης από παρόμοιους οργανισμούς.

1.2 Δομή της διατριβής

Η διδακτορική διατριβή αποτελείται από επτά (7) κεφάλαια. Στο Κεφάλαιο 2 παρουσιάζονται οι κύριες μεθοδολογίες Ανάλυσης και Διαχείρισης Επικινδυνότητας (ΑΔΕ), τα βήματα από τα οποία

αποτελούνται, καθώς και οι αδυναμίες οι οποίες εντοπίστηκαν. Το κεφάλαιο αυτό κλείνει με τα ανοιχτά προβλήματα που εντοπίστηκαν και την συνεισφορά της διατριβής.

Στο 3ο Κεφάλαιο παρουσιάζεται το πρόβλημα της Ανάλυσης και Διαχείρισης Επικινδυνότητας ως ένα πολυκριτηριακό πρόβλημα συνεργατικής λήψης αποφάσεων. Παρουσιάζονται και αξιολογούνται οι υπάρχουσες μεθοδολογίες επίλυσης τέτοιου είδους προβλημάτων και γίνεται η αναλυτική περιγραφή της μεθοδολογίας AHP η οποία επιλέχθηκε να ενσωματωθεί στην προτεινόμενη μεθοδολογία.

Στο 4^{ο} Κεφάλαιο παρουσιάζεται η προτεινόμενη μεθοδολογία ΑΔΕ, STORM-RM. Περιγράφεται αναλυτικά το πεδίο εφαρμογής και οι στόχοι της προτεινόμενης μεθοδολογίας, καθώς και οι φάσεις και τα βήματα από τα οποία αποτελείται. Στο τέλος του κεφαλαίου παρατίθενται συμπεράσματα και ανοιχτά θέματα.

Στο 5^{ο} Κεφάλαιο γίνεται αναφορά στην ανάγκη χρήσης συνεργατικών τεχνολογιών στην Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων. Παρουσιάζεται το προτεινόμενο συνεργατικό περιβάλλον STORM, η αρχιτεκτονική και οι τεχνολογίες οι οποίες επιλέχθηκαν για την ανάπτυξή του και οι υπηρεσίες οι οποίες παρέχονται από αυτό με στόχο την συνεργατική Διαχείριση Ασφάλειας. Ταυτόχρονα παρουσιάζεται η ενσωμάτωση της προτεινόμενης μεθοδολογίας STORM-RM ως παρεχόμενη υπηρεσία στο συνεργατικό περιβάλλον Διαχείρισης Ασφάλειας STORM.

Στην συνέχεια στο 6^{ο} Κεφάλαιο παρουσιάζεται η χρήση του προτεινόμενου εργαλείου και της μεθοδολογίας (ως υπηρεσία) στην διαχείριση ασφάλειας ΠΣ εμπορικών λιμένων και των μικρών, μεσαίων και μικρομεσαίων επιχειρήσεων (ΜΜΕ). Πιο αναλυτικά, αποτυπώνεται η υπάρχουσα κατάσταση, αναλύονται οι ανάγκες και οι ιδιαιτερότητες των ΠΣ εμπορικών λιμένων και παρουσιάζεται η παραμετροποίηση του προτεινόμενου περιβάλλοντος προκειμένου να καλύψει τις απαιτήσεις των κρίσιμων υποδομών εμπορικών λιμένων. Στην συνέχεια, περιγράφεται η υφιστάμενη κατάσταση διαχείρισης ασφάλειας ΠΣ ΜΜΕ, καταγράφονται οι ελλείψεις και λαμβάνοντας τις ιδιαίτερες απαιτήσεις που έχουν τέτοιου είδους επιχειρήσεις, παρουσιάζεται η προτεινόμενη λύση.

Τέλος στο 7^{ο} Κεφάλαιο παρατίθενται συνολικά συμπεράσματα όπως προκύπτουν από την ανάλυση των προηγούμενων κεφαλαίων, καθώς και μελλοντικές κατευθύνσεις για έρευνα και επεκτάσεις πάνω στο αντικείμενο της διατριβής.

1.3 Βασικοί ορισμοί - Συντομογραφίες

Στην ενότητα αυτή περιλαμβάνονται κάποιοι βασικοί ορισμοί καθώς και συντομεύσεις ορολογιών οι οποίες θα χρησιμοποιηθούν στα επόμενα κεφάλαια της διατριβής.

ΟΡΟΣ	ΟΡΙΣΜΟΣ[2]
Πληροφοριακό Σύστημα (Information System, IS)	Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός και διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.
Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή κάποια άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης.
Απειλή (Threat)	Μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος.
Αδυναμία (Vulnerability)	Σημείο ενός ΠΣ που μπορεί να επιτρέψει να συμβεί μία παραβίαση.
Επικινδυνότητα (Risk)	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.
Ανάλυση και Διαχείριση Επικινδυνότητας	Η διαδικασία αποτίμησης της σημαντικότητας των αγαθών ενός ΠΣ, των πιθανών απειλών και των αδυναμιών έναντι σε αυτές τις απειλές με στόχο την εύρεση του επίπεδου επικινδυνότητας.
Ασφάλεια Πληροφοριακού Συστήματος (IS Security)	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τόσο τα στοιχεία του ΠΣ όσο και ολόκληρο το ΠΣ από τυχαία ή σκόπιμη απειλή.
Εγκυρότητα (Validity)	Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.
Αυθεντικότητα (Authenticity)	Αποφυγή ατελειών και ανακριβειών κατά την εξουσιοδοτημένη τροποποίηση μιας πληροφορίας.
Εμπιστευτικότητα (Confidentiality)	Αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
Ακεραιότητα (Integrity)	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
Διαθεσιμότητα (Availability)	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.
Ζημία (Damage)	Η απώλεια, μερική ή ολική, της αξίας ενός αγαθού.
Παραβίαση (Breach)	Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες:

[2] Σωκρ. Κάτσικας - Δ. Γκρίτζαλης - Στεφ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», ISBN: 960-8105-57-9, Εκδόσεις Νέων Τεχνολογιών, Έκδοση: 1η 2004.

	αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
Περιστατικό (Incident)	Ένα γεγονός, το οποίο έχει ως συνέπεια μία παραβίαση ή αποτελεί μία απόπειρα παραβίασης ή θέτει σε κίνδυνο την ασφάλεια ενός ΠΣ
Μέτρο ασφάλειας / προστασίας (Security Countermeasure)	Ένα μέτρο σχεδιασμένο με σκοπό να εμποδίσει μία παραβίαση, να μειώσει μία αδυναμία-σημείο ευπάθειας ή να μειώσει τις δυνητικές επιπτώσεις.
Πολιτική Ασφάλειας (Security Policy)	Περιγραφή, σε γενικό επίπεδο, του συνόλου των κανόνων, των μέτρων και των διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφάλειας, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των αγαθών.
Αυθεντικοποίηση (Authentication)	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της γνησιότητας της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.
Ανάδοχος, Συμβατικός συνεργάτης (Partner, Contracted Party)	Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρξαν, υπάρχουν, είτε πρόκειται να υπάρξουν εργασιακές συμβατικές σχέσεις.
Κρυπτογράφηση	Τα εμπιστευτικά δεδομένα θα πρέπει να προστατεύονται από κρυπτογραφικούς μηχανισμούς που θα υπόκεινται σε συγκεκριμένη πολιτική του οργανισμού που αφορά την χρήση της κρυπτογραφίας. Η πολιτική αυτή λαμβάνει υπόψη τα καθιερωμένα πρότυπα στον τομέα αυτό.

Συντομογραφίες

ΔΑ	Διαχείριση Ασφάλειας
ΠΣ	Πληροφοριακό Σύστημα
ΑΔΕ	Ανάλυση και Διαχείριση Επικινδυνότητας
ΔΚ	Διαχείριση Κινδύνου
ΠΣΕΛ	Πληροφοριακά Συστήματα Εμπορικών Λιμένων
ΜΜΕ	Μικρές, πολύ μικρές και μικρομεσαίες επιχειρήσεις

Κεφάλαιο 2ο

2 Πρότυπα και μεθοδολογίες Ανάλυσης και Διαχείρισης Ασφάλειας ΠΣ

2.1 Εισαγωγή

Η διαχείριση της ασφάλειας είναι μια συνεχής και συστηματική διαδικασία προσδιορισμού, ανάλυσης, χειρισμού και παρακολούθησης των επιχειρησιακών κινδύνων ενός οργανισμού [3][10][19]. Στόχο έχει την προστασία του ΠΣ από εσωτερικούς και εξωτερικούς κινδύνους που θα μπορούσαν να επηρεάσουν αρνητικά την επίτευξη των επιχειρησιακών στόχων του οργανισμού και την ομαλή λειτουργία του. Στο παρόν κεφάλαιο γίνεται ανασκόπηση των υπαρχόντων προτύπων διαχείρισης ασφάλειας καθώς και των υφιστάμενων μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας. Συγκεκριμένα περιγράφονται οι βασικοί στόχοι και οι οδηγίες των προτύπων διαχείρισης ασφάλειας, και στην συνέχεια αποτυπώνονται τα βασικά βήματα και τα χαρακτηριστικά των μεθοδολογιών. Το κεφάλαιο καταλήγει με μια συνολική αξιολόγηση των μεθοδολογιών, αναδεικνύοντας τις αδυναμίες τους ως προς την εφαρμοστικότητά τους στα σημερινά ΠΣ, την έλλειψη συνεργατικότητας και την απουσία εύχρηστων αυτοματοποιημένων εργαλείων με αποτέλεσμα να γίνεται αντιληπτή η ανάγκη ύπαρξης αναβαθμισμένων μεθοδολογιών.

2.2 Πρότυπα Διαχείρισης Ασφάλειας

2.2.1 Το πρότυπο ISO / IEC 27001:2005

Το ISO / IEC 27001:2005 [14] είναι ένα εμπορικό πρότυπο το οποίο καθορίζει τις βασικές αρχές για τη δημιουργία, υλοποίηση, παρακολούθηση, αξιολόγηση, διατήρηση και βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας (ΣΔΑ). Το ΣΔΑ είναι ένα συνολικό πλαίσιο διαχείρισης και ελέγχου της ασφάλειας Πληροφοριακών Συστημάτων ενός οργανισμού.

Συνήθως, μια ομάδα αναλυτών με υψηλή ειδίκευση και εμπειρία στις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ) επαληθεύει τη συμμόρφωση του οργανισμού με τις καθορισμένες απαιτήσεις. Ωστόσο, παρότι η διαδικασία συμμόρφωσης απαιτεί την εμπλοκή πολλών

χρηστών οι συνεργατικές ικανότητες του προτύπου είναι περιορισμένες λόγω της εγγενούς πολυπλοκότητάς του.

Το πρότυπο καλύπτει ως επί το πλείστον μεγάλης κλίμακας επιχειρήσεις (π.χ. κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις), ενώ θεωρείται «πολύ βαρύ» (πολύπλοκο) για τις πολύ μικρές, μικρές και μεσαίου μεγέθους επιχειρήσεις. Παρόλα αυτά είναι χρήσιμο και αναγκαίο για οποιασδήποτε φύσης οργανισμό.

Θα πρέπει να σημειωθεί ότι το πρότυπο δίνει μεγάλη έμφαση στον πληροφοριακό κίνδυνο (risk based) και όλες οι απαιτήσεις και οδηγίες του επικεντρώνονται στον προσδιορισμό, την εκτίμηση και τον μετριασμό των κινδύνων που αντιμετωπίζει ο υπό εξέταση οργανισμός. Μία από τις υποχρεωτικές τεκμηριωμένες διαδικασίες τις οποίες απαιτεί το πρότυπο είναι η χρήση μιας μεθοδολογίας για την ανάλυση και διαχείριση επικινδυνότητας, χωρίς όμως να παρέχει μια συγκεκριμένη μέθοδο.

2.2.2 Το πρότυπο ISO / IEC 27005:2008

Το πρότυπο ISO / IEC 27005:2008 [13] αποτελεί ένα εμπορικό πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που ορίζει τις βασικές αρχές, τις πτυχές και τις δραστηριότητες μιας καλά ορισμένης διαδικασίας διαχείρισης επικινδυνότητας. Έτσι, μπορεί να θεωρηθεί ως ένα ελάχιστο πλαίσιο το οποίο περιγράφει τις απαιτήσεις για τη διαδικασία αξιολόγησης του κινδύνου και όχι ως μία ολοκληρωμένη μέθοδο διαχείρισης επικινδυνότητας. Το πρότυπο αυτό υποστηρίζει τις γενικές έννοιες που ορίζει το πρότυπο ISO / IEC 27001:2005, καθώς και τις κύριες διαδικασίες και τους κανόνες που περιγράφονται στο πρότυπο ISO / IEC 27002:2005. Έχει εφαρμογή σε όλους τους τύπους των οργανισμών (π.χ. κυβερνητικούς οργανισμούς, μεγάλες εταιρείες, μικρές και μεσαίες επιχειρήσεις) οι οποίες προτίθενται να διαχειρίζονται τους κινδύνους οι οποίοι θα μπορούσαν να διακυβεύσουν την ομαλή λειτουργία του ΠΣ του οργανισμού τους.

Το πρότυπο ISO 27005 προτείνει τη χρήση τόσο ποσοτικής όσο και ποιοτικής μεθοδολογίας για τον υπολογισμό του επιπέδου του κινδύνου, ωστόσο δεν υποστηρίζει καμία συγκεκριμένη τεχνική για το σκοπό αυτό ή οποιαδήποτε υπολογιστική μέθοδο για τη συλλογή και την ανάλυση της απαιτούμενης πληροφορίας για την ανάλυση και διαχείριση επικινδυνότητας. Επίσης, η γενική φύση του προτύπου δεν περιλαμβάνει στοιχεία που προωθούν τη συνεργασία μεταξύ των χρηστών.

Στο πλαίσιο αυτό, πιο ολοκληρωμένες μεθοδολογίες διαχείρισης κινδύνων, όπως η EBIOS [11], η MAGERIT [6][7][8], η MEHARI [4] συμμορφώνονται με τους κανόνες και τις οδηγίες που ορίζονται από το συγκεκριμένο πρότυπο.

2.2.3 Το πρότυπο ISO / IEC 27002:2005

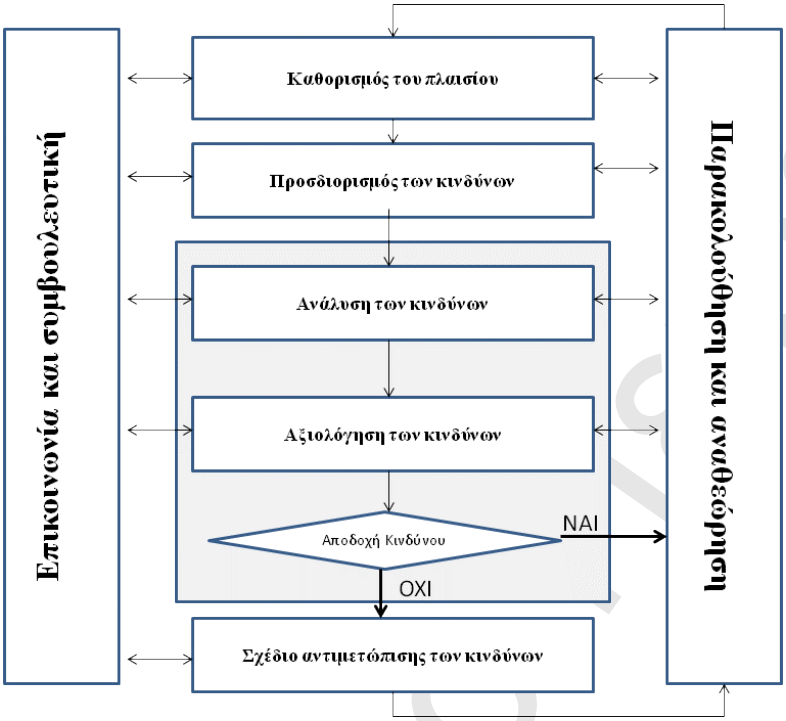
Το ISO / IEC 27002:2005 [15] περιλαμβάνει τις βασικές αρχές του ISO / IEC 17799:2005 [16]. Πρόκειται για ένα εμπορικό πρότυπο που παρέχει προδιαγραφές με αναλυτικές οδηγίες για την υλοποίηση, εφαρμογή και βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (ΣΔΑΠΣ) σε έναν οργανισμό. Ως εκ τούτου, το πρότυπο ISO / IEC 27002 θεωρείται ως ο οδηγός που επιτρέπει σε εσωτερικούς και εξωτερικούς αναλυτές, συνήθως με υψηλή τεχνογνωσία και εμπειρία στις ΤΠΕ, να αξιολογήσει το επίπεδο ασφάλειας ενός οργανισμού και να καθοριστούν τα θέματα που θα βελτιώσουν τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων του.

Ωστόσο, το πρότυπο ISO / IEC 27002 δεν περιλαμβάνει μια μέθοδο για την ανάλυση και διαχείριση επικινδυνότητας, αλλά περιλαμβάνει μια λίστα από 10 βασικούς τομείς ελέγχου (Οργάνωση της Ασφάλειας των Πληροφοριακών Συστημάτων, Διαχείριση Πόρων, Ασφάλεια Προσωπικού, Φυσική και Περιβαλλοντική Ασφάλεια, Διαχείριση Επικοινωνιών και Λειτουργιών, Έλεγχος Πρόσβασης, Προμήθεια/Ανάπτυξη και Συντήρηση ΠΣ, Διαχείριση Περιστατικών Ασφαλείας, Διαχείριση Επιχειρησιακής Συνέχειας, Συμμόρφωση) που αποτελείται από 36 σημεία ελέγχου (control objectives) και 127 ελέγχους (controls) που καθορίζουν τις προϋποθέσεις ότι ένας οργανισμός θα πρέπει να είναι συμβατός με το πρότυπο. Αν και το συγκεκριμένο πρότυπο, δεν αποτελεί μια μέθοδο για την αξιολόγηση και τη διαχείριση κινδύνων, περιλαμβάνει συγκεκριμένες πτυχές χειρισμού του κινδύνου, όπως τον προσδιορισμό των κινδύνων και τη δημιουργία ενός αρχικού σχεδίου αντιμετώπισης του κινδύνου.

Το πρότυπο είναι σε θέση να καλύψει όλα τα είδη των οργανισμών (π.χ. κυβερνητικές οργανισμούς, μικρής, μεσαίας και μεγάλης κλίμακας επιχειρήσεις). Υπάρχουν διάφορα εργαλεία που υλοποιούν το πρότυπο ISO / IEC 27002:2005. Τα πιο αντιπροσωπευτικά παραδείγματα είναι το δωρεάν εργαλείο EBIOS [11] και το εμπορικό λογισμικό RiskWatch [22].

2.2.4 Το πρότυπο AS / NZS 4360

Το AS / NZS 4360 [2] αποτελεί ένα συλλογικό πρότυπο της Αυστραλίας και της Νέας Ζηλανδίας με πρώτη δημοσίευση το 1999. Στόχος του συγκεκριμένου προτύπου είναι ένα γενικό πλαίσιο για τον εντοπισμό, την ανάλυση, την αξιολόγηση και την διαχείριση του κινδύνου των πληροφοριακών συστημάτων.



Εικόνα 1: Βασικά βήματα του AS/NZS 4360

Τα βασικά βήματα του προτύπου (Εικόνα 1) είναι:

Καθορισμός του πλαισίου :

- Καθορισμός του (εσωτερικού και εξωτερικού) πλαισίου του οργανισμού
- Καθορισμός των κριτηρίων βάσει των οποίων θα αξιολογηθεί η επικινδυνότητα
- Καθορισμός της δομής της υπόλοιπης διαδικασίας

Προσδιορισμός των κινδύνων

- Προσδιορισμός των πηγών κινδύνου και των γεγονότων που θα μπορούσαν να έχουν αντίκτυπο στην ομαλή λειτουργία του οργανισμού
- Προσδιορισμός του πώς μπορούν να συμβούν οι κίνδυνοι

Ανάλυση των κινδύνων

- Αξιολόγηση των υφιστάμενων μέτρων ασφαλείας

- Υπολογισμός του μεγέθους των συνεπειών και την πιθανότητα εκδήλωσης των κινδύνων

Αξιολόγηση των κινδύνων

- Λήψη αποφάσεων σχετικά με την αντιμετώπιση των κινδύνων, με βάση τα αποτελέσματα της ανάλυσης κινδύνου

Σχέδιο αντιμετώπισης των κινδύνων

- Προσδιορισμός των εναλλακτικών επιλογών για την αντιμετώπιση των κινδύνων
- Επιλογή του πιο κατάλληλου τρόπου αντιμετώπισης των κινδύνων, εξισορροπώντας το κόστος της εφαρμογής έναντι του οφέλους αντιμετώπισης
- Καθορισμός και εφαρμογή σχεδίου αντιμετώπισης των κινδύνων

Εκτός από τα βασικά βήματα, το πρότυπο προτείνει και δύο άλλες διαδικασίες οι οποίες θα πρέπει να διεξάγονται καθόλη τη διάρκεια των βημάτων ανάλυσης και διαχείρισης επικινδυνότητας:

Επικοινωνία και Συμβουλευτική: ενεργή επικοινωνία με όλα τα αρμόδια μέλη του οργανισμού που συμμετέχουν στην διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας με στόχο να λαμβάνονται οι σωστές αποφάσεις κατά τη διάρκεια των απαιτούμενων διαδικασιών.

Παρακολούθηση και Αναθεώρηση: ώστε να διασφαλιστεί η επικαιροποίηση της πληροφορίας η οποία συλλέγεται κατά τη διάρκεια εκτέλεσης όλων των βημάτων και, ταυτόχρονα, να επιτευχθεί η όσο το δυνατόν σωστότερη αντιμετώπιση των κινδύνων.

Το συγκεκριμένο πρότυπο μπορεί να εφαρμοστεί σε διαφορετικού είδους οργανισμούς, όπως κυβερνητικούς οργανισμούς, και μικρής, μεσαίας ή μεγάλης κλίμακας επιχειρήσεις.

2.2.5 Το πρότυπο NIST SP 800-30

Το πρότυπο Διαχείρισης Επικινδυνότητας ΠΣ NIST 800-30 [17] είναι ένας δωρεάν οδηγός που καθορίζει όλες τις πτυχές ενός αποτελεσματικού προγράμματος διαχείρισης κινδύνων. Ενσωματώνει τις κατευθυντήριες γραμμές και τη διαδικασία που απαιτείται για την αξιολόγηση και τον μετριασμό των κινδύνων των ΠΣ. Το NIST 800-30 στοχεύει στο να βοηθήσει ως επί το πλείστον μεγάλης

κλίμακας οργανισμούς (όπως κυβερνητικούς οργανισμούς και μεγάλες εταιρείες) για την καλύτερη διαχείριση της ασφάλειας των ΠΣ.

Η προτεινόμενη προσέγγιση της διαχείρισης κινδύνου περιλαμβάνει τρεις κύριες διαδικασίες:

i. Η Ανάλυση Επικινδυνότητας, περιλαμβάνει τον προσδιορισμό και την αξιολόγηση των απειλών, αδυναμιών και κινδύνων, καθώς και τη σύσταση των κατάλληλων μέτρων προστασίας. Η διαδικασία Ανάλυσης Επικινδυνότητας περιλαμβάνει εννέα (9) βασικά βήματα: Βήμα 1 - Χαρακτηρισμός του Συστήματος, Βήμα 2 - Προσδιορισμός απειλών, Βήμα 3 - Προσδιορισμός αδυναμιών, Βήμα 4 – Καταγραφή υπαρχόντων μέτρων ασφάλειας, Βήμα 5 - Προσδιορισμός πιθανότητας, Βήμα 6 - Ανάλυση των επιπτώσεων ασφάλειας, Βήμα 7 - Προσδιορισμός των κινδύνων, Βήμα 8 – Προτεινόμενα μέτρα ασφάλειας, Βήμα 9 - Αποτελέσματα Τεκμηρίωσης. Σύμφωνα με το NIST 800-30, ο κίνδυνος είναι συνάρτηση της πιθανότητας μιας συγκεκριμένης απειλής, η οποία εκμεταλλεύεται συγκεκριμένες αδυναμίες και των επιπτώσεων της εν λόγω ανεπιθύμητης απειλής στην ομαλή λειτουργία του ΠΣ. Ο τελικός προσδιορισμός του κινδύνου (Χαμηλός - Μεσαίος - Υψηλός) υπολογίζεται από τον πολλαπλασιασμό της πιθανότητας της απειλής (Υψηλή, Μεσαία και Χαμηλή) και των επιπτώσεων της απειλής (Υψηλή, Μεσαία και Χαμηλή)

ii. Η Διαχείριση Κινδύνου, περιλαμβάνει την αξιολόγηση των υλοποιημένων μέτρων προστασίας που καταγράφηκαν στην προηγούμενη διαδικασία (Ανάλυση Επικινδυνότητας).

iii. Η Αξιολόγηση και Εκτίμηση παρέχει τις κατευθυντήριες γραμμές μιας συνεχούς ανάλυσης επικινδυνότητας.

Θα πρέπει να σημειωθεί ότι η χρήση της πρωτόγονης μεθόδου για τον υπολογισμό του επιπέδου κινδύνου σε συνδυασμό με την έλλειψη μιας αποτελεσματικής υπολογιστικής τεχνικής για τη συλλογή και την ανάλυση της απαιτούμενης γνώσης και πληροφορίας μειώνουν τις δυνατότητες του NIST 800-30 για μια πιο ολοκληρωμένη προσέγγιση. Επιπλέον, παρά το γεγονός ότι η μέθοδος έχει υιοθετήσει και χρησιμοποιεί εκτεταμένες τεχνικές και ερωτηματολόγια που απαιτούν τη συμμετοχή ενός μεγάλου αριθμού χρηστών, η έννοια της συνεργασίας στον προσδιορισμό των συνολικών αποτελεσμάτων και τη διαμόρφωση του τελικού σχεδίου διαχείρισης επικινδυνότητας είναι περιορισμένη. Η ανάλυση κινδύνου και η διαδικασία διαχείρισης που καθορίζεται στο NIST 800-30 συνήθως εκτελείται από συγκεκριμένη ομάδα ειδικών σε θέματα ασφάλειας ΠΣ.

Η μέθοδος είναι συμβατή με το πρότυπο ISO / IEC 27001:2005 και λαμβάνει υπόψη της όλες τις προϋποθέσεις για την καθιέρωση και εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (ΣΔΑΠΣ). Μέχρι σήμερα το NIST 800-30 δεν υποστηρίζεται από κάποια δωρεάν ή εμπορική εφαρμογή.

2.3 Μεθοδολογίες Ανάλυσης και Διαχείρισης Επικινδυνότητας

Καθώς είναι ευρέως αποδεκτό ότι οι απειλές ασφάλειας δεν μπορούν να εξαλειφθούν, τα πρότυπα διαχείρισης ασφάλειας ακολουθούν μια προσέγγιση βασισμένη στους κινδύνους (Risk based approach). Αυτό απαιτεί την εκτέλεση μιας μεθοδολογίας ανάλυσης και διαχείρισης επικινδυνότητας, προκειμένου να εντοπιστούν και να μετριαστούν οι απειλές, τα τρωτά σημεία και οι πιθανές επιπτώσεις και, τελικά, να αποτιμηθούν οι κίνδυνοι ασφαλείας που αντιμετωπίζει ο υπό εξέταση οργανισμός. Το πρότυπο ISO 27005:2008 [13] καθορίζει τις απαιτήσεις που πρέπει να έχουν οι μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας για τον προσδιορισμό, αξιολόγηση και αντιμετώπιση των κινδύνων ασφάλειας. Στις ενότητες που ακολουθούν, παρουσιάζεται ένα ευρύ φάσμα μεθοδολογιών οι οποίες έχουν αναπτυχθεί και περιγράφουν συγκεκριμένα βήματα για την ανάλυση και διαχείριση κινδύνου. Πολλές από αυτές τις προσεγγίσεις υλοποιούνται σε εμπορικά ή σε ορισμένες περιπτώσεις δωρεάν εργαλεία. Αυτά τα εργαλεία αυτοματοποιούν τη διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας και σε ορισμένες περιπτώσεις είναι σε θέση να υποστηρίξουν τις απαραίτητες διαδικασίες για την ανάπτυξη της πολιτικής ασφάλειας του υπό εξέταση οργανισμού.

2.3.1 CRAMM

Η CRAMM (CCTA Risk Assessment and Management Methodology) [12] είναι μια μεθοδολογία η οποία αναπτύχθηκε για να βοηθήσει κυρίως μεγάλης κλίμακας οργανισμούς (όπως δημόσιους φορείς και μεγάλες επιχειρήσεις) και μπορεί να εφαρμοστεί σε διαφορετικού τύπου ΠΣ. Είναι συμβατή με το πρότυπο ασφάλειας ISO 17799 [16] και μπορεί να καλύψει όλες τις φάσεις του κύκλου ζωής της ασφάλειας πληροφοριών (π.χ. σχεδιασμός, ανάπτυξη - υλοποίηση και αναβάθμιση) .

Η μεθοδολογία CRAMM χρησιμοποιεί τρεις (3) φάσεις οι οποίες υλοποιούνται από επιμέρους βήματα:

- ✓ Φάση 1: Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)
  - Βήμα 1: Περιγραφή των πληροφοριακών συστημάτων και των εγκαταστάσεων

- Βήμα 2: Αποτίμηση των αγαθών των πληροφοριακών συστημάτων και των εγκαταστάσεων
- Βήμα 3: Επιβεβαίωση και επικύρωση της αποτίμησης

✓ Φάση 2: Ανάλυση επικινδυνότητας (risk analysis)
- Βήμα 1: Προσδιορισμός των απειλών που αφορούν σε κάθε Αγαθό (Asset)
- Βήμα 2: Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)
- Βήμα 3: Υπολογισμός επικινδυνότητας συνδυασμών «Αγαθό-Απειλή-Αδυναμία»
- Βήμα 4: Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας

✓ Φάση 3: Διαχείριση επικινδυνότητας (risk management)
- Βήμα 1: Προσδιορισμός προτεινόμενων αντιμέτρων
- Βήμα 2: Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Σε αυτή τη μέθοδο, ένας αναλυτής ή μια ομάδα αναλυτών αναλαμβάνει την ευθύνη να αξιολογήσει το επίπεδο ασφάλειας και κινδύνου του υπό εξέταση οργανισμού, αναλύοντας και συνδυάζοντας την πολύπλευρη γνώση η οποία βρίσκεται κατανεμημένη στο εταιρικό περιβάλλον. Η υπολογιστική μέθοδος και η τεχνική την οποία υιοθετεί η CRAMM για το συσχετισμό και τον προσδιορισμό των αποτελεσμάτων είναι αρκετά πρωτόγονη και βασίζεται σε μια ποιοτική προσέγγιση. Ταυτόχρονα, η συμμετοχή των χρηστών του υπό εξέταση οργανισμού στην αξιολόγηση της ασφάλειας μπορεί να θεωρηθεί αρκετά χαμηλή, με αποτέλεσμα οι συνεργατικές δυνατότητες της μεθοδολογίας να είναι περιορισμένες. Για την εκτέλεση όλων των φάσεων της μεθοδολογίας, δηλαδή τη συλλογή της κατάλληλης πληροφορίας, τον εντοπισμό των απειλών και των ευάλωτων σημείων, την εκτίμηση κινδύνου και την επιλογή των κατάλληλων μέτρων προστασίας απαιτεί υψηλό επίπεδο γνώσεων και εμπειρίας σε θέματα ασφάλειας

Η CRAMM είναι αρκετά αναλυτική σαν μεθοδολογία και είναι ικανή να καλύψει ένα ευρύ φάσμα διοικητικών, επιχειρησιακών και τεχνικών απαιτήσεων. Επίσης, η CRAMM υποστηρίζεται από ένα εμπορικό εργαλείο ανεπτυγμένο από την Insight Consulting [12] το οποίο υλοποιεί όλες τις φάσεις και τα επιμέρους βήματα της μεθοδολογίας.

2.3.2 EBIOS

Η EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) [11] είναι μια μεθοδολογία διαχείρισης επικινδυνότητας η οποία δημιουργήθηκε από την Γαλλική Γενική Γραμματεία Εθνικής Άμυνας και έχει ως στόχο να παρέχει μια ολοκληρωμένη και συστημική

μεθοδολογία για την αξιολόγηση και την αντιμετώπιση των κινδύνων των ΠΣ. Η προτεινόμενη προσέγγιση περιλαμβάνει πέντε φάσεις:

- ✓ Φάση 1: Προσδιορισμός του υπό εξέταση ΠΣ και των αλληλεξαρτήσεων των αγαθών του
- ✓ Φάση 2 και 3: Προσδιορισμός και αξιολόγηση των πιθανών απειλών του ΠΣ
- ✓ Φάση 4: Αξιολόγηση επικινδυνότητας
- ✓ Φάση 5: Προσδιορισμός και επιλογή μέτρων προστασίας για το υπό εξέταση ΠΣ

Η μεθοδολογία EBIOS είναι μια σχετικά εύκολη μεθοδολογία η οποία μπορεί να βρει εφαρμογή σε διαφορετικού τύπου οργανισμούς, μεγάλες και μικρές εταιρείες καλύπτοντας όμως μόνο διοικητικές και επιχειρησιακές απαιτήσεις. Η μεθοδολογία διαθέτει συνεργατικές δυνατότητες, δεδομένου ότι συγκεντρώνει και συνδυάζει την επιχειρηματική γνώση με έναν αποτελεσματικό τρόπο ο οποίος βασίζεται σε μια ποιοτική προσέγγιση. Ωστόσο, η έλλειψη μιας προηγμένης υπολογιστικής τεχνικής για το συσχετισμό και τον προσδιορισμό των αποτελεσμάτων μπορεί να θεωρηθεί ένα βασικό μειονέκτημα της μεθόδου.

Η EBIOS καλύπτει όλες τις απαιτήσεις, τα βήματα και τις διαδικασίες ενός μεγάλου εύρους προτύπων ασφάλειας, όπως των προτύπων ISO/IEC 27005:2008 [13], ISO/IEC 27001:2005 [14] και ISO/IEC 27002:2005 [15]. Επίσης, υποστηρίζεται από ένα ανοιχτού κώδικα εργαλείο το οποίο αναπτύχθηκε από την Κεντρική Διεύθυνση Ασφάλειας Πληροφοριακών Συστημάτων της Γαλλίας, το οποίο ενσωματώνει όλες τις φάσεις τις μεθόδου και βοηθά τους χρήστες με χαμηλή εξειδίκευση και πείρα σε θέματα πληροφορικής να είναι σε θέση να προσδιορίσουν και να αξιολογήσουν τους κινδύνους του ΠΣ τους.

2.3.3 OCTAVE

Η OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [20][21] είναι μια μεθοδολογία η οποία βασίζεται στη χρήση ομάδων εργασίας (workshop-based), εμπλέκοντας σε αρκετά στάδια τους χρήστες του υπό εξέταση οργανισμού. Η OCTAVE υιοθετεί μια τριών φάσεων προσέγγιση για την κατανόηση του επιχειρησιακού προφίλ και τη δημιουργία των τεχνολογικών και των επιχειρησιακών επιπέδων ασφάλειας του υπό εξέταση οργανισμού. Οι φάσεις αυτές είναι :

- ✓ Φάση 1: Δημιουργία προφίλ Απειλών με βάση τα Αγαθά
  - Διεργασία 1: Προσδιορισμός της γνώσης στη διοίκηση
  - Διεργασία 2: Προσδιορισμός της γνώσης σε επιτελικό επίπεδο
  - Διεργασία 3: Προσδιορισμός της γνώσης στο προσωπικό
  - Διεργασία 4: Δημιουργία προφίλ απειλών

- ✓ Φάση 2: Εντοπισμός Ευπαθειών
  - Διεργασία 5: Προσδιορισμός κύριων συνιστωσών
  - Διεργασία 6: Αξιολόγηση επιλεγμένων συνιστωσών
- ✓ Φάση 3: Ανάπτυξη στρατηγικής και σχεδίων ασφάλειας
  - Διεργασία 7: Εκτίμηση επικινδυνότητας
  - Διεργασία 8: Ανάπτυξη στρατηγικής προστασίας

Για την επίτευξη των στόχων της, η μέθοδος βασίζεται σε workshops και εκτενή ερωτηματολόγια. Μέσω αυτών των διαύλων επικοινωνίας, η OCTAVE ενθαρρύνει την ανοικτή συζήτηση και τη συνεργασία μεταξύ των συμμετεχόντων και διευκολύνει την ανταλλαγή και την συσσώρευση της γνώσης και της πληροφορίας σχετικά με την ασφάλεια πληροφοριών. Στη μέθοδο αυτή, οι εταιρικοί χρήστες μπορούν να συμμετέχουν ενεργά σε διάφορα μέρη της διαδικασίας αξιολόγησης.

Για τη διαδικασία ανάλυσης κινδύνου, η OCTAVE χρησιμοποιεί μια πρωτόγονη προσέγγιση που βασίζεται σε μια ποιοτική κλίμακα (υψηλή, μέση, χαμηλή). Ωστόσο, η μέθοδος δεν ενσωματώνει μια προηγμένη τεχνική για την ανάλυση και τον συνδυασμό της γνώσης η οποία βρίσκεται στο εταιρικό περιβάλλον.

Τέλος, η OCTAVE υποστηρίζεται από ένα εμπορικό εργαλείο το οποίο το έχει αναπτύξει το Advanced Technology Institute (ATI) [1]. Το εργαλείο αυτό είναι σε θέση να βοηθήσει τον χρήστη στην συλλογή της απαιτούμενης πληροφορίας, οργανώνει την πληροφορία αυτή και παράγει όλες τις απαραίτητες εκθέσεις ασφάλειας της μεθοδολογίας.

2.3.4 MEHARI

Η MEHARI [5] είναι μια ποιοτική μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας. Περιλαμβάνει δραστηριότητες όπως τον προσδιορισμό του πλαισίου εφαρμογής, την ανάλυση και κατηγοριοποίηση των αγαθών, τον εντοπισμό του κινδύνου, την ανάλυση κινδύνου, την αξιολόγηση του κινδύνου, τη διαχείριση κινδύνου και τα αποδεκτά επίπεδα κινδύνου.

Η MEHARI παρέχει μια ολοκληρωμένη μεθοδολογία με τις κατάλληλες βάσεις γνώσεων (π.χ. εγχειρίδια και οδηγούς που περιγράφουν τις διαφορετικές ενότητες), και έχει σχεδιαστεί για να βοηθήσει τους εμπλεκόμενους στη διαχείριση της ασφάλειας (τους διαχειριστές, την ομάδα ασφάλειας και τους ελεγκτές) να επιτελέσουν το έργο και τις δράσεις τους. Συγκεκριμένα απευθύνεται σε χρήστες με διοικητικές, επιχειρησιακές αλλά και τεχνικές αρμοδιότητες. Ταυτόχρονα, η συγκεκριμένη μεθοδολογία μπορεί να χρησιμοποιηθεί και για την υλοποίηση ενός Συστήματος Διαχείρισης Ασφάλειας καλύπτοντας πλήρως τις απαιτήσεις του ISO/IEC 27001:2005 [14].

Η MEHARI είναι κατάλληλη για μεσαίας και μεγάλης κλίμακας οργανισμούς, όπως κυβερνητικές υπηρεσίες, μεσαίες ή μεγάλες επιχειρήσεις. Οι εταιρικοί χρήστες μπορούν να συμμετέχουν μόνο σε συγκεκριμένες φάσεις της μεθοδολογίας οι οποίες σχετίζονται με τον προσδιορισμό των αγαθών και των αδυναμιών τους. Σε αυτό το πλαίσιο, οι συνεργατικές δυνατότητες της μεθόδου μπορεί να θεωρηθούν περιορισμένες, δεδομένου ότι οι χρήστες δεν εμπλέκονται άμεσα στον υπολογισμό του κινδύνου και τη διαμόρφωση του σχεδίου αντιμετώπισης κινδύνου. Επιπλέον, η μέθοδος χρησιμοποιεί μια πρωτόγονη υπολογιστική μέθοδο για την ανάλυση και τον συνδυασμό της πληροφορίας, προκειμένου να συναγάγει τα τελικά αποτελέσματα.

Υποστηρίζεται από δύο αυτόνομα (standalone) εργαλεία. Το ένα από αυτά είναι το εμπορικό το οποίο αναπτύχτηκε από την Risicare [18] και το δεύτερο είναι μια δωρεάν εφαρμογή (MEHARI 2010 - basic tool) ανεπτυγμένο από την CLUSIF (Club de la Sécurité de l'Information Français) [5].

2.3.5 MAGERIT

Η MAGERIT [6][7][8] είναι μια ανοικτή μεθοδολογία για την ανάλυση και διαχείριση κινδύνου, η οποία αναπτύχθηκε από το Ισπανικό Ανώτατο Συμβούλιο για την Ηλεκτρονική Διακυβέρνηση. Είναι η απάντηση στην αυξανόμενη εξάρτηση των δημόσιων και των ιδιωτικών οργανισμών στις τεχνολογίες της πληροφορίας με στόχο την εκπλήρωση της αποστολής τους και την επίτευξη των επιχειρηματικών στόχων τους. Η προσέγγιση αυτή καλύπτει όλες τις αρχές της ολοκληρωμένης ανάλυσης και διαχείρισης κινδύνων και περιέχει βήματα όπως τον προσδιορισμό των περιουσιακών στοιχείων, τον εντοπισμό των απειλών, τον προσδιορισμό των επιπτώσεων, καθώς και τον προσδιορισμό και τον μετριασμό των κινδύνων.

Στην MAGERIT, η αξιολόγηση του κινδύνου μπορεί να είναι ποσοτική (χρησιμοποιώντας μια πρωτόγονη συνάρτηση) ή ποιοτική (με χρήση της κλίμακας: πολύ χαμηλό, χαμηλό, μεσαίο, υψηλό, πολύ υψηλό επίπεδο κινδύνου). Για τον υπολογισμό του κινδύνου οι δύο παράμετροι που λαμβάνονται υπόψη είναι ο αντίκτυπος που έχει μία απειλή πάνω σε ένα αγαθό και η συχνότητα εμφάνισης των απειλών. Πρέπει επίσης να σημειωθεί ότι η υπολογιστική τεχνική που εφαρμόζεται από την MAGERIT δεν είναι επαρκής δεδομένου ότι η ανάλυση και η συσχέτιση των στοιχείων αξιολόγησης βασίζονται σε πρωτόγονες λειτουργίες.

Οργανισμοί οι οποίοι διαθέτουν μία σύνθετη πληροφοριακή υποδομή (κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις), ή μία βασική υποδομή (μικρού και μεσαίου μεγέθους επιχειρήσεις) είναι σε θέση να εφαρμόσουν αυτή τη μέθοδο για τον εντοπισμό και τον μετριασμό των κινδύνων ασφάλειας των ΠΣ τους. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί μόνο από χρήστες με υψηλή τεχνογνωσία και εμπειρία στα ΠΣ. Αυτοί οι χρήστες αναλαμβάνουν την ευθύνη για την

εκτέλεση της διαδικασίας ανάλυσης κινδύνου μέσω συνεντεύξεων με ειδικούς εκπροσώπους του οργανισμού που συμμετέχουν μόνο σε συγκεκριμένες φάσεις της διαδικασίας αξιολόγησης. Στο πλαίσιο αυτό, η μέθοδος δεν υποστηρίζει την συνεργατικότητα.

Η Magerit είναι συμβατή με ένα σύνολο προτύπων ασφάλειας. Συγκεκριμένα, πληροί όλες τις οδηγίες και τα βήματα του ISO/IEC 27005:2008, καλύπτει όλες τις απαιτήσεις του ISO/IEC 27001:2005 και συμμορφώνεται με τον κώδικα εφαρμογής ενός Συστήματος Διαχείρισης Ασφάλειας που ορίζει το ISO/IEC 27002:2005.

Το EAR / PILAR είναι ένα εμπορικό εργαλείο το οποίο έχει υλοποιηθεί από την A.L.H. J. Mañas [9] και υλοποιεί και επεκτείνει την μεθοδολογία.

2.4 Ανοιχτά προβλήματα - Συνεισφορά διατριβής

Έπειτα από την περιγραφή των μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας που πραγματοποιήθηκε στις προηγούμενες ενότητες, στην παρούσα ενότητα γίνεται η αξιολόγησή τους, παρουσιάζονται τα ανοιχτά προβλήματα και αποτυπώνεται η συνεισφορά της διατριβής. Στον πίνακα που ακολουθεί (Πίνακας 1), συνοψίζονται οι υπάρχουσες μεθοδολογίες και κάποια από τα βασικά κριτήρια βάσει των οποίων γίνεται η αξιολόγησή τους, όπως το κόστος, η ύπαρξη ή όχι εργαλείου, η υποστήριξη ή όχι της συνεργατικότητας, η συμβατότητά τους με τα πρότυπα ασφάλειας, η εφαρμοσιμότητά τους σε πολύπλοκους οργανισμούς ή σε μικρές και μικρομεσαίες επιχειρήσεις (ΜΜΕ) και η γλώσσα στην οποία είναι διαθέσιμες.

Πίνακας 1: Υπάρχουσες μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας

Μεθοδολογίες / **Κριτήρια**	**CRAMM**	**EBIOS**	**OCTAVE**	**MEHARI**	**MAGERIT**
Κόστος	Εμπορικό	Δωρεάν	Δωρεάν	Δωρεάν	Δωρεάν
Εργαλείο/ Κόστος	Ναι/ Εμπορικό	Ναι/ Δωρεάν	Ναι/ Εμπορικό	Ναι/ Εμπορικό / Δωρεάν	Ναι/ Εμπορικό
Συνεργατικότητα	Όχι	Όχι	Ναι	Όχι	Όχι
Συμβατότητα με πρότυπα	Ναι	Ναι	Όχι	Ναι	Ναι
Υποστήριξη ΜΜΕ	Όχι	Όχι	Ναι	Ναι	Ναι
Πολύγλωσσο	Μόνο Αγγλικά	Ναι	Μόνο Αγγλικά	Μόνο Γαλλικά	Αγγλικά, Ισπανικά

Οι υπάρχουσες μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας αδυνατούν να συλλάβουν την πολυπλοκότητα των σημερινών υποδομών, τις επιπτώσεις από ένα κακόβουλο γεγονός, τις εξαρτήσεις τους από άλλα συστήματα ή υποδομές και τις πολλαπλές επιπτώσεις σε έναν ή περισσότερους τομείς. Συνεπώς, απαιτούνται αρκετές τροποποιήσεις προκειμένου να μπορέσουν να ανταπεξέλθουν στις ανάγκες των σημερινών πολύπλοκων ΠΣ.

Πιο συγκεκριμένα, θα πρέπει να δοθεί έμφαση στο γεγονός ότι παρόλο που αρκετές μεθοδολογίες συνοδεύονται από κάποια αυτοματοποιημένα εργαλεία (π.χ. CRAMM, OCTAVE, MEHARI, MAGERIT), αυτά είναι δύσκολα στην χρήση και απαιτούν υψηλού επιπέδου

τεχνογνωσία. Επιπλέον, η πλειοψηφία αυτών των εργαλείων είναι μονολιθικά και αδυνατούν να αντιμετωπίσουν τις προηγμένες απαιτήσεις των σύγχρονων πληροφοριακών συστημάτων. Η χρήση προηγμένων και διαδραστικών web-based διεπαφών χρήστη καθώς και η συνεργατικότητα αποτελούν δύο σημαντικές προϋποθέσεις τις οποίες τα υπάρχοντα εργαλεία δεν ικανοποιούν. Έτσι, οι λύσεις αυτές δεν διευκολύνουν τη ανταλλαγή πληροφοριών, εμπειρίας και τεχνογνωσίας στο πλαίσιο μιας επιχείρησης και δεν ενθαρρύνουν τους χρήστες να εργαστούν από κοινού για την υλοποίηση των φάσεων της ανάλυσης και διαχείρισης κινδύνων με ομαλό και αποτελεσματικό τρόπο.

Όσον αφορά στην αποτίμηση των επιπτώσεων, το ISO 27005:2008 [13] και το πρότυπο ISO 27002:2005 [15] επιβάλλουν ότι οι επιπτώσεις ενός συμβάντος ασφάλειας αξιολογούνται με βάση την επιχειρησιακή επίπτωση που θα έχει το συμβάν αυτό. Στη Mehari, οι αναλυτές που συμμετέχουν στη διαδικασία ανάλυσης κινδύνου υπολογίζουν το επίπεδο των επιπτώσεων με βάση ένα "σταθερό" σενάριο επιπτώσεων. Από την άλλη, η CRAMM και η MAGERIT δίνουν τη δυνατότητα στους αναλυτές να ορίσουν διαφορετικά σενάρια τα οποία απεικονίζουν τις αρνητικές επιπτώσεις ενός γεγονότος για τον οργανισμό. Η OCTAVE υπολογίζει την επίπτωση με βάση το βαθμό με τον οποίο ένα γεγονός ασφάλειας θα επηρεάσει ένα κρίσιμο αγαθό του οργανισμού.

Όσον αφορά στον υπολογισμό του κινδύνου, στην CRAMM και στη Méhari, ο κίνδυνος περιλαμβάνει την πιθανότητα και τις επιπτώσεις της απειλής σε μια ομάδα αγαθών και το επίπεδο αδυναμίας αυτής της ομάδας αγαθών. Στη MAGERIT, ο κίνδυνος περιλαμβάνει την πιθανότητα να συμβεί ένα περιστατικό (δηλαδή, μια απειλή να εκμεταλλευτεί ορισμένες αδυναμίες), καθώς και τις θετικές ή αρνητικές συνέπειες αυτού του περιστατικού. Από την άλλη πλευρά, οι EBIOS και OCTAVE έχουν υιοθετήσει μια ποιοτική μέθοδο για την αξιολόγηση του κινδύνου.

Όλες οι μέθοδοι βασίζονται σε πλήθος συνεντεύξεων για να συγκεντρώσουν την απαιτούμενη πληροφορία για την αξιολόγηση ασφάλειας. Ωστόσο, οι περισσότερες από αυτές παρουσιάζουν περιορισμένες δυνατότητες συνεργασίας, δεδομένου ότι δεν προωθούν την ευρεία και αποτελεσματική συνεργασία μεταξύ των εμπλεκόμενων χρηστών, την αποτελεσματική συζήτηση και την ανταλλαγή πληροφοριών, ιδεών και σκέψεων καθώς και την ενεργή συμμετοχή των εκπροσώπων των επιχειρήσεων. Μόνο η OCTAVE και η EBIOS παρέχουν βασικές δυνατότητες συνεργασίας οι οποίες επιτρέπουν στους χρήστες να συμμετέχουν ενεργά σε διάφορα μέρη της διαδικασίας αξιολόγησης.

Επίσης, παρόλο που οι περισσότερες από τις μεθοδολογίες προσπαθούν να καλύψουν τις απαιτήσεις των προτύπων ασφάλειας (ISO/IEC 27005:2008 [13], ISO/IEC 27001:2005 [14],

ISO/IEC 27002:2005 [15]), μόνο η EBIOS και η MAGERIT επιτυγχάνουν πλήρη συμμόρφωση με τους κανόνες και τις διαδικασίες τους.

Οι μεθοδολογίες ανάλυσης και διαχείρισης ασφάλειας και τα εργαλεία από τα οποία υλοποιούνται χρησιμοποιούν μια πληθώρα από ερωτηματολόγια και συνεντεύξεις για να αξιολογήσουν τις απειλές και τις αδυναμίες. Είναι πολύ γενικές και δεν παρέχουν στοχευμένες τεχνικές λύσεις που απευθύνονται ειδικά στα προβλήματα, τις απειλές και τις νομοθεσίες των σημερινών οργανισμών. Οι περισσότερες από αυτές δεν επιτρέπουν τη συνεργατικότητα, δεδομένου ότι δεν προωθούν την ευρεία και αποτελεσματική συνεργασία μεταξύ των εμπλεκόμενων χρηστών, την αποτελεσματική συζήτηση και την ανταλλαγή πληροφοριών, ιδεών και σκέψεων καθώς και την ενεργό συμμετοχή των εκπροσώπων των επιχειρήσεων. Αυτό είναι ένα σημαντικό μειονέκτημα, δεδομένου ότι στα σημερινά ΠΣ υπάρχουν πολλοί χρήστες και οι απαιτούμενες συνεντεύξεις απαιτούν χρόνο, προσπάθεια και πόρους.

Τέλος, ένα άλλο σημαντικό μειονέκτημα των υπαρχουσών μεθόδων ανάλυσης κινδύνου είναι η έλλειψη αποτελεσματικών και προηγμένων υπολογιστικών τεχνικών. Συνήθως βασίζονται σε απλοϊκές μεθόδους για τον προσδιορισμό, την αξιολόγηση και τον περιορισμό των εταιρικών κινδύνων και χρησιμοποιούν αναποτελεσματικές διαδικασίες και τεχνικές για να αναλύσουν και να συνδυάσουν την πολύπλευρη γνώση που βρίσκεται κατανεμημένη στους σημερινούς οργανισμούς. Απαιτείται, λοιπόν, η υιοθέτηση πιο εξελιγμένων μεθόδων οι οποίες ενισχύουν τις δυνατότητες ανάλυσης του κινδύνου ώστε να αυξηθεί η ακρίβεια των συμπερασμάτων τους, καθώς και καινοτόμα αυτοματοποιημένα εργαλεία για την εξοικονόμηση χρόνου και κόστους.

Η παρούσα διδακτορική διατριβή, πρόκειται να ανταπεξέλθει στα παραπάνω ανοιχτά θέματα προτείνοντας μια συνεργατική μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας (βλ. 4ο Κεφάλαιο) η οποία βασίζεται σε αλγόριθμους πολυκριτηριακής λήψης αποφάσεων με στόχο την άμεση εμπλοκή όλων των χρηστών στις διάφορες φάσεις και τις διαδικασίες ανάλυσης και διαχείρισης επικινδυνότητας. Ταυτόχρονα, όλες οι φάσεις και τα βήματα της προτεινόμενης μεθοδολογίας θα υλοποιηθούν και θα παρέχονται ως υπηρεσίες από το αυτοματοποιημένο συνεργατικό περιβάλλον διαχείρισης ασφάλειας STORM (το οποίο θα παρουσιαστεί στο 5ο Κεφάλαιο). Στόχος λοιπόν της παρούσας διδακτορικής διατριβής είναι ο αποτελεσματικός, ολιστικός και αντικειμενικός εντοπισμός, εκτίμηση και μετριασμός των πληροφοριακών κινδύνων που αντιμετωπίζουν τα σημερινά ΠΣ, με τον συνδυασμό μιας σύγχρονης μεθοδολογίας και ενός πρωτοποριακού εργαλείου διαχείρισης ασφάλειας τα οποία θα οδηγήσουν σε εξοικονόμηση πόρων (χρόνου και χρήματος, ανθρωποπροσπάθειας) που στις μέρες μας αποτελούν πλέον επιτακτική ανάγκη.

2.5 Βιβλιογραφία 2ου Κεφαλαίου

[1] Advanced Technology Institute, http://www.aticorp.org/**,** (accessed August 2012)**.**

[2] AS/NZS 4360. Risk management standards australia. Strathfield, 1999.

[3] Basel Committee on Banking Supervision: Sound practices for the management and supervision of operational risk. BSI, Basel, Switzerland, 2001.

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

[5] CLUSIF (Club de la Sécurité de l'Information Français). http://www.clusif.asso.fr/, (accessed December 2011)

[6] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Books I – The Method", Ministerio de Administraciones Publicas, June 2006.

[7] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Book II – Catalogue of Elements", Ministerio de Administraciones Publicas, June 2006.

[8] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Book III – Techniques", Ministerio de Administraciones Publicas, June 2006.

[9] EAR / PILAR , A.L.H. J. Mañas, http://ar-tools.com**,** (accessed August 2012)**.**

[10] ENISA, "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools", 2006.

[11] Expression of Needs and Identification of Security Objectives PREMIER MINISTRE Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil. Available at: www.ssi.gouv.fr**,** (accessed August 2012).

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

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

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

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

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

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

[18] Risicare, http://www.risicare.fr/index.htm, (accessed August 2012).

[19] Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. "Information Systems Security Management: A Review and a Classification of the ISO Standards", A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 220-235, 2010.

[20] OCTAVE. http://www.gnu.org/software/octave/, (accessed August 2012).

[21] OCTAVE Method Implementation Guide Version 2.0, Carnegie Mellon University, June 2001 http://www.cert.org/octave/, (accessed August 2012).

[22] RiskWatch: Information systems & ISO 17799 2005 Product Sheet, available at http://www.riskwatch.com (accessed August 2012).

Κεφάλαιο 3ο

3 Η Ανάλυση και Διαχείριση Επικινδυνότητας ως πολυκριτηριακό πρόβλημα

3.1 Εισαγωγή

Τα σημερινά Πληροφοριακά Συστήματα (ΠΣ) παρέχουν κρίσιμες ηλεκτρονικές υπηρεσίες, πολλές φορές σε αδιάκοπη λειτουργία (24-ώρες το εικοσιτετράωρο για 365 μέρες το χρόνο), απαραίτητες για την ομαλή λειτουργία τόσο των ίδιων των οργανισμών, όσο και άλλων εξαρτώμενων φορέων-οργανισμών. Η αδιάλειπτη παροχή αυτών των υπηρεσιών είναι αναγκαία, καθώς οποιαδήποτε κακόβουλη ή μή ενέργεια η οποία θα προκαλούσε τη διακοπή τους, θα οδηγούσε σε σημαντικές κοινωνικές, οικονομικές και άλλες συνέπειες.

Απαραίτητο είναι λοιπόν να υιοθετηθούν κύριες προληπτικές στρατηγικές για τον περιορισμό των περιστατικών ασφάλειας που μπορούν να προκαλέσουν την παρακώλυση της λειτουργίας των ΠΣ ή την παραβίαση της διαθεσιμότητας, της εμπιστευτικότητας ή της ακεραιότητάς τους.

Τα υπάρχοντα πρότυπα ασφάλειας και οι μεθοδολογίες ανάλυσης επικινδυνότητας (που παρουσιάστηκαν στο προηγούμενο κεφάλαιο), δεν είναι σε θέση να καλύψουν απόλυτα τις ανάγκες των σημερινών ΠΣ λόγω:

- ✓ της αυξανόμενης πολυπλοκότητας των συστημάτων αυτών,
- ✓ του πλήθους και της διαφορετικής φύσης των ηλεκτρονικών υπηρεσιών που προσφέρουν,
- ✓ του πλήθους και της διαφορετικής φύσης των επιθέσεων και της χωροχρονικής διασποράς των συνεπειών που μπορεί να επιφέρουν,
- ✓ του ενδεχόμενου μεγάλου κόστους που θα επιφέρει ένα τυχαίο περιστατικό ασφάλειας ή μία κακόβουλη επίθεση, τόσο στον ίδιο τον οργανισμό όσο και στους συνεργαζόμενους φορείς,
- ✓ της αλληλεπίδρασης - αλληλεξάρτησης των τμημάτων των ίδιων των οργανισμών αλλά και την εξάρτησή τους από άλλους φορείς,
- ✓ του μεγάλου αριθμού χρηστών και διαχειριστών αυτών των συστημάτων και την διασπορά τους σε παραπάνω από ένα κτίρια, και

- ✓ του μεγάλου αριθμού των ανθρώπων που επηρεάζονται από τη συνεχή και καλή λειτουργία των συστημάτων αυτών.

Συνεπώς, δημιουργείται πρόβλημα στη συνεργατική, ολιστική και αποτελεσματική αντιμετώπιση της διαχείρισης κινδύνων. Καθίσταται λοιπόν επιτακτική ανάγκη, η ανάπτυξη συνεργατικής μεθοδολογίας Ανάλυσης και Διαχείρισης Επικινδυνότητας ΠΣ, η οποία θα είναι σε θέση να ανταποκρίνεται στις αυξημένες ανάγκες πολύπλοκων ΠΣ όπως αυτών των κρίσιμων υποδομών.

Η Ανάλυση και Διαχείριση Επικινδυνότητας (Risk Management) σε πολύπλοκα ΠΣ, αντιμετωπίζεται ως πολυκριτηριακό πρόβλημα συνεργατικής λήψης αποφάσεων, όπου συμμετέχουν πολλοί αποφασίζοντες (διαχειριστές, προϊστάμενοι τμημάτων, ομάδα ασφάλειας, τοπικοί χρήστες, συνεργάτες), οι οποίοι καλούνται να λύσουν τα εξής προβλήματα:

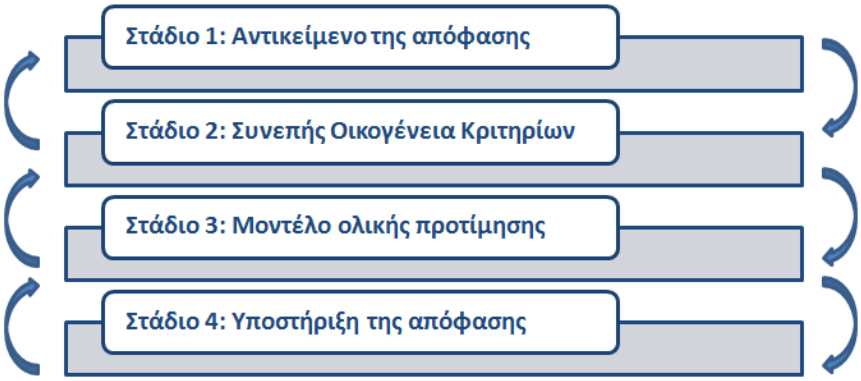
- ✓ προσδιορισμός της κρισιμότητας των ηλεκτρονικών υπηρεσιών,
- ✓ προσδιορισμός της σημαντικότητας όλων των αγαθών του ΠΣ, όπως φυσικά αγαθά (π.χ. κτίρια), δικτυακές υποδομές, λογισμικό, υλικό και ανθρώπινο δυναμικό,
- ✓ προσδιορισμός και κατηγοριοποίηση όλων των απειλών που αντιμετωπίζουν τα αγαθά,
- ✓ προσδιορισμός και κατηγοριοποίηση των αδυναμιών που αντιμετωπίζουν τα κρίσιμα αγαθά του οργανισμού απέναντι στις πιο κρίσιμες απειλές, και
- ✓ επιλογή των κατάλληλων μέτρων προστασίας των κρίσιμων αγαθών.

Σε κάθε ένα από τα παραπάνω συνεργατικά προβλήματα συμμετέχουν διαφορετικές κατηγορίες χρηστών, δίνοντας τη γνώση και την εμπειρία από την δική τους οπτική γωνία (π.χ. επιχειρησιακή, τεχνολογική, νομική).

3.2 Πολυκριτηριακή λήψη αποφάσεων

Η Πολυκριτηριακή Λήψη Αποφάσεων (Multiple Criteria Decision Making -MCDM) εμφανίζεται το προηγούμενο αιώνα όπου εξετάζεται για πρώτη φορά η ύπαρξη και σύγκριση δύο εναλλακτικών επιλογών [10]. Η αδυναμία των μέχρι τότε υπαρχόντων μεθοδολογιών, οδήγησε στην ανάπτυξη της Πολυκριτηριακής Ανάλυσης Αποφάσεων η οποία ήρθε να αντιμετωπίσει και να λύσει πολυδιάστατα προβλήματα πολλαπλών, αντικρουόμενων μεταξύ τους, κριτηρίων αξιολόγησης. Από το 1970 μέχρι σήμερα ο τομέας αυτός συνεχώς εξελίσσεται και οι μεθοδολογίες επίλυσης πολυκριτηριακών προβλημάτων εφαρμόζονται σε διάφορους τομείς.

Τα στάδια λήψης αποφάσεων σύμφωνα με τον Roy [12] είναι τέσσερα (4), όπως φαίνεται και στην Εικόνα 2. Τα στάδια αυτά κατά τη διάρκεια επίλυσης ενός προβλήματος δεν πραγματοποιούνται κατά ανάγκη διαδοχικά, αλλά ο αναλυτής είναι σε θέση να επιστρέψει σε κάποιο από τα προηγούμενα βήματα ώστε να ελέγξει ή να διαφοροποιήσει κάποιες από τις ενέργειές του [16].



Εικόνα 2: Στάδια λήψης απόφασης

Πιο αναλυτικά τα στάδια που προτείνει ο Roy [12] είναι:

Στάδιο 1: Αντικείμενο της απόφασης

Προσδιορισμός του προβλήματος που απαιτεί λήψη απόφασης. Τα μέλη της ομάδας απόφασης καθορίζουν τον στόχο της απόφασης και τον χώρο των εφικτών λύσεων. Συγκεκριμένα στο στάδιο αυτό πρέπει να ολοκληρωθούν οι εξής βασικές εργασίες:

- ✓ **Αυστηρός ορισμός του συνόλου Α των δράσεων**. Πρέπει δηλαδή το αντικείμενο της απόφασης να αναλυθεί σε ένα διακριτό ή συνεχές σύνολο δράσεων Α (εναλλακτικών αποφάσεων-επιλογών).

- ✓ **Ο καθορισμός μιας προβληματικής**. Καθορίζεται το αντικείμενο της απόφασης, ο τρόπος δηλαδή με τον οποίο θα εξεταστούν οι εναλλακτικές. Η εξέταση των εναλλακτικών μπορεί να πραγματοποιηθεί με μία από τις παρακάτω προβληματικές ανάλογα με την φύση του προβλήματος:

  - **Προβληματική α**: επιλογή μιας και μόνο δράσης (εναλλακτικής) από το σύνολο Α
  - **Προβληματική β**: ταξινόμηση των δράσεων σε ομογενείς προκαθορισμένες κατηγορίες.

- **Προβληματική γ**: κατάταξη των δράσεων του συνόλου Α από την καλύτερη μέχρι την χειρότερη
- **Προβληματική δ**: περιγραφή των δράσεων και των συνεπειών τους στη γλώσσα των εμπλεκόμενων κατά την διαδικασία της απόφασης.

Στάδιο 2: Συνεπής Οικογένεια Κριτηρίων

Στο συγκεκριμένο στάδιο, γίνεται η εύρεση των κατάλληλων κριτηρίων αξιολόγησης των εναλλακτικών λύσεων-επιλογών της απόφασης. Κριτήριο θεωρείται οποιοσδήποτε παράγοντας που επιδρά στη λήψη της απόφασης. Ένα κριτήριο μοντελοποιείται από μια πραγματική συνάρτηση:

$$g: A \rightarrow R \,/\, a \rightarrow g(a), \qquad (3.1)$$

όπου g (a) είναι η τιμή ή αξιολόγηση της δράσης a ∈ A πάνω στο κριτήριο g.

Στο στάδιο αυτό δημιουργείται μια συνεπής οικογένεια κριτηρίων F = {g_1, g_2,…g_n}, η οποία περιλαμβάνει n κριτήρια τα οποία πρέπει να πληρούν τις παρακάτω συνθήκες:

- ✓ **Συνέπεια ή μονοτονία (cohesiveness).** Αν για ένα ζεύγος δράσεων (a,b) ισχύει: g_i(a) = g_i (b), και g_j(a) > g_j (b), ∀ $i \neq j$, τότε η δράση a υπερέχει της b (aSb).
- ✓ **Επάρκεια (exhaustiveness).** Αν για ένα ζεύγος δράσεων (a,b) ισχύει: g_i(a) = g_i(b), ∀ i = 1,2, …, n, τότε συνεπάγεται ότι η δράση a είναι αδιάφορη της b. Δηλαδή δεν απουσιάζει κανένα κριτήριο απόφασης από το σύνολο των n κριτηρίων.
- ✓ **Μη πλεονασμός (non redundancy**). Η διαγραφή ενός κριτηρίου g_i από το σύνολο των κριτηρίων είναι ικανή να αναιρέσει μία από τις προηγούμενες συνθήκες για κάποια ζεύγη δράσεων.

Οι σημαντικότεροι τύποι κριτηρίων είναι:

- ✓ **Κριτήρια ποσοτικά ή μετρικά (measurable criteria)..** Πρόκειται για κριτήρια των οποίων η κλίμακα προτίμησης είναι μία κλίμακα μέτρου.
- ✓ **Κριτήρια ποιοτικά ή διάταξης (ordinal criteria)**. Πρόκειται για κριτήρια των οποίων η κλίμακα προτίμησης είναι μία κλίμακα διάταξης.

- ✓ **Κριτήρια πιθανοτικά (stochastic criteria).** Πρόκειται για κριτήρια στα οποία η αξιολόγηση μιας δράσης είναι κατά πιθανότητα γνωστή πάνω στην κλίμακα του κριτηρίου. Αν [g ∗,g*] είναι η κλίμακα του κριτηρίου g, η τιμή της δράσης a ορίζεται μέσω μιας πυκνότητας πιθανότητας f για την οποία ισχύει:

$$\sum_j f(g^j) = 1 \text{ , όταν η κλίμακα είναι διακριτή} \quad (3.2)$$

$$\int_{g*}^{g^*} f(g)dg = 1 \text{ , όταν η κλίμακα είναι συνεχής.} \quad (3.3)$$

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

Στάδιο 3: Μοντέλο ολικής προτίμησης

Γίνεται μοντελοποίηση των προτιμήσεων (κριτηρίων) των μελών και προσπάθεια για σύνθεσή τους και ενσωμάτωσή τους στο μοντέλο του προβλήματος. Στο στάδιο αυτό ο αναλυτής πρέπει να επιλέξει μία μέθοδο πολυκριτήριας σύνθεσης με την οποία θα γίνει η σύγκριση των δράσεων του συνόλου Α λαμβάνοντας υπόψη όλες τις τιμές των δράσεων (εναλλακτικών) πάνω στα κριτήρια της συνεπούς οικογένειας κριτηρίων.

Στάδιο 4: Υποστήριξη της απόφασης

Διερεύνηση και αξιολόγηση της απόφασης. Στο στάδιο αυτό κρίνεται η μέθοδος που χρησιμοποιήθηκε για να λυθεί το πρόβλημα όσον αφορά στην επιλογή της προβληματικής αλλά και στον τρόπο σύνθεσης των προτιμήσεων. Πρόκειται για ένα συμπληρωματικό στάδιο του προηγούμενου, όπου ο αναλυτής είναι σε θέση να εξετάσει και να αξιολογήσει τα αποτελέσματα του μοντέλου το οποίο επιλέχθηκε στο Στάδιο 3.

3.3 Υπάρχουσες πολυκριτηριακές μέθοδοι λήψης αποφάσεων

Στην βιβλιογραφία, συναντούνται διάφορες μεθοδολογίες επίλυσης πολυκριτηριακών προβλημάτων και έχουν γίνει αρκετές προσπάθειες κατηγοριοποίησής τους, οι σημαντικότερες από τις οποίες παρουσιάζονται στην συνέχεια.

Ο Σίσκος [16] διακρίνει τις παρακάτω κατηγορίες πολυκριτηριακών μεθοδολογιών:

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

Άλλη μία κατηγοριοποίηση των μεθόδων η οποία έγινε από τους Pardalos et al. [9], είναι η εξής:

- ✓ **Πολυκριτήριος μαθηματικός προγραμματισμός (Multiobjective mathematical programming).** Η ομάδα αυτή αποτελείται από μοντέλα μαθηματικού προγραμματισμού με περισσότερες από μία αντικειμενικές συναρτήσεις. Στην κατηγορία αυτή, ανήκει η μεθοδολογία Goal Programming, που αναπτύχθηκε από τους Charnes και Cooper (1961) [2], καθώς και οι τεχνικές βελτιστοποίησης διανύσματος (για τον υπολογισμό του συνόλου των μη κυριαρχούμενων λύσεων) οι οποίες αναπτύχθηκαν από πολλούς συγγραφείς (Evans and Stuer, 1973 [3], Gal, 1977 [4], Goicoechea et al., 1982 [5]).
- ✓ **Μέθοδοι σχέσεων υπεροχής (outranking relations).** Οι μέθοδοι των σχέσεων υπεροχής διευκολύνουν την σύγκριση μεταξύ εναλλακτικών με την αντιστοίχιση αρχικών βαρών στα κριτήρια αποφάσεων και στη συνέχεια μεταβάλλουν αυτά τα βάρη στα πλαίσια της ανάλυσης ευαισθησίας εάν δεν είναι γνωστή η αρχική τους τιμή. Η σύγκριση μεταξύ εναλλακτικών συνεχίζεται για κάθε κριτήριο απόφασης, καθορίζοντας την υπεροχή μίας εναλλακτικής έναντι μίας άλλης. Το τελικό αποτέλεσμα της διαδικασίας αυτής είναι η κατάταξη των διαφόρων επιλογών. Όλες οι μέθοδοι των σχέσεων υπεροχής λειτουργούν σε δύο στάδια. Αρχικά αναπτύσσεται η σχέση υπεροχής βάσει πληροφοριών που παρέχει ο λήπτης αποφάσεων και στην συνέχεια χρησιμοποιούνται ευρετικές διαδικασίες για την αξιοποίηση των σχέσεων υπεροχής με σκοπό την αξιολόγηση των εναλλακτικών δραστηριοτήτων ως προς την επιλογή, την κατάταξη και την ταξινόμηση. Οι πιο γνωστές μεθοδολογίες της κατηγορίας αυτής είναι η ELECTRE (I,II,III, IV, TRI) η οποία αναπτύχθηκε από τον Roy [11], η PROMETHEE [1], καθώς και άλλες προσεγγίσεις οι οποίες καλύπτουν την περίπτωση ύπαρξης αβεβαιότητας, όπως αυτές που παρουσιάζονται από τους Martel και D'Avignon [7][8] και Σίσκος 1983 [15].
- ✓ **Θεωρία Πολυκριτήριας χρησιμότητας (Multiattribute Utility Theory - MAUT).** Οι Roy και Vincke το 1984 διατύπωσαν το αξίωμα της ολικής και μεταβατικής συγκρισιμότητας, με το οποίο διερευνούνται εκείνες οι ιδιότητες που χαρακτηρίζουν ένα σύστημα προτιμήσεων, ώστε

αυτό να μπορεί να εκφραστεί από ένα συγκεκριμένο μοντέλο χρησιμότητας. Στην κατηγορία αυτή ανήκει και η μεθοδολογία Αναλυτικής Ιεράρχησης (Analytic Hierarchy Process - AHP) που αναπτύχθηκε από τον Saaty το 1980 [13].

- ✓ **Αναλυτική - συνθετική προσέγγιση (preference disaggregation approach).** Στην κατηγορία αυτή γίνεται χρήση μοντέλων ανάλυσης παλινδρόμησης στην προσπάθεια προσέγγισης της συλλογικής των αποφασιζόντων. Μια αντιπροσωπευτική οικογένεια μεθοδολογιών της κατηγορίας αυτής είναι η UTA (UTilités Additives) η οποία παρουσιάστηκε από τους Jacquet–Lagrèze και Siskos το 1982 [6]**.**

Οι υπάρχουσες μεθοδολογίες επίλυσης πολυκριτηριακών προβλημάτων έχουν εφαρμογή σε πολλά και διαφορετικής φύσεως προβλήματα (οικονομικά, προβλήματα επιλογής προσωπικού, προβλήματα ενέργειας κλπ.), ενώ ταυτόχρονα έχουν αναπτυχθεί αυτοματοποιημένα εργαλεία τα οποία υλοποιούν τις μεθοδολογίες αυτές και αποτελούν πολύτιμα εφόδια για τους αποφασίζοντες.

Για την ανάπτυξη της μεθοδολογίας STORM-RM χρησιμοποιήθηκαν στοιχεία της μεθοδολογίας AHP (Analytical Hierarchy Process), διότι η AHP καλύπτει τα παρακάτω σημαντικά κριτήρια:

- ✓ επιτρέπει την συνεργατικότητα (πολλοί συμμετέχοντες, διαφορετικά βάρη συμμετοχής), η οποία είναι απαραίτητη για την συλλογή της απαραίτητης γνώσης από όλους τους εμπλεκόμενους χρήστες του ΠΣ στην επίλυση του πολυκριτηριακού προβλήματος ανάλυσης και διαχείρισης επικινδυνότητας,
- ✓ απεικονίζει ένα πρόβλημα σε ιεραρχική δομή παρέχοντας τη δυνατότητα μείωσης της πολυπλοκότητας δύσκολων προβλημάτων (επιμερισμός σε μικρότερα υπο-προβλήματα), το οποίο είναι αρκετά σημαντικό για το πρόβλημα της ανάλυσης επικινδυνότητας ειδικά σε πολύπλοκα ΠΣ (όπως αυτά των εμπορικών λιμένων),
- ✓ μπορεί να υλοποιηθεί εύκολα με την βοήθεια γνωστών γλωσσών προγραμματισμού και να ενσωματωθεί σε κάποιο αυτοματοποιημένο εργαλείο.

Στην ενότητα που ακολουθεί, θα παρουσιαστεί αναλυτικά ο τρόπος με τον οποίο επιλύει ένα πρόβλημα η μεθοδολογία AHP, καθώς και ένα ενδεικτικό παράδειγμα για την καλύτερη κατανόηση του αλγορίθμου επίλυσης που χρησιμοποιεί.

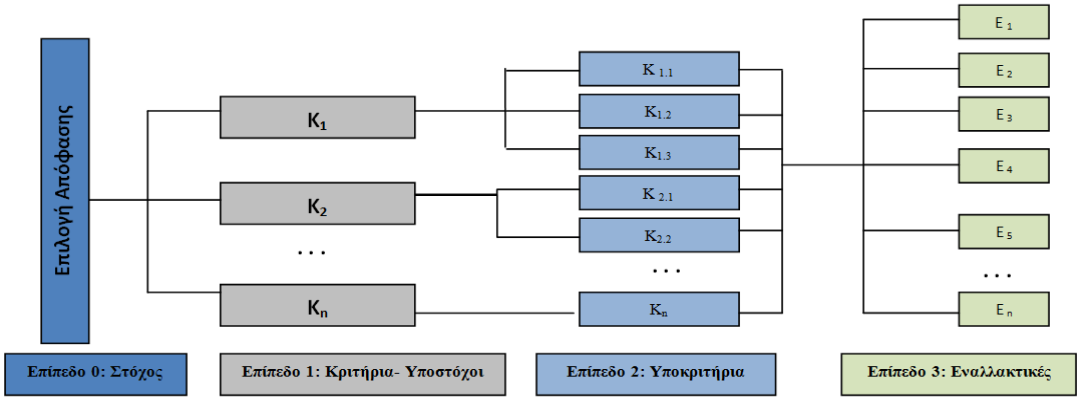
3.4 Analytical Hierarchy Process (AHP)

Η μέθοδος AHP αναπτύχθηκε από τον Thomas Saaty (1980) [13][14] και συνδυάζει ανάλυση πολλαπλών κριτηρίων σε ιεραρχική δομή, εξαγωγή της σχετικής σημαντικότητας των κριτηρίων, σύγκριση των εναλλακτικών λύσεων για κάθε κριτήριο και καθορισμός της συνολικής βαθμολογίας των εναλλακτικών λύσεων. Η AHP έχει βρει εφαρμογή σε πολλούς διαφορετικούς τομείς δραστηριοτήτων, όπως σε επιχειρήσεις, κυβερνήσεις, κοινωνικές μελέτες, έρευνα και ανάπτυξη και άλλους τομείς όπου απαιτείται η λήψη αποφάσεων και στις οποίες βασικό ρόλο παίζει η επιλογή, η προτεραιότητα και η πρόβλεψη. Συμβάλλει στην οργάνωση του προβλήματος και στη δόμηση της πολυπλοκότητας, μέσω της ανάλυσης του προβλήματος σε μικρότερα επιμέρους προβλήματα, γεγονός που την κάνει κατάλληλη για ένα πλήθος εφαρμογών.

Τα βασικά βήματα της μεθοδολογίας είναι τα εξής:

- ✓ Ανάλυση του προβλήματος σε μια ιεραρχική δομή.
- ✓ Σύγκριση των στοιχείων απόφασης (ανά ζεύγη) από τον αποφασίζοντα (ες) και συλλογή των προτιμήσεων.
- ✓ Υπολογισμός των προτεραιοτήτων και των σχετικών βαρών κάθε στοιχείου απόφασης.
- ✓ Σύνθεση των επιμέρους βαρών και εξαγωγή των γενικών προτεραιοτήτων των εναλλακτικών επιλογών.

Τα δύο πρώτα βήματα απαιτούν τη συμμετοχή του αποφασίζοντα (ή της ομάδας απόφασης) κατά την διαδικασία απόφασης, ενώ τα δύο τελευταία είναι υπολογιστικά. Το στάδιο της ιεραρχικής ανάλυσης του προβλήματος αποτελεί το πιο σημαντικό στάδιο της μεθόδου. Στην Εικόνα 3 φαίνεται πώς είναι δομημένη μια ιεραρχία σε ένα πρόβλημα AHP. Ο απώτερος στόχος αναλύεται σε υποστόχους ή κριτήρια (K_1, K_2, ... K_n) που αποτελούν τα κύρια στοιχεία της απόφασης. Τα κριτήρια αυτά με τη σειρά τους αναλύονται σε επιμέρους υποκριτήρια. Για παράδειγμα, το κριτήριο K_1 αναλύεται στα υποκριτήρια $K_{1.1}$, $K_{1.2}$ και $K_{1.3}$, ενώ το κριτήριο K_2 αναλύεται στα υποκριτήρια $K_{2.1}$, $K_{2.2.}$ Αυτό μπορεί να επαναλαμβάνεται σε βάθος, δημιουργώντας το δένδρο της απόφασης, συνθέτοντας μια ιεραρχική ανάλυση, ώσπου να φτάσουμε στο επίπεδο των εναλλακτικών λύσεων E_1, E_2, E_3, E_4, E_5... E_n. Αυτό είναι το κατώτατο επίπεδο κάθε κλάδου του δένδρου της ιεραρχίας, με τις εναλλακτικές προς αξιολόγηση λύσεις να αποτελούν τα φύλλα του δένδρου.



Εικόνα 3: Ιεραρχική Δομή Προβλήματος

Η σύγκριση των στόχων (κριτηρίων, υποκριτηρίων και εναλλακτικών) ανά ζεύγη γίνεται ως εξής: Ξεκινώντας από τη ρίζα του δένδρου, γίνεται για κάθε στοιχείο συγκριτική αξιολόγηση ανά ζεύγη των στοιχείων στα οποία αναλύεται. Για κάθε ζεύγος, ο αποφασίζων εκτιμά υποκειμενικά τη σπουδαιότητα του ενός σε σχέση με τη σπουδαιότητα του άλλου. Αυτό γίνεται με ανά ζεύγη συγκρίσεις της μορφής: "πόσο πιο σημαντικό είναι το στοιχείο 1 από το στοιχείο 2". Οι συγκρίσεις αυτές γίνονται για όλα τα επίπεδα του δένδρου μέχρι να φτάσουμε στο επίπεδο των εναλλακτικών, όπου θα λάβουμε υπόψη μας όλες τις συγκρίσεις για τον υπολογισμό των τελικών προτεραιοτήτων των εναλλακτικών του προβλήματος. Οι συγκρίσεις γίνονται με την αριθμητική κλίμακα του Πίνακα 2.

Πίνακας 2: Αριθμητική Κλίμακα σημαντικότητας Saaty [13][14]

Σημασία	Βαθμός	Περιγραφή
Ίση σημασία	**1**	Δύο στοιχεία συμβάλλουν εξίσου στον στόχο
Ασθενώς σημαντικότερο	**3**	Το ένα στοιχείο υπερισχύει ελαφρώς από το άλλο
Σημαντικότερο	**5**	Το ένα στοιχείο υπερισχύει σημαντικά από το άλλο
Πολύ πιο σημαντικό	**7**	Ένα στοιχείο υπερισχύει πολύ έντονα από ένα άλλο
Απόλυτα πιο σημαντικό	**9**	Ένα στοιχείο υπερισχύει με τη δυνατότερη ένταση από ένα άλλο
Οι τιμές 2,4,6, 8 μπορούν να χρησιμοποιηθούν ως ενδιάμεσες τιμές, ενώ αν κριθεί απαραίτητο μπορούν να χρησιμοποιηθούν και τιμές όπως 1.1, 1.2, ..., 1.9 αν η σημαντικότητα των κριτηρίων είναι πολύ κοντά		

Η βαθμολογία αυτή συγκεντρώνεται σε τετραγωνικούς πίνακες (pairwise comparison matrices) της μορφής του Πίνακα 3.

Πίνακας 3: Πίνακας Συγκρίσεων AHP

Κριτήρια (Criteria)	K_1	K_2	K_3	...	K_n
K_1 :	a_{11}	a_{12}	a_{13}	..	a_{1n}
K_2 :	a_{21}	a_{22}	a_{23}	..	a_{2n}
K_3 :	a_{31}	a_{32}	a_{33}	..	a_{3n}
...	..	..	..	..	
K_n	a_{n1}	a_{n2}	a_{n3}	...	a_{nn}
Άθροισμα στηλών	S_1	S_2	S_3		S_n

Τα a_{ij} είναι οι βαθμοί σημαντικότητας που προκύπτουν από τις ανά δύο συγκρίσεις των στοιχείων i και j. Τα στοιχεία της κύριας διαγωνίου του πίνακα συγκρίσεων είναι 1 (δηλαδή a_{ij} =1 για i=j), τα στοιχεία που βρίσκονται πάνω από την κύρια διαγώνιο εκφράζουν τους βαθμούς σημαντικότητας (από την σύγκριση ανά ζεύγη) των στοιχείων ενώ τα στοιχεία που βρίσκονται κάτω από την κύρια διαγώνιο είναι τα αντίστροφα των βαθμών σημαντικότητας. Για παράδειγμα το a_{12} δηλώνει τον βαθμό σημαντικότητας του στοιχείου K_1 έναντι το στοιχείου K_2,όπως φαίνονται στον Πίνακα 4.

Πίνακας 4: Παράδειγμα Πίνακας Συγκρίσεων AHP

Κριτήρια (Criteria)	K_1	K_2	K_3	...	K_n
K_1 :	1	a_{12}	a_{13}	..	a_{1n}
K_2 :	$1/a_{12}$	1	a_{23}	..	a_{2n}
K_3 :	$1/a_{13}$	$1/a_{23}$	1	..	a_{3n}
...	..	..	..	1	
K_n	$1/a_{1n}$	$1/a_{2n}$	$1/a_{3n}$		1
Άθροισμα στηλών	S_1	S_2	S_3		S_n

Για την αποφυγή ασυνέπειας, ο Saaty υιοθετεί ένα δείκτη συνέπειας ή ευαισθησίας των εκτιμήσεων (Consistency Index - CI). Ο δείκτης αυτός βασίζεται στη μέγιστη ιδιοτιμή λmax του αντίστοιχου πίνακα συγκρίσεων, και υπολογίζεται ως εξής:

$$CI = \frac{\lambda max - n}{n-1}, \qquad (3.4)$$

Η τιμή του δείκτη συγκρίνεται με τυχαίους δείκτες ευαισθησίας (Random Consistency Index). Ο δείκτης RI (Random Consistency Index) παίρνει τιμές ανάλογα με τη διάσταση n, του πίνακα συγκρίσεων όπως φαίνεται στον Πίνακα 5.

Πίνακας 5: Πίνακας Τυχαίων Δεικτών (Random Consistency Index)

Τυχαίοι Δείκτες (Random Consistency Index - RI)															
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Στην συνέχεια, υπολογίζεται ο Λόγος Ευαισθησίας (Consistency Ratio - CR) ο οποίος προκύπτει από την σύγκριση του Δείκτη Ευαισθησίας CI, με τον Τυχαίο Δείκτη Ευαισθησίας, RI, ως εξής:

$$CR= \frac{CI}{RI}, \tag{3.5}$$

και δεν επιτρέπεται να υπερβαίνει το 10% (CR<10%).

Τα αξιώματα στα οποία βασίζεται η AHP [13] είναι:

- ✓ Το πρόβλημα της απόφασης μπορεί να διαμορφωθεί σε μία ιεραρχία, όπου απεικονίζονται όλα τα κριτήρια, υποκριτήρια και οι εναλλακτικές του προβλήματος.
- ✓ Ο αποφασίζων μπορεί να παρέχει συγκρίσεις ανά ζεύγη α_{ij} δύο εναλλακτικών i και j αναφορικά με ένα κριτήριο/ υπο-κριτήριο στη βάση μίας αντίστροφης κλίμακας $\alpha_{ij}=\frac{\mathbf{1}}{\boldsymbol{a_{ji}}}$.
- ✓ Ο αποφασίζων ποτέ δεν κρίνει μία εναλλακτική ως απόλυτα καλύτερη από μία άλλη αναφορικά με ένα κριτήριο, δηλαδή $\alpha_{ij}\neq\infty$.

Όταν καταστρωθεί ένας πίνακας συγκρίσεων, υπολογίζουμε την προτεραιότητα (σχετική σημαντικότητα) που έχουν τα κριτήρια του επιπέδου αυτού μεταξύ τους, ως αποτέλεσμα των εκτιμήσεων που έχουμε καταχωρίσει στον πίνακα. Η σχετική σημαντικότητα των στοιχείων του κάθε επιπέδου δίνεται από το κύριο ιδιοδιάνυσμα (eigenvector) του πίνακα. Το άθροισμα των συστατικών του ιδιοδιανύσματος είναι ίσο με τη μονάδα. Κατανέμονται έτσι οι προτεραιότητες σε κάθε στοιχείο του κάθε επιπέδου. Ο τρόπος υπολογισμού των προτεραιοτήτων αυτών είναι ο εξής:

- ✓ Υπολογίζουμε το άθροισμα των στοιχείων S_j κατά μήκος κάθε στήλης j.

- ✓ Στην συνέχεια διαιρούμε κάθε στοιχείο a_{ij} του πίνακα με το άθροισμα της στήλης S_i στην οποία ανήκει $b_{ij}=a_{ij}/S_j$.
- ✓ Αθροίζουμε τα νέα αυτά στοιχεία b_{ij} κατά μήκος κάθε γραμμής i και διαιρούμε με τον αριθμό των στηλών j (δηλαδή, υπολογίζουμε τον μέσο όρο των νέων αυτών στοιχείων, ανά γραμμή). Ο μέσος αυτός όρος είναι η προτεραιότητα του κριτηρίου που εκφράζεται από την αντίστοιχη γραμμή (Πίνακας 6).

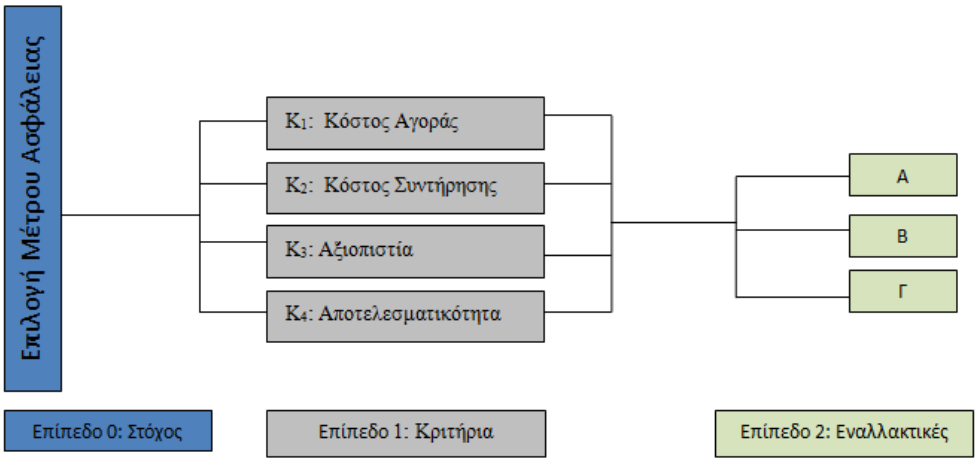
Πίνακας 6: Υπολογισμός Προτεραιοτήτων

Κριτήρια (Criteria)	K_1	K_2	K_3	...	K_n	Προτεραιότητες (eigenvector)
K_1 :	$b_{11}=a_{11}/S_1$	$b_{12}=a_{12}/S_2$	$b_{13}=a_{13}/S_3$	..	b_{1n}	$W_1=\frac{\sum_{j=1}^{n} b_{1j}}{j}$
K_2 :	$b_{21}=a_{21}/S_1$	$b_{22}=a_{22}/S_2$	$b_{23}=a_{23}/S_3$	..	b_{2n}	$W_2=\frac{\sum_{j=1}^{n} b_{2j}}{j}$
K_3 :	$b_{31}=a_{31}/S_1$	$b_{32}=a_{32}/S_2$	$b_{33}=a_{33}/S_3$	..	b_{3n}	$W_3=\frac{\sum_{j=1}^{n} b_{3j}}{j}$
...	..	..	..	..		
K_n	$b_{n1}=a_{n1}/S_1$	$b_{n2}=a_{n2}/S_2$	$b_{n3}=a_{n3}/S_3$	..	b_{nn}	$W_n=\frac{\sum_{j=1}^{n} b_{nj}}{j}$
Άθροισμα στηλών	1	1	1		1	

Η παραπάνω διαδικασία συνεχίζεται για κάθε επίπεδο του δένδρου μέχρι να φτάσουμε στο τελευταίο επίπεδο που είναι οι εναλλακτικές της απόφασής μας.

Παράδειγμα χρήσης της AHP στην επιλογή κατάλληλου μέτρου ασφάλειας:

Για να γίνει πιο κατανοητός ο τρόπος επίλυσης της AHP ακολουθεί ένα παράδειγμα όπου ο στόχος είναι η επιλογή του κατάλληλου μέτρου ασφάλειας ανάμεσα από τρεις εναλλακτικές (μέτρα ασφάλειας: Α, Β, Γ). Τα κριτήρια αξιολόγησης είναι το *Κόστος Αγοράς*, το *Κόστος Συντήρησης*, η *Αξιοπιστία* και η *Αποτελεσματικότητα*.



Εικόνα 4: Ιεραρχική δομή του προβλήματος επιλογής μέτρου ασφάλειας

Κάθε στοιχείο του επιπέδου i συγκρίνεται με όλα τα στοιχεία του ίδιου επιπέδου αναφορικά με κάθε στοιχείο του ανώτερου επιπέδου. Στο παράδειγμά μας θα συγκριθούν πρώτα τα κριτήρια μεταξύ τους και στην συνέχεια οι εναλλακτικές αναφορικά με κάθε κριτήριο του επιπέδου 1. Ο πίνακας συγκρίσεων που ακολουθεί είναι ενδεικτικός και προέκυψε από τις ανά δύο συγκρίσεις των στοιχείων (κριτηρίων) του επιπέδου 1.

Πίνακας 7: Πίνακας Συγκρίσεων 1ου επιπέδου

Κριτήρια (Criteria)	Κόστος Αγοράς	Κόστος Συντήρησης	Αξιοπιστία	Αποτελεσματικότητα
K_1: Κόστος Αγοράς	1	2	3	3
K_2: Κόστος Συντήρησης	1/2	1	3	3
K_3: Αξιοπιστία	1/3	1/3	1	1/2
K_4: Αποτελεσματικότητα	1/3	1/3	2	1
Άθροισμα στηλών	S_1=2,17	S_2=3,67	S_3= 9,00	S_4=7,50
Λόγος Ευαισθησίας (consistency ratio)=0,05				

Πιο συγκεκριμένα από την πρώτη γραμμή του παραπάνω πίνακα φαίνεται ότι το κριτήριο *Κόστος Αγοράς* είναι ασθενώς πιο σημαντικό (2) από το κριτήριο *Κόστος Συντήρησης* και μέτρια σημαντικότερο (3) από τα κριτήρια *Αξιοπιστία* και *Αποτελεσματικότητα*. Στην συνέχεια γίνεται η κανονικοποίηση των στηλών διαιρώντας κάθε στοιχείο του πίνακα συγκρίσεων (Πίνακας 7) με το άθροισμα S_j της στήλης j στην οποία ανήκει. Επίσης βρίσκουμε την προτεραιότητα (ή ειδικό βάρος) του κάθε κριτηρίου w_i υπολογίζοντας τον μέσο όρο κάθε γραμμής i του κανονικοποιημένου πίνακα, όπως φαίνεται στον Πίνακα 8.

Πίνακας 8: Πίνακας Προτεραιοτήτων 1ου Επιπέδου

Κριτήρια (Criteria)	Κόστος Αγοράς	Κόστος Συντήρησης	Αξιοπιστία	Αποτελεσματικότητα	Προτεραιότητες (w_i)
K_1 : Κόστος Αγοράς	0,46	0,55	0,33	0,40	0,44
K_2 : Κόστος Συντήρησης	0,23	0,27	0,33	0,40	0,31
K_3 : Αξιοπιστία	0,15	0,09	0,11	0,07	0,11
K_4 : Αποτελεσματικότητα	0,15	0,09	0,22	0,13	0,15
Άθροισμα στηλών	1	1	1	1	

Στη συνέχεια, αφού έχουμε υπολογίσει τις προτεραιότητες, w_i, κάθε στοιχείου (κριτηρίου) του επιπέδου 1, συγκρίνουμε όλα τα στοιχεία (εναλλακτικές) του επιπέδου 2, αναφορικά με τα κριτήρια, με τρόπο παρόμοιο με παραπάνω. Έτσι προκύπτουν οι Πίνακες 9,10,11 και 12.

Πίνακας 9: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κόστος Αγοράς

Κόστος Αγοράς	Α	Β	Γ	Προτεραιότητα (w_i)
Α	1	4	3	0,63
Β	1/4	1	2	0,22
Γ	1/3	1/2	1	0,15

Πίνακας 10: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κόστος Συντήρησης

Κόστος Συντήρησης	Α	Β	Γ	Προτεραιότητα (w_i)
Α	1	1	2	0,41
Β	1	1	1	0,33
Γ	1/2	1	1	0,26

Πίνακας 11: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Αξιοπιστία

Αξιοπιστία	Α	Β	Γ	Προτεραιότητα (w_i)
Α	1	3	1	0,43
Β	1/3	1	1/3	0,14
Γ	1	3	1	0,43

Πίνακας 12: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Αποτελεσματικότητα

Αποτελεσματικότητα	Α	Β	Γ	Προτεραιότητα (w_i)
Α	1	1/3	5	0,28
Β	3	1	7	0,64
Γ	1/5	1/7	1	0,07

Για να βρούμε τις τελικές προτεραιότητες FP_a κάθε εναλλακτικής πολλαπλασιάζουμε τις προτεραιότητες Pa_i των εναλλακτικών ως προς ένα κριτήριο i με το ειδικό βάρος w_i του κριτηρίου i και, στην συνέχεια, τα αθροίζουμε. Δηλαδή

$$FP_a = \sum_{i=1}^{n} w_i * Pa_i \quad (3.6)$$

Έτσι, για την τελική προτεραιότητα των μέτρων ασφάλειας Α, Β και Γ έχουμε:

$$FP_A = 0,44*0,63 + 0,31*0,41 + 0,11*0,43 + 0,15*0,28 \quad (3.7)$$

$$FP_B = 0,44*0,22 + 0,31*0,33 + 0,11*0,14 + 0,15*0,64 \quad (3.8)$$

$$FP_\Gamma = 0,44*0,15 + 0,31*0,26 + 0,11*0,43 + 0,15*0,07 \quad (3.9)$$

Πίνακας 13: Τελικές Προτεραιότητες Εναλλακτικών

Κριτήρια (Criteria)	Κόστος Αγοράς	Κόστος Συντήρησης	Αξιοπιστία	Αποτελεσματικότητα	FP_a
w_i	0,44	0,31	0,11	0,15	
Α	0,63	0,41	0,43	0,28	**0,49**
Β	0,22	0,33	0,14	0,64	**0,31**
Γ	0,15	0,26	0,43	0,07	**0,20**

Όπως φαίνεται από τις τελικές προτεραιότητες των εναλλακτικών (μέτρα ασφάλειας) του Πίνακα 13, η καλύτερη επιλογή είναι το μέτρο ασφάλειας Α το οποίο υπερέχει με 0,49 ή 49% από τα άλλα μέτρα ασφάλειας. Συγκεκριμένα, λαμβάνοντας υπόψη τις προτιμήσεις ως προς τα κριτήρια Κόστος

Αγοράς, Κόστος Συντήρησης, Αξιοπιστία και Αποτελεσματικότητα, το μέτρο ασφάλειας φαίνεται να καλύπτει τις ανάγκες του αποφασίζοντα του παραδείγματος και αποτελεί την βέλτιστη επιλογή του.

3.5 Συμπεράσματα Κεφαλαίου

Το γεγονός ότι τα σημερινά ΠΣ χαρακτηρίζονται από πολυπλοκότητα (κατανεμημένα και πολύπλοκα συστήματα, μεγάλος αριθμός χρηστών, πλήθος ηλεκτρονικών υπηρεσιών και κρίσιμα πληροφοριακά δεδομένα) σε συνδυασμό με τις αδυναμίες των υπαρχουσών μεθοδολογιών (όπως αυτές περιγράφηκαν στο 2^{ο} Κεφάλαιο) να ανταπεξέλθουν στην σημερινή πραγματικότητα, δημιουργεί την ανάγκη για αναβαθμισμένες μεθοδολογίες ανάλυσης και διαχείρισης της επικινδυνότητας.

Στο κεφάλαιο αυτό, παρουσιάστηκε η ανάλυση και διαχείριση της επικινδυνότητας ως ένα πολυκριτηριακό πρόβλημα συνεργατικής λήψης αποφάσεων όπου πολλοί συμμετέχοντες καλούνται να το επιλύσουν. Συγκεκριμένα, οι αποφασίζοντες οι οποίοι είναι χρήστες των ΠΣ (διαχειριστές, προϊστάμενοι τμημάτων, ομάδα ασφάλειας, τοπικοί χρήστες και συνεργάτες), καλούνται με βάση τις δικές τους προτιμήσεις (βάζοντας διαφορετικά κριτήρια) να προσδιορίσουν και να αξιολογήσουν τις επιτπώσεις ασφάλειας, τις απειλές και τις αδυναμίες και ως αποτέλεσμα και την κρισιμότητα των αγαθών του ΠΣ του οργανισμού τους.

Στην συνέχεια παρουσιάστηκαν οι βασικές έννοιες της πολυκριτηριακής λήψης αποφάσεων, έγινε αναφορά στον τρόπο επίλυσης πολυκριτηριακών προβλημάτων και παρουσιάστηκαν οι κατηγορίες των υφιστάμενων μεθοδολογιών, όπως καταγράφονται στην σύγχρονη βιβλιογραφία.

Τέλος, αναλύθηκε η μέθοδος AHP της οποίας βασικά στοιχεία επιλέχθηκαν να ενσωματωθούν στον αλγόριθμο της μεθοδολογίας η οποία παρουσιάζεται στο κεφάλαιο που ακολουθεί.

3.6 Βιβλιογραφία 3ου Κεφαλαίου

[1] Brans, J.P., and Vincke, P.,. A preference ranking organization method: The PROMETHEE method for MCDM, Management Science, Vol. 31, No. 6, pp.647-656., 1985.

[2] Charnes, A. and Cooper, W.W. . "Management Models and Industrial Applications of Linear Programming, John Wiley and Sons, New York, 1961.

[3] Evansj. P. And Steuer r. E. "Generating Efficient Extreme Points in Linear Multiple Objective Programming: Two Algorithms and Computing Experience" In J. L. Cochrane and M. Zeleny (Eds.).Multiple Criteria Decision Making, University of South Carolina Press. Columbia. SC.. 349-365, 1973.

[4] GAL, T.. "A General Method for Determining the Set of ,all Efficient Solutions to a Linear Vectormaximum Problem." European J. Oper. Res.. I , 307-322, 1977.

[5] Goicoechea, A., Hansen, D. R. and Duckstein, L.. "Multiobjective Decision Analysis with Engineering and Business Applications", Wiley, New York, 1982.

[6] Jacquet-Lagreze, E. and Siskos, J., "Assessing a set of additive utility functions for multicriteria decision-making, the UTA method", EJOR, vol. 10, 151-164, 1982.

[7] Martel, J. M., D' Avignon, G. R. Project ordering with Multicriteria analysis, European Journal of Operational Research, 10, p. 56-69, 1982.

[8] Martel, J. M., D' Avignon, G. R. "A fuzzy outranking relation in multicriteria decision making", European Journal of Operational Research, Volume 25, Issue 2, p. 258-271, 1986.

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

[10] Pareto, V., "Cours d'Économie Politique. Lausanne", F. Rouge, 1896 and 1897. Tome Premier, viii, 430 pp. Tome Second, 426 pp.

[11] Roy, B. "Classement et choix en présence de points de vue multiples (la méthode ELECTRE)". la Revue d'Informatique et de Recherche Opérationelle (RIRO) (8): 57–75., 1968.

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

[13] Saaty, T. L. "The Analytic Hierarchy Process", McGraw-Hill, New York, 1980.

[14] Saaty, T. L. "Decision making with the analytic hierarchy process", Int. J. Service Sciences, Vol. 1, No I, pp. 83-98, 2008.

[15] Siskos, J. "Analyse de systèmes de décision multicritère en univers aléatoire", Foundations of Control Engineering 8, pp. 193-212, 1983.

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

Κεφάλαιο 4ο

4 Συνεργατική Μεθοδολογία Ανάλυσης και Διαχείρισης Επικινδυνότητας (STORM-RM)

4.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται η μεθοδολογία Ανάλυσης και Διαχείρισης Επικινδυνότητας STORM-RM. Αρχικά αποτυπώνονται οι στόχοι της μεθοδολογίας, παρουσιάζονται οι απαιτήσεις οι οποίες πρέπει να καλύπτονται καθώς και τα χαρακτηριστικά της μεθοδολογίας και, στην συνέχεια, περιγράφονται λεπτομερώς οι φάσεις και τα επιμέρους βήματά της.

4.2 Πεδίο εφαρμογής και στόχοι

Στο πεδίο εφαρμογής της μεθοδολογίας STORM-RM περιλαμβάνονται Πληροφοριακά Συστήματα τα οποία υποστηρίζουν τις κρίσιμες η-υπηρεσίες των υπό εξέταση οργανισμών και τις επιχειρησιακές λειτουργίες τους. Το πεδίο εφαρμογής της μεθοδολογίας καλύπτει τον προσδιορισμό των κρίσιμων η-υπηρεσιών, το στάδιο της ανάλυσης επικινδυνότητας και τον προσδιορισμό των κυριότερων κινδύνων, όσο και το στάδιο της διαχείρισης επικινδυνότητας και τον προσδιορισμό των κατάλληλων μέτρων ασφάλειας.

Στόχοι της μεθοδολογίας είναι η κάλυψη των βασικών απαιτήσεων ασφάλειας και η υποστήριξη των φάσεων της ανάλυσης επικινδυνότητας που αναφέρονται παρακάτω:

- ✓ Συμβατότητα με τις απαιτήσεις των διεθνών προτύπων ασφάλειας ΠΣ (ISO 27001:2005 [16] και ISO 27005:2008 [15]).
- ✓ Υποστήριξη της συμμετοχής όλων των χρηστών του ΠΣ του υπό εξέταση οργανισμού στην ανάλυση επικινδυνότητας.
- ✓ Συμβατότητα με τη φύση των κρίσιμων υποδομών και τις απαιτήσεις ασφαλείας τους.
- ✓ Συμβατότητα με τη σχετική νομοθεσία.

4.3 Απαιτήσεις και χαρακτηριστικά της STORM-RM

4.3.1 Απαιτήσεις της STORM-RM

Στην ενότητα αυτή παρουσιάζονται οι απαιτήσεις τις οποίες καλύπτει η προτεινόμενη μεθοδολογία STORM-RM.

Φιλικότητα. Κύριο γνώρισμα της μεθοδολογίας είναι η φιλικότητα και η ευχρηστία. Η STORM-RM έχει τις απαραίτητες προδιαγραφές ώστε να μην απευθύνεται μόνο σε εμπειρογνώμονες, αλλά και σε χρήστες των υπό εξέταση ΠΣ που δεν έχουν την απαραίτητη γνώση και εμπειρία πάνω σε θέματα ασφάλειας. Τα βήματα και τα ερωτηματολόγια που χρησιμοποιεί είναι δημιουργημένα με τέτοιο τρόπο ώστε να επιτυγχάνεται η κατά το δυνατόν πιο φιλική συλλογή της γνώσης και της απαραίτητης πληροφορίας που απαιτούνται από τα στάδια εύρεσης, αποτίμησης και διαχείρισης των επιχειρησιακών, λειτουργικών και τεχνολογικών κινδύνων του οργανισμού.

Προσαρμοστικότητα. Υπάρχει η δυνατότητα ευελιξίας ώστε να μπορεί να έχει εφαρμογή σε διαφορετικού είδους και μεγέθους οργανισμούς (π.χ. κρίσιμες υποδομές, ΜΜΕ) οι οποίοι διαφέρουν τόσο στην πολυπλοκότητα των ΠΣ τους, όσο και στον διαφορετικό βαθμό επίπτωσης από τυχόν απώλεια της ασφάλειας.

Εύκολα υλοποιήσιμη. Πολύ σημαντικό είναι η μεθοδολογία να είναι αλγοριθμική ώστε να είναι εφικτή η υλοποίησής της με χρήση γνωστών γλωσσών προγραμματισμού με τη μορφή ενός αυτοματοποιημένου εργαλείου ανάλυσης και διαχείρισης επικινδυνότητας. Με τον τρόπο αυτό οι χρήστες των ΠΣ θα είναι σε θέση να έχουν ένα πολύτιμο εφόδιο για τον προσδιορισμό, την αποτίμηση και την αντιμετώπιση των καθημερινών κινδύνων που αντιμετωπίζουν τα πληροφοριακά τους συστήματα.

Συμβατότητα με τα Πρότυπα Ασφάλειας. Η STORM-RM καλύπτει τις απαιτήσεις και τις γενικές οδηγίες των προτύπων ασφάλειας ΠΣ. Το κριτήριο αυτό είναι απαραίτητο διότι θα είναι χρήσιμο στους χρήστες της μεθοδολογίες να έχουν την δυνατότητα μέσα από τις φάσεις της να υλοποιούν και να εφαρμόζουν στον οργανισμό τους τις γενικές απαιτήσεις των προτύπων για την σχεδίαση, βελτίωση και επικαιροποίηση ενός Συστήματος Διαχείρισης Ασφάλειας.

Επεκτασιμότητα. Τέλος, μια ακόμη απαίτηση την οποία καλύπτει η προτεινόμενη μεθοδολογία είναι η δυνατότητα επέκτασης, τόσο στον τρόπο των ερωτηματολογίων, όπου δίνεται η δυνατότητα

να προσαρμόζονται στις τρέχουσες επιπτώσεις και απειλές που αντιμετωπίζουν τα διαρκώς εξελισσόμενα ΠΣ, όσο και στη δυνατότητα ενσωμάτωσης νέων αδυναμιών προκειμένου ο προσδιορισμός των κινδύνων να ανταποκρίνεται στην πραγματική εικόνα των υπό εξέταση οργανισμών.

4.3.2 Χαρακτηριστικά της STORM-RM

Στην παρούσα ενότητα παρουσιάζονται τα κύρια χαρακτηριστικά της προτεινόμενης μεθοδολογίας STORM-RM. Συγκεκριμένα, αυτά είναι:

Συνεργατικότητα. Η μεθοδολογία STORM-RM αντιμετωπίζει το πρόβλημα της αποτίμησης επικινδυνότητας ως ένα συνεργατικό πρόβλημα διαφορετικών ομάδων χρηστών με διαφορετικές οπτικές ή/και απαιτήσεις ασφάλειας. Βασικό χαρακτηριστικό της μεθοδολογίας είναι ότι επιτρέπει τη συμμετοχή πολλών κατηγοριών χρηστών του ΠΣ (π.χ. μέλη της διοίκησης, διαχειριστές, μέλη της ομάδας ασφάλειας, τοπικοί χρήστες), στις διάφορες φάσεις της μεθοδολογίας. Σε κάθε φάση της μεθοδολογίας οι απόψεις των χρηστών (της ίδιας ή διαφορετικών κατηγοριών) μπορεί να διαφέρουν, ανάλογα με την οπτική του καθενός (επιχειρησιακή, τεχνολογική, νομική κτλ.). Επιπρόσθετο χαρακτηριστικό της μεθοδολογίας είναι ότι η συμμετοχή των χρηστών σταθμίζεται με σαφώς καθορισμένο τρόπο σε κάθε στάδιο, ώστε να πραγματοποιείται ο κατανεμημένος υπολογισμός της επικινδυνότητας.

Προσανατολισμένη προς τους χρήστες του υπό εξέταση ΠΣ. Σε αντίθεση με την πλειονότητα των υπαρχουσών μεθοδολογιών ανάλυσης επικινδυνότητας, οι οποίες είναι καθοδηγούμενες από ειδικούς (αναλυτές επικινδυνότητας, εμπειρογνώμονες), στόχος της μεθοδολογίας STORM-RM είναι η καθοδήγηση από τους ίδιους τους χρήστες του ΠΣ. Η συμμετοχή των χρηστών στην ανάλυση της επικινδυνότητας αυξάνει την κατανόηση των χρηστών και τους ευαισθητοποιεί στο θέμα της ασφάλειας, γεγονός που βελτιώνει την μετέπειτα διαδικασία εφαρμογής των μέτρων προστασίας από τους χρήστες.

Ελάττωση πολυπλοκότητας. Η συμμετοχή πολλών χρηστών με διαφορετικές θεωρήσεις ως προς τις απαιτήσεις ασφάλειας του ΠΣ αυξάνει εγγενώς την πολυπλοκότητα. Επειδή δεν είναι ρεαλιστικό να υποθέσουμε ότι οι διάφοροι χρήστες θα είναι σε θέση να κατανοήσουν όλα τα βήματα της μεθοδολογίας, βασικό χαρακτηριστικό της STORM-RM είναι η ελάττωση της πολυπλοκότητας κατά τη συμμετοχή των χρηστών. Για το λόγο αυτό, η συμμετοχή κάθε ομάδας χρηστών περιορίζεται μόνο σε εκείνες τις φάσεις τις οποίες μπορούν να κατανοήσουν και, συνεπώς, η συμμετοχή τους

είναι περισσότερο ωφέλιμη. Επιπλέον, για την ελάττωση της πολυπλοκότητας η εκτέλεση των σύνθετων διαδικασιών είναι διαφανής προς τους τελικούς χρήστες, δηλαδή, όπως απαιτείται από τα σύγχρονα πρότυπα ανάλυσης επικινδυνότητας, δεν απαιτεί από τους χρήστες πλήρη κατανόηση της συλλογιστικής, αλλά μόνο των στόχων της ανάλυσης και των τελικών αποτελεσμάτων.

Ανθεκτικότητα σε σφάλματα. Όπως αναφέρθηκε προηγουμένως, οι απόψεις των συμμετεχόντων χρηστών σε κάθε φάση της μεθοδολογίας μπορεί να αποκλίνουν. Η μεθοδολογία STORM-RM έχει μεγάλη ανθεκτικότητα σε σφάλματα για τους ακόλουθους λόγους. Πρώτον, η συμμετοχή των χρηστών σταθμίζεται κατάλληλα με τη χρήση του αλγορίθμου της πολυκριτηριακής μεθόδου AHP, ανάλογα με την ομάδα που ανήκει ο κάθε χρήστης, στις διάφορες φάσεις της μεθοδολογίας. Δεύτερον, ο συνδυασμός της γνώσης, ο οποίος πηγάζει από τη διαφορετική αντίληψη που πιθανώς έχουν διαφορετικοί χρήστες ανάλογα με το ρόλο τους σε κάθε επιχειρησιακή λειτουργία, μπορεί να οδηγήσει στην εξόρυξη γνώσης που δεν είναι προφανής από μία απλή συλλογή δεδομένων. Και τρίτον, εκτιμάται ότι η πλειονότητα των χρηστών θα έχει ορθή άποψη για το αγαθό το οποίο χρησιμοποιεί από τη δική του οπτική για την επιχειρησιακή αξία του συγκεκριμένου αγαθού. Συνεπώς, η μεθοδολογία STORM-RM λαμβάνει υπόψη της όλες τις παραπάνω παραμέτρους και μέσω της συμμετοχής πολλών διαφορετικών χρηστών μπορεί να διορθώσει «εσφαλμένα» δεδομένα εισόδου, τα οποία για τους λόγους που αναλύθηκαν παραπάνω είναι πολύ σπάνια.

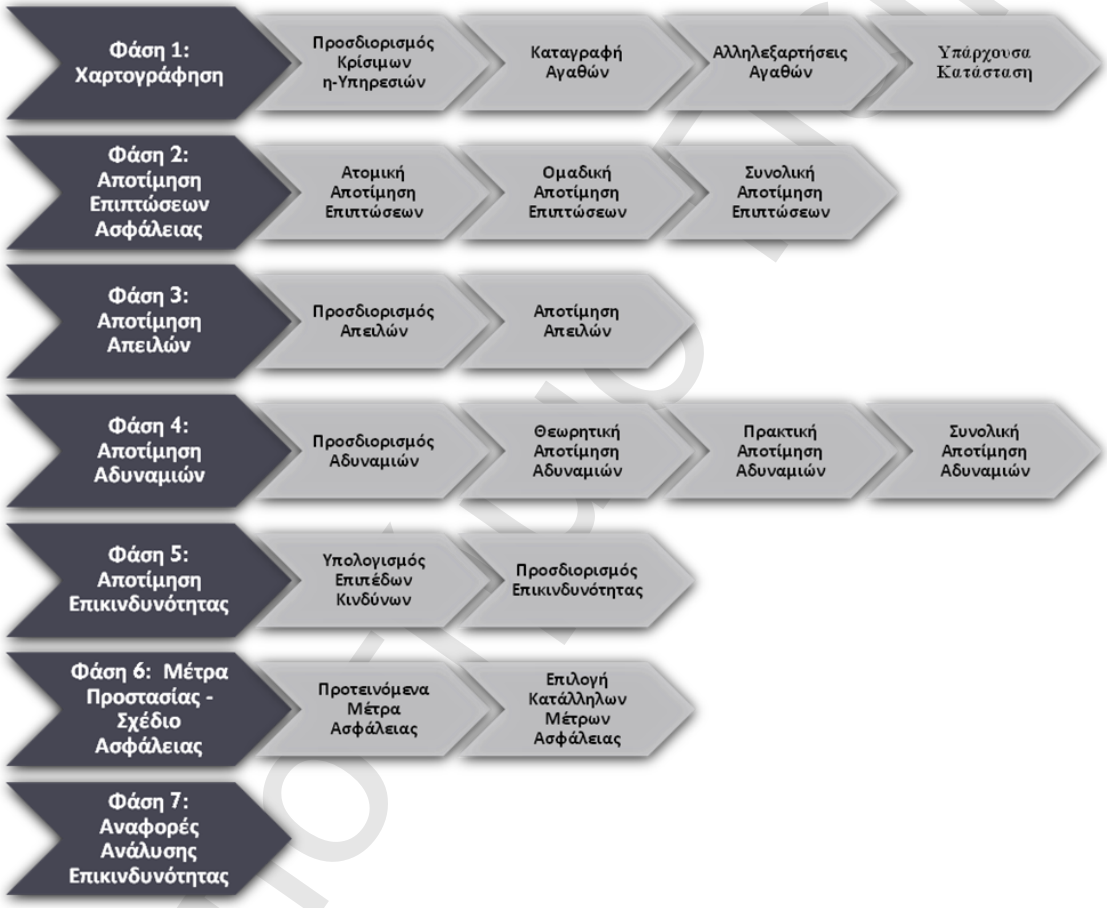
Αλγοριθμική. Επειδή η μεθοδολογία είναι αλγοριθμική είναι πολύ εύκολο να υλοποιηθεί και να ενσωματωθεί σε ένα εργαλείο ανάλυσης και διαχείρισης επικινδυνότητας με χρήση κάποιας από τις γνωστές γλώσσες προγραμματισμού.

Επεκτασιμότητα και προσαρμοστικότητα. Τέλος, η προτεινόμενη μεθοδολογία, επιτρέπει την επεκτασιμότητα σε όλες τις φάσεις και τα βήματά της. Πιο συγκεκριμένα, ο τρόπος με τον οποίο λαμβάνει υπόψη της τις γνώμες των χρηστών μπορεί να παραμετροποιηθεί ανάλογα με τις ανάγκες του υπό εξέταση ΠΣ. Δηλαδή μπορεί να υποστηρίξει από έναν χρήστη μέχρι όσους κριθεί αναγκαίο και ταυτόχρονα τα βάρη συμμετοχής μπορούν να ποικίλουν. Το γεγονός αυτό επιτρέπει στην μεθοδολογία να έχει εφαρμογή σε διαφορετικής φύσης ΠΣ, όπως σε κρίσιμες υποδομές, πολύπλοκους οργανισμούς με πολλούς χρήστες (εσωτερικούς ή εξωτερικούς) και πολύπλοκη τηλεπικοινωνιακή υποδομή καθώς και σε ΠΣ μικρών και μικρομεσαίων επιχειρήσεων (ΜΜΕ) όπου οι χρήστες είναι λίγοι και τα ΠΣ είναι μικρής πολυπλοκότητας.

4.4 Αναλυτική περιγραφή της μεθοδολογίας STORM-RM

Με βάση τις γενικές οδηγίες του προτύπου AS/NZS 4360 [1] και κάνοντας χρήση της πολυκριτηριακής μεθοδολογίας AHP, Analytic Hierarchy Process, [26][27], προτείνεται στην ενότητα αυτή η μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας STORM-RM [19][20].

Οι βασικές Φάσεις της μεθοδολογίας είναι επτά (7) με την κάθε μία να υλοποιείται από επιμέρους βήματα (Εικόνα 5).



Εικόνα 5: Φάσεις Μεθοδολογίας STORM-RM

Όλες οι φάσεις και τα βήματα της μεθοδολογίας περιγράφονται αναλυτικά στις ενότητες που ακολουθούν.

4.4.1 Φάση 1: Χαρτογράφηση

Με στόχο την απλοποίηση των βημάτων της Χαρτογράφησης αλλά και την μείωση της πολυπλοκότητας, ειδικά στις περιπτώσεις πολύπλοκων, κατανεμημένων ΠΣ, η Φάση της

Χαρτογράφησης πραγματοποιείται με τον τρόπο που περιγράφεται παρακάτω και απεικονίζεται στην Εικόνα 6.

Εικόνα 6: Βασικά Βήματα της Φάσης Χαρτογράφησης

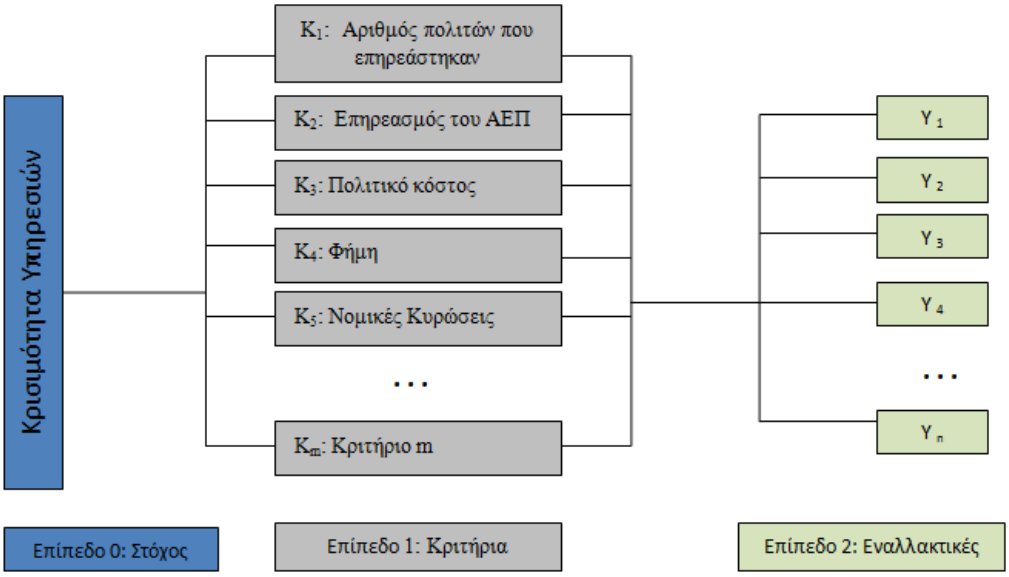
Ο *Νόμιμος Εκπρόσωπος (Legal Representative)* του οργανισμού, προσδιορίζει τις κρίσιμες ηλεκτρονικές υπηρεσίες του οργανισμού του για τις οποίες θα πραγματοποιηθεί η ανάλυση Επικινδυνότητας. Ο *Νόμιμος Εκπρόσωπος* είναι η ανώτατη διοίκηση του οργανισμού ή οποιοσδήποτε έχει λάβει αυτή την εξουσιοδότηση από την ανώτατη διοίκηση του οργανισμού. Στην συνέχεια, καταγράφει όλους τους απαραίτητους χρήστες και τους αναθέτει έναν από τους ρόλους του μοντέλου ομάδων χρηστών (όπως αναλύεται σε επόμενο υποκεφάλαιο και εμφανίζεται στην Εικόνα 8), ανάλογα με την θέση τους στον οργανισμό και την σχετική τους ειδικότητα και εμπειρία. Στην συνέχεια, οι χρήστες της ομάδας *Διοίκησης* είναι υπεύθυνοι για την καταγραφή των χρηστών του οργανισμού που εμπλέκονται στις υπηρεσίες, δηλαδή ο διοικητικός υπεύθυνος κάθε τομέα ευθύνης θα καταγράψει τους *Τελικούς Χρήστες* και τους *Διαχειριστές Συστημάτων* που εμπλέκονται στην παροχή των υπηρεσιών του συγκεκριμένου τομέα ευθύνης. Στη συνέχεια, οι χρήστες της ομάδας *Τελικοί Χρήστες* (End users) που έχουν προσδιοριστεί στο προηγούμενο βήμα πραγματοποιούν την καταγραφή των δεδομένων που σχετίζονται με τις η-υπηρεσίες. Τέλος, οι χρήστες της ομάδας *Διαχειριστές* καταγράφουν όλες τις απαραίτητες πληροφορίες σε ό,τι αφορά στα αγαθά Υλικού και Λογισμικού.

Βασική απαίτηση για τη διευκόλυνση της χαρτογράφησης είναι η μοντελοποίηση των επιχειρησιακών διαδικασιών του οργανισμού, η οποία και περιγράφεται παρακάτω. Στη συνέχεια, αναλύεται το βήμα της χαρτογράφησης, το οποίο αποτελείται από τέσσερα (4) βασικά βήματα που περιγράφονται στις παραγράφους που ακολουθούν.

4.4.1.1 Βήμα 1.1: Προσδιορισμός κρίσιμων η-υπηρεσιών

Στόχος του συγκεκριμένου βήματος είναι να προσδιοριστούν οι κρίσιμες για τον οργανισμό η-υπηρεσίες. Για τον σκοπό αυτό η μεθοδολογία χρησιμοποιεί ένα δένδρο απόφασης AHP (Εικόνα 7) όπου ο Νόμιμος Εκπρόσωπος του υπό εξέταση οργανισμού είναι σε θέση να αξιολογήσει τις η-υπηρεσίες σύμφωνα με διάφορα κριτήρια, δίνοντας έμφαση στα κριτήρια κρισιμότητας η-υπηρεσιών που προτείνει η Ευρωπαϊκή Ένωση [9]:

- ✓ Εθνικά / Κοινωνικά Κριτήρια:
  - Αριθμός πολιτών που επηρεάστηκαν
  - Επηρεασμός του ΑΕΠ
  - Απώλεια ανθρώπινης ζωής
  - Κοινωνικές διαταραχές
  - Εθνική ασφάλεια
  - Εμπορική στασιμότητα
  - Πολιτικό κόστος
  - Εμπιστοσύνη στην κυβέρνηση
  - Υποβάθμιση προϊόντων και υπηρεσιών
- ✓ Επιχειρηματικά Κριτήρια:
  - Κέρδος
  - Πωλήσεις
  - Ανταγωνιστικότητα
  - Φήμη
  - Νομικές κυρώσεις
  - Οικονομική επίπτωση
- ✓ Έκταση: Η απώλεια μιας συνιστώσας μια κρίσιμης υποδομής αξιολογείται με βάση τη γεωγραφική εμβέλεια των επιπτώσεών της (πχ. διεθνής, εθνική, περιφερειακή, τοπική)
- ✓ Επίδραση του χρόνου: Αφορά σε εκείνο το χρονικό σημείο της απώλειας μιας συνιστώσας, οπότε θα υπήρχε σημαντική επίδραση (πχ. άμεσα, μέσα στο επόμενο 24ωρο, σε μια εβδομάδα κτλ.)



Εικόνα 7: Δένδρο απόφασης AHP για την κρισιμότητα των η-υπηρεσιών

Με τη βοήθεια του δένδρου απόφασης της AHP, κατηγοριοποιούνται ως προς την κρισιμότητά τους οι υπηρεσίες του οργανισμού και προκύπτει μια ιεραρχημένη λίστα με τις πιο κρίσιμες η-υπηρεσίες για τις οποίες θα γίνει η μελέτη επικινδυνότητας στα επόμενα βήματα της μεθοδολογίας.

Σε περίπτωση που ο Νόμιμος Εκπρόσωπος του υπό εξέταση οργανισμού γνωρίζει εκ των προτέρων ποιες είναι οι κρίσιμες υπηρεσίες του οργανισμού του, υπάρχει η δυνατότητα παράκαμψης του δένδρου απόφασης και μπορεί να καταγράψει απευθείας τις κρίσιμες η-υπηρεσίες στην ιεραρχημένη λίστα.

4.4.1.1.1 Μοντελοποίηση Επιχειρησιακών Διαδικασιών των κρίσιμων η-υπηρεσιών

Αφού ολοκληρωθεί ο προσδιορισμός των κρίσιμων η-υπηρεσιών, η μεθοδολογία STORM-RM προτείνει την μοντελοποίηση των επιχειρησιακών διαδικασιών, η οποία αφορά στην διαδικασία αποτύπωσης και αναπαράστασης αυτών των η-υπηρεσιών.

Η αναπαράσταση των η-υπηρεσιών γίνεται με τη χρήση του προτύπου ερωτηματολογίων (Παράρτημα IV). Τα μέλη της Διοίκησης (συγκεκριμένα ο προϊστάμενος κάθε η-υπηρεσίας) καταγραφούν τα βήματα υλοποίησης, τους εμπλεκόμενους χρήστες και τα έγγραφα των κρίσιμων η-υπηρεσιών. Στη συνέχεια, χρησιμοποιούν κλασικές τεχνικές για την παραγωγή μοντέλων επιχειρησιακών διαδικασιών, χρησιμοποιώντας διαγράμματα ροής, διαγράμματα ελέγχου ροής, διαγράμματα Gantt, διαγράμματα PERT κ.α.. Οι σύγχρονες τεχνικές και μέθοδοι κάνουν χρήση της

περιγραφικής γλώσσας UML (Unified Modeling Language) [30][23] και της περιγραφικής γλώσσας και συμβολισμού BPMN (Business Process Modeling Notation) [3]. Οι σύγχρονες τεχνικές καλύπτουν μεγαλύτερο εύρος επιχειρησιακών διαδικασιών, με συμβολισμούς και παραδοχές για την διαλειτουργικότητα μεταξύ των διαφόρων σταδίων των καταγραφόμενων δραστηριοτήτων και μεταξύ των δραστηριοτήτων του ίδιου του οργανισμού. Αυτό έχει ως αποτέλεσμα την κάλυψη των απαιτήσεων μοντελοποίησης πολύπλοκων διαδικασιών. Οι χρήστες της μεθοδολογίας θα ορίσουν τους συγκεκριμένους συμβολισμούς που θα χρησιμοποιηθούν για την απεικόνιση των STORM-RM επιχειρησιακών διαδικασιών.

4.4.1.2 Βήμα 1.2: Καταγραφή αγαθών

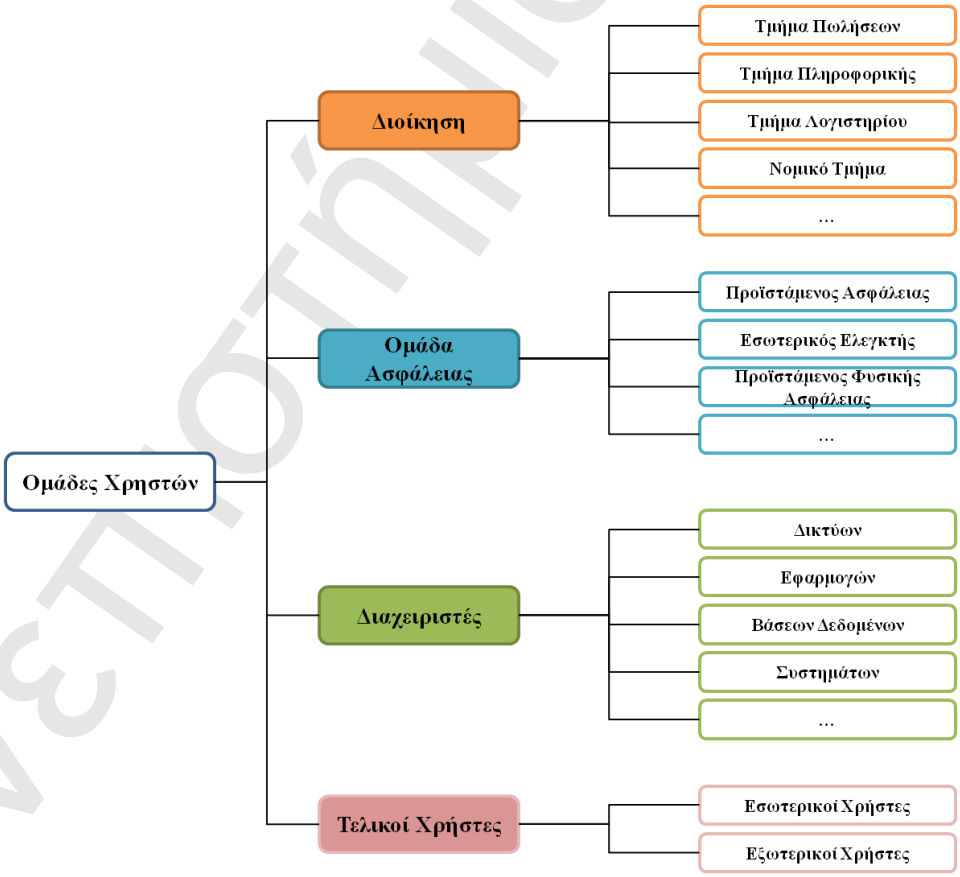
Στο συγκεκριμένο βήμα γίνεται η αναλυτική καταγραφή όλων των αγαθών του υπό εξέταση ΠΣ τα οποία σχετίζονται με τις κρίσιμες η-υπηρεσίες, όπως προέκυψαν από το προηγούμενο Βήμα. Η μεθοδολογία STORM-RM κατηγοριοποιεί τα αγαθά του υπό εξέταση ΠΣ στις παρακάτω βασικές ομάδες:

- ✓ **Υπηρεσίες (Services):** Καταγραφή όλων των κρίσιμων η-υπηρεσιών του υπό εξέταση ΠΣ.
- ✓ **Χρήστες (Users):** Για την καταγραφή των χρηστών προτείνονται τέσσερις (4) βασικές ομάδες: Διοίκηση (Management), Ομάδα ασφάλειας (Security Team), Διαχειριστές (Technical Experts) και Τελικοί Χρήστες (End users).
- ✓ **Φυσικά αγαθά (Physical Assets).** Ως φυσικά αγαθά θα καταγραφούν όλοι οι χώροι όπου στεγάζεται το ΠΣ του οργανισμού όπως δωμάτια, κτίρια κλπ.
- ✓ **Υλικά αγαθά (Hardware).** Καταγραφή όλων των υλικών αγαθών που συνδέονται με τις κρίσιμες η-υπηρεσίες, σύμφωνα με την παρακάτω κατηγοριοποίηση:
    - Υπολογιστής εξυπηρετητής (Server Computer)
    - Σταθμός εργασίας (Client Computer)
    - Δικτυακή πύλη (Gateway)
    - Δρομολογητής (Router)
    - Μεταγωγέας (Switch)
    - Μέσο αποθήκευσης (External Storage Equipment)
    - Εκτυπωτής (Printer)
    - Άλλο
- ✓ **Λογισμικό (Software).** Καταγραφή όλων των εφαρμογών που συνδέονται με τις κρίσιμες η-υπηρεσίες (που έχουν προσδιοριστεί στο Βήμα 1.1) σύμφωνα με την παρακάτω κατηγοριοποίηση:

- Λειτουργικό σύστημα (Operating System)
- Ανεξάρτητη εφαρμογή (stand-alone Application)
- Εφαρμογή πελάτη (Client Application)
- Λογισμικό διαχείρισης βάσης δεδομένων (Database SW)
- Λογισμικό παροχής ιστοσελίδων (Web Server SW)
- Λογισμικό υποστήριξης εφαρμογών (Application Server SW)
- Ενσωματωμένο λογισμικό (Embedded SW)
- Λογισμικό υποστήριξης δικτύωσης (Network SW)
- Άλλο

✓ **Δεδομένα (Data).** Καταγραφή όλων των δεδομένων-πληροφοριών που επεξεργάζεται το ΠΣ του υπό εξέταση οργανισμού.

Η πρώτη ομάδα αγαθών που πρέπει να καταγραφεί είναι η ομάδα των χρηστών, ώστε να δημιουργηθεί το απαραίτητο μοντέλο με τις ομάδες χρηστών (Εικόνα 8) που θα συμμετέχουν στην όλη διαδικασία της Ανάλυσης Επικινδυνότητας [20].

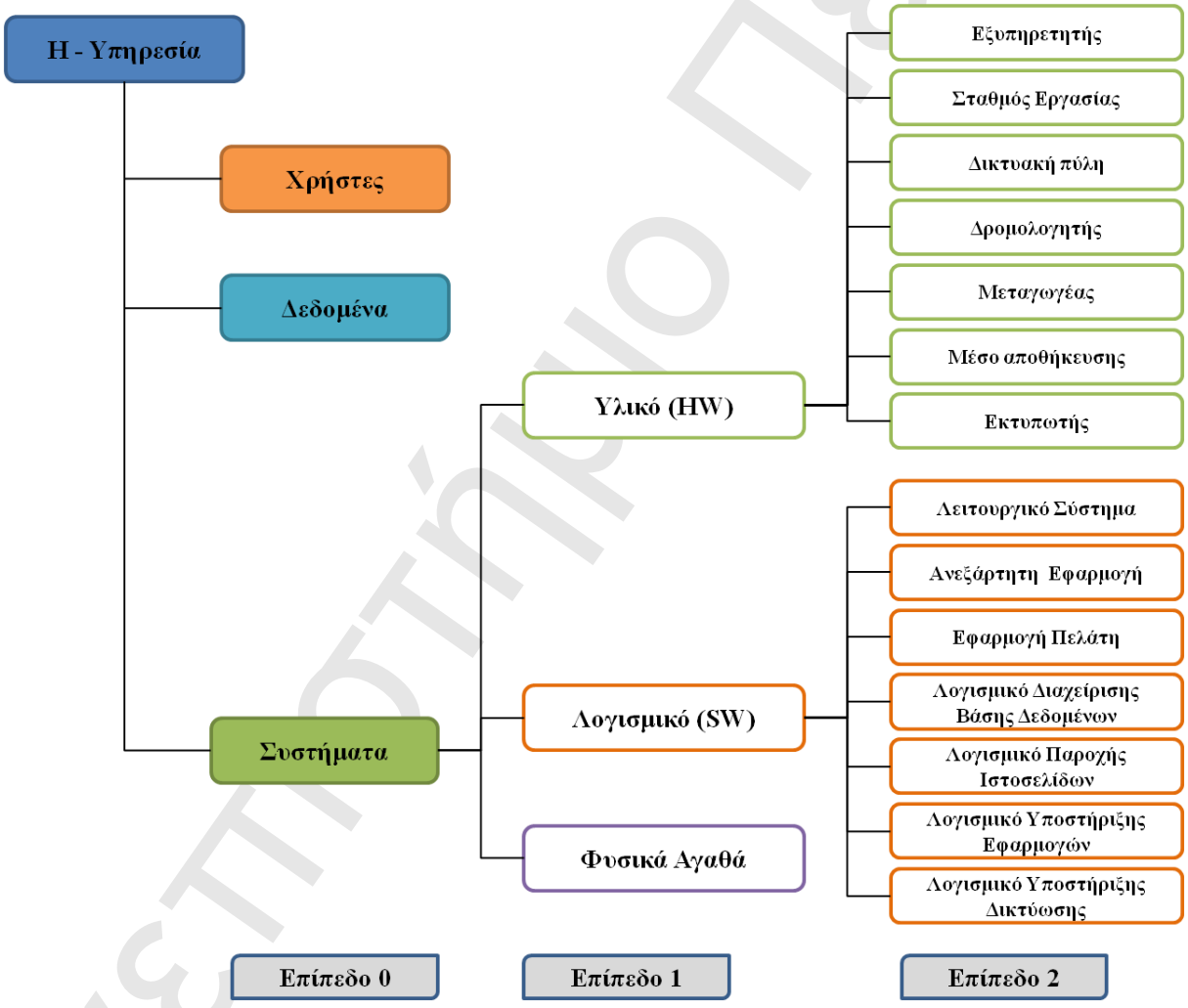


Εικόνα 8: Μοντέλο Ομάδων χρηστών (User Group Model)

Οι προτεινόμενες ομάδες χρηστών (οι οποίες προσαρμόζονται ανάλογα με την δομή του υπό εξέταση οργανισμού) χρησιμοποιούνται τόσο για την δημιουργία των αλληλεξαρτήσεων των αγαθών του υπό εξέταση ΠΣ όσο και για την εμπλοκή των διαφορετικών χρηστών στα επόμενα βήματα της μεθοδολογίας.

4.4.1.3 Βήμα 1.3: Αλληλεξαρτήσεις αγαθών

Σε αυτό το Βήμα πραγματοποιούνται οι αλληλεξαρτήσεις των αγαθών. Για την καταγραφή των αλληλεξαρτήσεων των αγαθών του υπό εξέταση ΠΣ χρησιμοποιείται το δένδρο της Εικόνας 9.



Εικόνα 9: Δένδρο αλληλεξαρτήσεων (Asset Group Model)

Σύμφωνα με το *Δένδρο Αλληλεξαρτήσεων* που χρησιμοποιεί η μεθοδολογία STORM-RM, η κύρια οντότητα είναι η *η-υπηρεσία* πάνω στην οποία συνδέονται τα υπόλοιπα αγαθά. Για την καλύτερη αποτύπωση των αλληλεξαρτήσεων αλλά και για την απλοποίηση και τη μείωση του αριθμού των

ερωτηματολογίων αποτίμησης επικινδυνότητας η μεθοδολογία STORM-RM ομαδοποιεί τα αγαθά *Υλικού, Λογισμικού* και *Φυσικά* με την οντότητα *Συστήματα.* Ένα *Σύστημα* μπορεί να είναι είτε ένα Υπολογιστικό Σύστημα είτε ένα Δίκτυο (π.χ. Εσωτερικό Δίκτυο – LAN, Ασύρματο Δίκτυο – WLAN, κλπ). Με αυτόν τον τρόπο δημιουργείται ένα δένδρο αλληλεξαρτήσεων για κάθε η-υπηρεσία το οποίο περιλαμβάνει:

- ✓ τους *Χρήστες* της υπηρεσίας, οι οποίοι κατηγοριοποιούνται σύμφωνα με το Μοντέλο Ομάδων Χρηστών (Εικόνα 8),
- ✓ τα *Δεδομένα* που χρησιμοποιεί η συγκεκριμένη η-υπηρεσία, τα οποία μπορεί να είναι είτε δεδομένα εισόδου είτε δεδομένα εξόδου, και
- ✓ τα *Συστήματα* τα οποία εμπλέκονται για την παροχή της συγκεκριμένη η-υπηρεσίας και τα οποία αποτελούνται από Υλικό, Λογισμικό και βρίσκονται σε κάποια φυσική τοποθεσία (Φυσικά Αγαθά).

4.4.1.4 Βήμα 1.4: Υπάρχοντα μέτρα προστασίας / διαδικασίες ασφάλειας

Στο βήμα αυτό καταγράφονται όλα τα υφιστάμενα μέτρα προστασίας του υπό εξέταση ΠΣ. Για κάθε ένα αγαθό γίνεται ο έλεγχος με βάση τα μέτρα που ορίζει το ISO 27001 (Παράρτημα ΙΙ). Τα μέτρα χαρακτηρίζονται σαν *Πλήρως Εγκατεστημένα, Μερικώς Εγκατεστημένα* και *Μη Εγκατεστημένα*. Τα αποτελέσματα του συγκεκριμένου βήματος θα χρησιμοποιηθούν στο *Βήμα 4.1* για την Ανάλυση Αδυναμιών καθώς και στο *Βήμα 6.1* όπου η μεθοδολογία προτείνει τα κατάλληλα μέτρα προστασίας.

4.4.2 Φάση 2: Αποτίμηση Επιπτώσεων Ασφάλειας

Στην συγκεκριμένη φάση της μεθοδολογίας, γίνεται η αποτίμηση του κάθε αγαθού σε περίπτωση απώλειας της *Διαθεσιμότητας*, της *Εμπιστευτικότητας* ή της *Ακεραιότητάς* τους. Για κάθε αγαθό θα προσμετρείται η άποψη των χρηστών που χρησιμοποιούν τα αγαθά αυτά, λαμβάνοντας υπόψη τα βάρη της ομάδας στην οποία ανήκουν (Εικόνα 8: Μοντέλο Ομάδων χρηστών (User Group Model)).

4.4.2.1 Κατηγορίες επιπτώσεων

Με στόχο να καλυφθούν όσο το δυνατόν περισσότερες επιπτώσεις (consequences) από την απώλεια της ασφάλειας (διαθεσιμότητας, εμπιστευτικότητας, ακεραιότητας) των αγαθών του ΠΣ του υπό εξέταση οργανισμού, αλλά και για να γίνει πιο εύκολο για τους χρήστες που συμμετέχουν στην

αποτίμηση των αγαθών να κατανοήσουν τις ενδεχόμενες επιπτώσεις, προτείνονται οι εξής κατηγορίες επιπτώσεων:

- ✓ Επιπτώσεις σε Εθνικό Επίπεδο
  - Επιπτώσεις στην άμυνα και την εθνική ασφάλεια
  - Επιπτώσεις στις διεθνείς σχέσεις
  - Επιπτώσεις στην εθνική οικονομία
  - Πληθυσμός (αριθμός χρηστών) που επηρεάζεται
  - Άμυνα και εθνική ασφάλεια
  - Διατάραξη της δημόσιας τάξης
- ✓ Ασφάλεια Προσωπικού και Κοινού
  - Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων
- ✓ Παρεμπόδιση Επιχειρηματικών Διαδικασιών του Οργανισμού
  - Παρεμπόδιση των λειτουργιών του οργανισμού
  - Παρεμπόδιση εμπορικών δραστηριοτήτων
  - Κόστος (σε ανθρωποώρες) για την ανάκαμψη των λειτουργιών
  - Επιπτώσεις στην ακεραιότητα όλων των άυλων οντοτήτων (π.χ. εμπορευμάτων)
- ✓ Παρεμπόδιση Επιχειρηματικών Δραστηριοτήτων άλλων Οργανισμών
  - Αλληλεξάρτηση λειτουργιών και δραστηριοτήτων άλλων οργανισμών
  - Παρεμπόδιση εμπορικών δραστηριοτήτων άλλων οργανισμών
  - Αλληλεξάρτηση κρίσιμων υποδομών
- ✓ Οικονομικές Απώλειες
  - Άμεσες οικονομικές συνέπειες
  - Έμμεσες / μακροπρόθεσμες οικονομικές συνέπειες
- ✓ Νομικές Επιπτώσεις
  - Παραβίαση της ιδιωτικότητας
  - Αποκάλυψη ευαίσθητων προσωπικών δεδομένων
  - Αποκάλυψη εμπορικών δεδομένων
  - Παρεμπόδιση ανταγωνισμού
  - Παρεμπόδιση της δικαιοσύνης
  - Παραβίαση ιδιωτικών συμφωνητικών
  - Παραβίαση συμφωνητικών μη αποκάλυψης
  - Παραβίαση νομοθεσίας περί πνευματικής ιδιοκτησίας
  - Παρεμπόδιση εφαρμογής της δικαιοσύνης και της εξιχνίασης παρανομιών

- ✓ Δυσφήμηση της Δημόσιας Εικόνας
  - Απώλεια της εμπιστοσύνης του κοινού στον οργανισμό
  - Απώλεια της εμπιστοσύνης των προμηθευτών ή / και των μετόχων στον οργανισμό

Με βάση τις παραπάνω κατηγορίες επιπτώσεων που προτείνει η μεθοδολογία STORM-RM πραγματοποιείται η αποτίμηση των επιπτώσεων των αγαθών στα επόμενα βήματα της συγκεκριμένης φάσης.

4.4.2.2 Κλίμακα επιπτώσεων

Η κλίμακα την οποία χρησιμοποιεί η μεθοδολογία STORM-RM για την αποτίμηση των επιπτώσεων βασίζεται στο πρότυπο AS/NZS 4360 [1] και φαίνεται στον Πίνακα 14.

Πίνακας 14: Κλίμακα Αποτίμησης Επιπτώσεων

Επίπεδο Επίπτωσης	Βαθμός	Περιγραφή	Οικονομική Απώλεια	Απώλεια Κύκλου Εργασιών
Πολύ Υψηλό (ΠΥ)	5	Καταστροφική Επίπτωση	> 10.000.000 €	100% του κύκλου εργασιών
Υψηλό (Υ)	4	Σημαντική Επίπτωση	έως 10.000.000 €	75% του κύκλου εργασιών
Μέτριο (Μ)	3	Μέτρια Επίπτωση	έως 1.000.000 €	50% του κύκλου εργασιών
Χαμηλό (Χ)	2	Χαμηλή Επίπτωση	έως 100.000 €	25% του κύκλου εργασιών
Πολύ Χαμηλό (ΠΧ)	1	Ασήμαντη Επίπτωση	έως 10.000 €	5% του κύκλου εργασιών

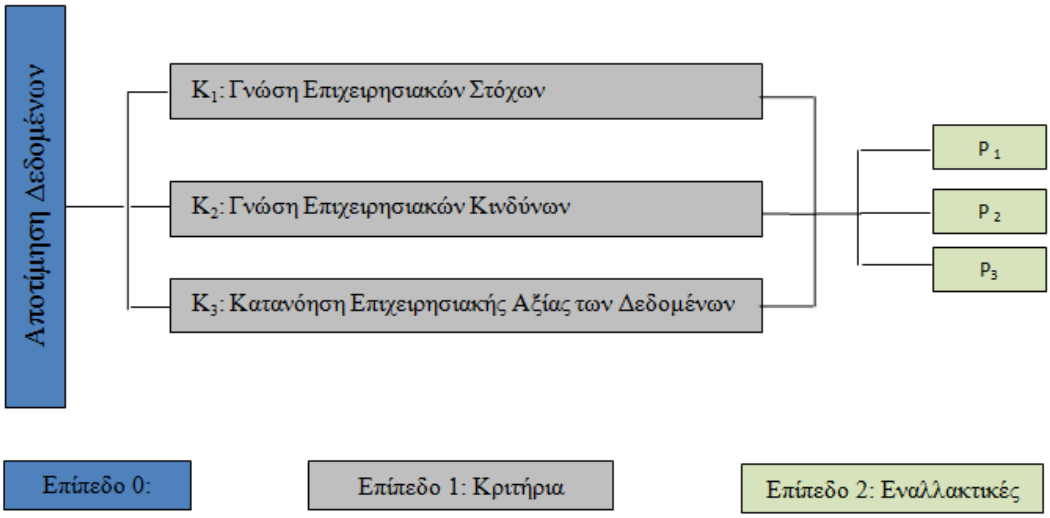
Σύμφωνα με την συγκεκριμένη κλίμακα αποτίμησης επιπτώσεων, μπορεί να γίνει η αποτίμηση των επιπτώσεων απώλειας της ασφάλειας (διαθεσιμότητας, εμπιστευτικότητας, ακεραιότητας) των αγαθών ενός ΠΣ τόσο με ποιοτική όσο και με ποσοτική κλίμακα. Με τον τρόπο αυτό μπορεί να γίνει εύκολα αντιληπτό στους χρήστες (που καλούνται να αποτιμήσουν τα αγαθά του οργανισμού τους) ποιο είναι το μέγεθος της επίπτωσης, εκφράζοντάς το είτε σε οικονομική κλίμακα είτε σε ποσοστό απώλειας του κύκλου εργασιών του οργανισμού τους. Με τον τρόπο αυτό, είναι εύκολο να καλυφθεί το μέγεθος της επίπτωσης σε διαφορετικής φύσης οργανισμούς (π.χ. πολύπλοκοι οργανισμοί, ΜΜΕ) όπου οι οικονομικές απώλειες διαφέρουν. Με βάση λοιπόν την κλίμακα αυτή γίνεται η αποτίμηση των αγαθών στα βήματα που ακολουθούν.

4.4.2.3 Βήμα 2.1: Ατομική αποτίμηση

Στο βήμα αυτό κάθε χρήστης καλείται να εκτελέσει την αποτίμηση των αγαθών με βάση την επίπτωση που θα είχε η απώλεια του αγαθού για την ομαλή λειτουργία του οργανισμού. Για την μείωση της πολυπλοκότητας, η μεθοδολογία STORM-RM εμπλέκει διαφορετικές ομάδες χρηστών

για την αποτίμηση των διαφορετικών ομάδων αγαθών (υλικό, λογισμικό, δεδομένα). Κάθε χρήστης είναι σε θέση να αποτιμήσει το κάθε αγαθό (για όποιο είναι υπεύθυνος ή χειρίζεται) από την δική του θεώρηση και εμπειρία, και η ατομική αποτίμηση σε συνδυασμό με το βάρος της ομάδας που ανήκει λαμβάνεται υπόψη για τον υπολογισμό της τελικής ομαδικής αποτίμησης του αγαθού. Για το σκοπό αυτό, με την βοήθεια της μεθοδολογίας AHP, έχουν δημιουργηθεί βάρη w_k , k=1,..., m, για τις εκτιμήσεις των ομάδων χρηστών, διαφορετικά για κάθε κατηγορία αγαθού.

Για παράδειγμα για την αποτίμηση των **Δεδομένων** εμπλέκονται οι χρήστες των ομάδων *P_1: Διοίκηση*, *P_2: Διαχειριστές* και *P_3: Τελικοί Χρήστες*. Για τον υπολογισμό των βαρών συμμετοχής στην διαδικασία αποτίμησης χρησιμοποιείται το δένδρο απόφασης της AHP (Εικόνα 10), όπου τα κριτήρια είναι τα *K_1: Γνώση Επιχειρησιακών Στόχων*, *K_2: Γνώση Επιχειρησιακών Κινδύνων* και *K_3: Κατανόηση Επιχειρησιακής Αξίας των Δεδομένων*.



Εικόνα 10: Δένδρο Απόφασης για τον υπολογισμό των βαρών συμμετοχής στην αποτίμηση Δεδομένων

Σύμφωνα λοιπόν με το παραπάνω δένδρο απόφασης γίνονται οι ανά δύο συγκρίσεις ως προς τα προτεινόμενα κριτήρια. Οι πίνακες 15, 16 και 17 παρουσιάζουν τις ανά δύο συγκρίσεις, ενώ σημειώνεται ότι οι συγκρίσεις αυτές καθώς και τα τελικά αποτελέσματα (Πίνακας 18) με τα βάρη των συμμετεχόντων ομάδων είναι ενδεικτικές και μπορούν να προσαρμοστούν στις ανάγκες του υπό εξέταση οργανισμού.

Πίνακας 15: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Επιχειρησιακών Στόχων

K_1: Γνώση Επιχειρησιακών Στόχων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1: Διοίκηση	1	3	3	0,600
P_2: Διαχειριστές	1/3	1	1	0,200
P_3: Τελικοί Χρήστες	1/3	1	1	0,200
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Πίνακας 16: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Επιχειρησιακών Κινδύνων

K_2: Γνώση Επιχειρησιακών Κινδύνων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1: Διοίκηση	1	3	7	0,685
P_2: Διαχειριστές	1/3	1	1	0,179
P_3: Τελικοί Χρήστες	1/7	1	1	0,136
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

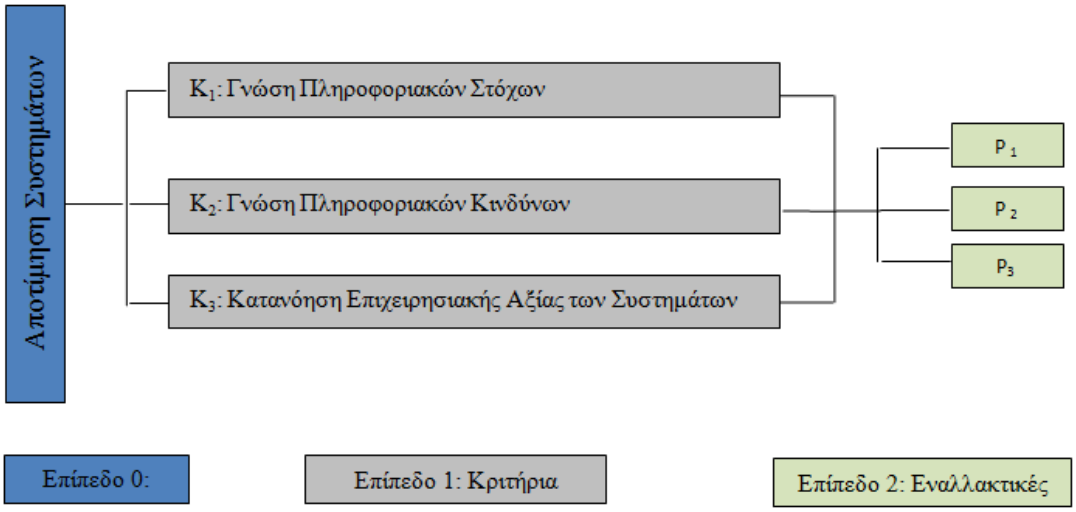
Πίνακας 17: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κατανόηση Επιχειρησιακής Αξίας των Δεδομένων

K_3: Κατανόηση Επιχειρησιακής Αξίας των Δεδομένων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1: Διοίκηση	1	3	3	0,574
P_2: Διαχειριστές	1/3	1	3	0,286
P_3: Τελικοί Χρήστες	1/3	1/3	1	0,140
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Πίνακας 18: Βάρη συμμετοχής στην αποτίμηση των Δεδομένων

Κριτήρια	**K_1**	**K_2**	**K_3**	
Προτεραιότητες Κριτηρίων	**0,333**	**0,333**	**0,333**	**Βάρη (w_i)**
P_1: Διοίκηση	0,600	0,685	0,574	0,620
P_2: Διαχειριστές	0,200	0,179	0,286	0,222
P_3: Τελικοί Χρήστες	0,200	0,136	0,140	0,159
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Για την αποτίμηση των **Συστημάτων** εμπλέκονται οι χρήστες των ομάδων *P_1: Διαχειριστές*, *P_2: Διοίκηση Πληροφορικής* και *P_3: Ομάδα Ασφάλειας* και τα κριτήρια τα οποία επιλέχθηκαν στο συγκεκριμένο δένδρο απόφασης είναι κριτήρια είναι *K_1: Γνώση Πληροφοριακών Στόχων*, *K_2: Γνώση Πληροφοριακών Κινδύνων* και *K_3: Κατανόηση Επιχειρησιακής Αξίας των Συστημάτων* (Εικόνα 11).



Εικόνα 11: Δένδρο Απόφασης για τον υπολογισμό των βαρών συμμετοχής στην αποτίμηση Συστημάτων

Οι αντίστοιχοι πίνακες συγκρίσεων καθώς και τα τελικά βάρη συμμετοχής των ομάδων παρουσιάζονται στους πίνακες 19-22.

Πίνακας 19: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Πληροφοριακών Στόχων

K_1: Γνώση Πληροφοριακών Στόχων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1 : Διαχειριστές	1	1	5	0,480
P_2 : Διοίκηση	1	1	3	0,405
P_3 : Τελικοί Χρήστες	1/5	1/3	1	0,115
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Πίνακας 20: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Γνώση Πληροφοριακών Κινδύνων

K_2: Γνώση Πληροφοριακών Κινδύνων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1 : Διαχειριστές	1	3	5	0,633
P_2 : Διοίκηση	1/3	1	3	0,260
P_3 : Τελικοί Χρήστες	1/5	1/3	1	0,106
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Πίνακας 21: Πίνακας Συγκρίσεων εναλλακτικών ως προς το κριτήριο Κατανόηση Επιχειρησιακής Αξίας των Συστημάτων

K_3: Κατανόηση Επιχειρησιακής Αξίας των Συστημάτων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1 : Διαχειριστές	1	1	3	0,405
P_2 : Διοίκηση	1	1	5	0,480
P_3 : Τελικοί Χρήστες	1/3	1/5	1	0,115
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Πίνακας 22: Βάρη συμμετοχής στην αποτίμηση των Συστημάτων

Κριτήρια	**K_1**	**K_2**	**K_3**	
Προτεραιότητες Κριτηρίων	**0,333**	**0,333**	**0,333**	**Βάρη (w_i)**
P_1 : Διαχειριστές	0,480	0,633	0,405	0,506
P_2 : Διοίκηση	0,405	0,260	0,480	0,382
P_3 : Τελικοί Χρήστες	0,115	0,106	0,115	0,112
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Η αποτίμηση των επιπτώσεων γίνεται με διαφορετική προσέγγιση, ανάλογα με το είδος του κάθε αγαθού (Βήμα 1.2). Συγκεκριμένα, για τα αγαθά Δεδομένων γίνεται αποτίμηση ως προς:

- ✓ **Απώλεια Διαθεσιμότητας:** Εξετάζεται η απώλεια της διαθεσιμότητας κάθε αγαθού για τα παρακάτω χρονικά διαστήματα: μέχρι 3 ώρες (πολύ μικρή διάρκεια μη διαθεσιμότητας), από 3 ώρες μέχρι 1 ημέρα (μικρή διάρκεια), από 1 ημέρα μέχρι 1 εβδομάδα (μέτρια διάρκεια), μεγαλύτερο από 1 εβδομάδα (μεγάλης διάρκεια μη διαθεσιμότητας) και οριστική απώλεια της διαθεσιμότητας.
- ✓ **Απώλεια Εμπιστευτικότητας:** Αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού, Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού.
- ✓ **Απώλεια Ακεραιότητας**: Μερική καταστροφή, ολική καταστροφή, σκόπιμη αλλοίωση, ακούσια αλλοίωση.

Για την αποτίμηση των *Συστημάτων* και κατ' επέκταση των αγαθών από τα οποία αποτελείται κάθε Σύστημα (σύμφωνα με το Δένδρο αλληλεξαρτήσεων της Εικόνας 9) εξετάζεται ο *Βαθμός Συσχέτισης (Correlation Factor – CF)*, του Συστήματος με κάθε η-υπηρεσία με την οποία συνδέεται / υποστηρίζει. Ως Βαθμός Συσχέτισης, CF (System S, Service E), ορίζεται το ποσοστό με το οποίο το Σύστημα, S, επηρεάζει την Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα της η-υπηρεσίας, E, με την οποία είναι συνδεδεμένο. Με τον τρόπο αυτό επιτυγχάνεται η απλοποίηση της διαδικασίας

αποτίμησης των Υλικών αγαθών, αγαθών Λογισμικού και Φυσικών αγαθών τα οποία συνδέονται με το συγκεκριμένο Σύστημα.

Τόσο για τη αποτίμηση των επιπτώσεων ασφάλειας των Δεδομένων όσο και των Συστημάτων, κάθε χρήστης (ο οποίος συνδέεται με τα συγκεκριμένα αγαθά, σύμφωνα με το δένδρο αλληλεξαρτήσεων) απαντάει ειδικά διαμορφωμένα ερωτηματολόγια για τα αγαθά στα οποία εμπλέκεται και δίνει τους ατομικούς βαθμούς αποτίμησης με την βοήθεια πενταβάθμιας κλίμακας, όπως φαίνεται στον Πίνακα 14.

4.4.2.4 Βήμα 2.2: Ομαδική αποτίμηση

Αφού έχει ολοκληρωθεί όλη η προηγούμενη διαδικασία και έχουν συγκεντρωθεί οι βαθμοί αποτίμησης κάθε χρήστη, στο βήμα αυτό υπολογίζεται ο ομαδικός βαθμός αποτίμησης της επίπτωσης του κάθε αγαθού. Πιο αναλυτικά, για κάθε χρήστη U_j, με j=1,...,n, που ανήκει στην ομάδα G_k, k=1,..., m, υπολογίζονται οι μέγιστοι (max) ατομικοί βαθμοί αποτίμησης για απώλεια Διαθεσιμότητας, $Iun_{j,k}(A_i)$, απώλεια Εμπιστευτικότητας, $Idis_{j,k}(A_i)$, και απώλεια Ακεραιότητας, $Imod_{j,k}(A_i)$, του αγαθού A_i. (ως αγαθό A_i εννοούμε στην φάση αυτή είτε Δεδομένα είτε Σύστημα). Η διατήρηση των μέγιστων ατομικών βαθμών αποτίμησης συνεπειών οφείλεται στο γεγονός ότι ακολουθείται μία θεώρηση «χειρότερου σεναρίου» (worst case scenario), σύμφωνα με το πρότυπο ISO 27005:2008 [15].

Για τον υπολογισμό των βαθμών αποτίμησης της επίπτωσης κάθε ομάδας G_k παίρνουμε τον μέσο όρο των παραπάνω μεγίστων και τα πολλαπλασιάζουμε με το βάρος της αντίστοιχης ομάδας (w_k) σύμφωνα με τους παρακάτω τύπους :

$$Iun_k(A_i) = \left(\frac{\sum_{j=1}^{n} Iun_{j,k}(A_i)}{n}\right) * w_k \quad (4.1)$$

$$Idis_k(A_i) = \left(\frac{\sum_{j=1}^{n} Idis_{j,k}(A_i)}{n}\right) * w_k \quad (4.2)$$

$$Imod_k(A_i) = \left(\frac{\sum_{j=1}^{n} Imod_{j,k}(A_i)}{n}\right) * w_k \quad (4.3)$$

4.4.2.5 Βήμα 2.3: Συνολική αποτίμηση

Για τους τελικούς βαθμούς αποτίμησης της επίπτωσης ενός αγαθού A_i, ως προς απώλεια Διαθεσιμότητας I_{un}, Εμπιστευτικότητας I_{dis}, και Ακεραιότητας I_{mod}, αθροίζουμε όλα τα $Iun_k(A_i)$, $Idis_k(A_i)$, $Imod_k(A_i)$ για κάθε ομάδα k, σύμφωνα με τους τύπους:

$$I_{un}(A_i) = \sum_{k=1}^{m} Iun_k(A_i) \quad (4.4)$$

$$I_{dis}(A_i) = \sum_{k=1}^{m} Idis_k(A_i) \quad (4.5)$$

$$I_{mod}(A_i) = \sum_{k=1}^{m} Imod_k(A_i). \quad (4.6)$$

Αποτέλεσμα της παραπάνω διαδικασίας είναι η αποτίμηση όλων των αγαθών κάθε υπηρεσίας όπως φαίνεται στον Πίνακα 23.

Πίνακας 23: Αποτελέσματα Αποτίμησης Επιπτώσεων

Αγαθό	**Τρόπος υπολογισμού Βαθμών Αποτίμησης Επιπτώσεων**
Δεδομένα:	Ο Βαθμός Αποτίμησης ως προς την απώλεια *Διαθεσιμότητας* των *Δεδομένων* προκύπτει από τον τύπο : $I_{un}(A_i) = \sum_{k=1}^{m} Iun_k(A_i)$ (4.7) Ο Βαθμός Αποτίμησης ως προς την απώλεια *Εμπιστευτικότητας* των *Δεδομένων* προκύπτει από τον τύπο : $I_{dis}(A_i) = \sum_{k=1}^{m} Idis_k(A_i)$ (4.8) Ο Βαθμός Αποτίμησης ως προς την απώλεια *Ακεραιότητας* των *Δεδομένων* προκύπτει από τον τύπο : $I_{mod}(A_i) = \sum_{k=1}^{m} Imod_k(A_i)$ (4.9)
Υπηρεσίες:	Ο βαθμός αποτίμησης κάθε *η-υπηρεσίας*, $\mathbf{E_e}$ με e=1,2,.. προκύπτει από τον μέγιστο βαθμό των συνδεδεμένων Δεδομένων με την συγκεκριμένη η-υπηρεσία. Πιο συγκεκριμένα, Ο Βαθμός Αποτίμησης ως προς την απώλεια Διαθεσιμότητας: $I_{un}(E_e) = \max(I_{un}(A_1), I_{un}(A_2), I_{un}(A_3), \ldots)$ (4.10) Ο Βαθμός Αποτίμησης ως προς την απώλεια Εμπιστευτικότητας: $I_{dis}(E_e) = \max(I_{dis}(A_1), I_{dis}(A_2), I_{dis}(A_3), \ldots)$ (4.11) Ο Βαθμός Αποτίμησης ως προς την απώλεια Ακεραιότητας: $I_{mod}(E_e) = \max(I_{mod}(A_1), I_{mod}(A_2), I_{mod}(A_3), \ldots)$ (4.12)

Φυσικά αγαθά / Υλικό / Λογισμικό:	Για τα αγαθά τα οποία ανήκουν σε μία από τις κατηγορίες Φυσικά αγαθά, Υλικό, και Λογισμικό, οι βαθμοί αποτίμησης επιπτώσεων υπολογίζονται σύμφωνα με το **CF** (System S, Service E) του Συστήματος **S** και της η-υπηρεσίας **E** με τα οποία συνδέονται. Πιο συγκεκριμένα: Ο Βαθμός Αποτίμησης ως προς την απώλεια *Διαθεσιμότητας* : $I_{un} = I_{un}(E_e) * CF_{un}(S_s, E_e)$ (4.13) Ο Βαθμός Αποτίμησης ως προς την απώλεια *Εμπιστευτικότητας*: $I_{dis} = I_{dis}(E_e) * CF_{dis}(S_s, E_e)$ (4.14) Ο Βαθμός Αποτίμησης ως προς την απώλεια *Ακεραιότητας*: $I_{mod} = I_{mod}(E_e) * CF_{mod}(S_s, E_e)$ (4.15)

Παράδειγμα τρόπου υπολογισμού του Βαθμού Αποτίμησης Επιπτώσεων:

Για την καλύτερη κατανόηση του τρόπου υπολογισμού του βαθμού αποτίμησης των επιπτώσεων ενός αγαθού, ακολουθεί ένα αναλυτικό παράδειγμα. Έστω ότι στην διαδικασία συμμετέχουν ένας χρήστης $U_{1,1}$ από την ομάδα *Διοίκηση*, ένας χρήστης $U_{1,2}$ από την ομάδα *Διαχειριστές και* δύο χρήστες $U_{1,3}$ $U_{2,3}$ από την ομάδα *Τελικοί Χρήστες*. Υποθέτουμε ότι και οι τέσσερις παραπάνω χρήστες εμπλέκονται στη διαδικασία αποτίμησης επιπτώσεων (απώλεια Διαθεσιμότητας, Εμπιστευτικότητας και Ακεραιότητας) του αγαθού A_i (το οποίο είναι ένα αγαθό Δεδομένων), συμμετέχοντας με τα βάρη των ομάδων στις οποίες ανήκουν (Πίνακας 18). Πιο συγκεκριμένα, το βάρος της ομάδας *Διοίκηση* είναι w_1 = 0.620, της ομάδας, *Διαχειριστές* είναι w_2 = 0.2222 και της ομάδας *Τελικοί Χρήστες* είναι w_2 = 0. 159.

Ο χρήστης $U_{1,1}$ της ομάδας *Διοίκηση* έχει δώσει στο αγαθό A_i βαθμό αποτίμησης ως προς την απώλεια Διαθεσιμότητας δύο τιμές: Εκτιμάει ότι σε περίπτωση που θα έχει απώλεια διαθεσιμότητας το συγκεκριμένο αγαθό, θα υπάρξει οικονομική απώλεια επιπέδου 5 και Δυσφήμηση επιπέδου 3. Οπότε σαν ατομικός βαθμός αποτίμησης του συγκεκριμένου χρήστη λαμβάνεται ο μέγιστος, ο οποίος είναι $Iun_{1,1}(A_i)$=max(5,3)=5. Στην συνέχεια η τιμή αυτή πολλαπλασιάζεται με το βάρος της ομάδας στην οποία ανήκει ο χρήστης για να προκύψει ο βαθμός αποτίμησης της ομάδας του:

$$Iun_1(A_i)=\left(\frac{\sum_{j=1}^{n} Iun_{j,1}(A_i)}{n}\right) * w_1 = \left(\frac{\sum_{j=1}^{1} Iun_{j,1}(A_i)}{1}\right) * w_1 = 5*0.620 = 3.1 \quad (4.16)$$

Ο χρήστης $U_{1,2}$ της ομάδας *Διαχειριστές* έχει αποτιμήσει την απώλεια διαθεσιμότητας του αγαθού A_i με βαθμό 5. Οπότε για να υπολογιστεί ο βαθμός τις ομάδας στην οποία ανήκει χρησιμοποιείται ο παρακάτω πίνακας:

$$Iun_3(A_i)=\left(\frac{\sum_{j=1}^{1} Iun_{j,3}(A_i)}{1}\right) * w_3 = 5*0.222 = 1.1 \quad (4.17)$$

Ο χρήστης $U_{1,3}$ της ομάδας *Τελικοί χρήστες* έχει δώσει και αυτός δύο τιμές στο αγαθό A_i, Νομικές επιπτώσεις: 5 και Δυσφήμηση: 4, οπότε ο ατομικός του βαθμός αποτίμησης είναι ο μέγιστος και είναι $Iun_{1,3}(A_i)$=max (5,4)=5. Από την ίδια ομάδα συμμετέχει και ο χρήστης $U_{2,3}$ του οποίου ο ατομικός βαθμός αποτίμησης είναι $Iun_{2,3}(A_i)$=max (3,4)=4. Για να υπολογιστεί ο βαθμός αποτίμησης της ομάδας *Τελικοί Χρήστες,* βρίσκουμε τον μέσο όρο των ατομικών βαθμών αποτίμησης $Iun_{1,3}(A_i)$, $Iun_{2,3}(A_i)$ των χρηστών $U_{1,3}$ και $U_{2,3}$ της ομάδας και το πολλαπλασιάζουμε με το βάρος της ομάδας ως εξής:

$$Iun_2(A_i)=\left(\frac{\sum_{j=1}^{2} Iun_{j,2}(A_i)}{2}\right) * w_2 = \left(\frac{Iun_{1,2}(A_i) + Iun_{2,2}(A_i)}{2}\right) * w_2 = 4.5*0.159 = 0.7 \quad (4.18)$$

Για να βρεθεί ο τελικός βαθμός αποτίμησης της επίπτωσης απώλειας Διαθεσιμότητας I_{un} του αγαθού A_i, αθροίζονται οι τιμές των ομάδων που συμμετείχαν στην αποτίμησης, δηλαδή:

$$Iun = \sum_{k=1}^{m} Iun_k\ (Ai) = \sum_{k=1}^{3} Iun_k\ (A_i) = Iun_1\ (A_i) + Iun_2\ (A_i) + Iun_3\ (A_i) = 3.1+1.1+0.7 = 4.9 \quad (4.19)$$

Στον πίνακα που ακολουθεί φαίνονται όλες οι τιμές του παραδείγματος για τον υπολογισμό του βαθμού αποτίμησης επιπτώσεων σε περίπτωση απώλειας της διαθεσιμότητας του αγαθού, καθώς και οι τιμές αποτίμησης σε περίπτωση απώλειας εμπιστευτικότητας και ακεραιότητας, οι οποίες υπολογίζονται με πανομοιότυπο τρόπο.

Πίνακας 24: Υπολογισμός των βαθμών αποτίμησης επιπτώσεων ενός αγαθού A_i

Ομάδες Χρηστών	Χρήστες	I_{un}
G_1: Διοίκηση $w_1 = 0.620$	$U_{1,1}$: Προϊστάμενος Τμήματος Πληροφορικής	Οικονομική απώλεια: 5 Δυσφήμηση: 3 $I\,un_{1,1}(A_i) = \max(5,3) = 5$
	$Iun_1(A_i) = \left(\frac{\sum_{j=1}^{1} Iun_{j,1}(A_i)}{n}\right) * w_1$	$Iun_1(A_i) = \left(\frac{5}{1}\right) * 0.620 = 3.1$
G_2: Διαχειριστές $w_2 = 0.222$	$U_{1,2}$: Διαχειριστής Βάσεων Δεδομένων	Παρεμπόδιση εμπορικών δραστηριοτήτων: 5
	$Iun_2(A_i) = \left(\frac{\sum_{j=1}^{1} Iun_{j,2}(A_i)}{1}\right) * w_2$	$Iun_2(A_i) = \left(\frac{5}{1}\right) * 0{,}222 = 1.1$
G_3: Τελικοί Χρήστες $W_3 = 0.159$	$U_{1,3}$: Χρήστης Τμήματος Λογιστηρίου	Νομικές επιπτώσεις: 5 Δυσφήμηση: 4 $Iun_{1,3}(A_i) = \max(5,4) = 5$
	$U_{2,3}$:Χρήστης Τμήματος Πληροφορικής	Νομικές επιπτώσεις: 3 Δυσφήμηση:4 $Iun_{1,3}(A_i) = \max(3,4) = 4$
	$Iun_3(A_i) = \left(\frac{\sum_{j=1}^{2} Iun_{j,3}(A_i)}{2}\right) * w_3$	$Iun_3(A_i) = \left(\frac{4+5}{2}\right) * 0{,}159 = 0.7$
Τελικός Βαθμός Αποτίμησης Επιπτώσεων του αγαθού	$Iun(A_i) = \sum_{k=1}^{m} Ia_k\ (A_i)$	$Iun_1(A_i) + Iun_2(A_i) + Iun_3(A_i) = 4.9$

Από το παραπάνω παράδειγμα φαίνεται ότι οι τελικοί βαθμοί αποτίμησης επιπτώσεων για την απώλεια Διαθεσιμότητας, $I_{un}(A_i)$, του συγκεκριμένου αγαθού $A_ι$ είναι :

$$I_{un}(A_i) = 4.9 \quad (4.20)$$

Με τον ίδιο τρόπο υπολογίζονται και οι βαθμοί αποτίμησης επιπτώσεων του αγαθού A_i ως προς απώλεια Εμπιστευτικότητας I_{dis}, και Ακεραιότητας I_{mod}. Η μεθοδολογία STORM-RM κρατάει και τους τρεις ξεχωριστούς βαθμούς αποτίμησης ώστε στη Φάση 5, όπου υπολογίζεται η επικινδυνότητα, να συμπεριληφθεί ο κάθε ένας από αυτούς σε συνδυασμό με τον βαθμό αποτίμησης των απειλών που προκαλούν αντίστοιχα απώλεια διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας. Με τον τρόπο αυτό θα είναι σε θέση η μεθοδολογία να εντοπίσει και να προτείνει στην συνέχεια (στο Βήμα 6.1) και τα κατάλληλα μέτρα προστασίας.

4.4.3 Φάση 3: Αποτίμηση Απειλών

4.4.3.1 Βήμα 3.1: Προσδιορισμός Απειλών

Στο συγκεκριμένο Βήμα γίνεται ο προσδιορισμός των απειλών για κάθε αγαθό, ανάλογα με το είδος του αγαθού, σύμφωνα με την κατηγοριοποίηση του Βήματος 1.2. Η μεθοδολογία διαθέτει μια λίστα από πιθανές απειλές, η οποία βασίζεται στις κατηγοριοποιήσεις απειλών διάφορων γνωστών μεθοδολογιών (OCTAVE [21][22], CRAMM [12], NIST [25]). Συγκεντρώθηκε ένας μεγάλος αριθμός απειλών, οι οποίες ομαδοποιήθηκαν στις παρακάτω κατηγορίες:

- ✓ **φυσικές απειλές** (π.χ. σεισμός, πλημμύρα, τυφώνας, κεραυνοί)
- ✓ **τεχνολογικές απειλές** (π.χ. αστοχία υλικού)
- ✓ **περιβαλλοντολογικές απειλές** (π.χ. ρύπανση, χημικές ουσίες)
- ✓ **ανθρώπινες απειλές** (π.χ. επιθέσεις στο δίκτυο, προσβολή από τον ιό, πρόσβαση χωρίς άδεια)
- ✓ **οργανωμένη ή εσκεμμένη επίθεση** (π.χ. τρομοκρατική ενέργεια - τοποθέτηση εκρηκτικού μηχανισμού, δολιοφθορά, εμπρησμός)
- ✓ **απειλές αλλοίωσης δεδομένων** (π.χ. κακόβουλη καταστροφή δεδομένων, μη εξουσιοδοτημένη πρόσβαση σε δεδομένα).

Σύμφωνα λοιπόν με την κατηγορία στην οποία ανήκει ένα αγαθό (Φυσικό αγαθό, Υλικό, Λογισμικό, Δεδομένα, Δικτυακός εξοπλισμός), αντιστοιχίζονται μία ή και περισσότερες ομάδες των πιθανών απειλών. Στον Πίνακα 25 φαίνεται ένα ενδεικτικό παράδειγμα αντιστοίχισης των απειλών σε μια ομάδα αγαθών. Η πλήρης λίστα παρατίθεται στο Παράρτημα ΙΙ. Σημειώνεται ότι η λίστα αυτή μπορεί να ανανεωθεί εφόσον προκύψουν νέες απειλές.

Πίνακας 25: Αντιστοίχιση Αγαθών -Απειλών

ΕΙΔΟΣ ΑΓΑΘΟΥ	ΑΠΕΙΛΕΣ
ΦΥΣΙΚΑ ΑΓΑΘΑ	Πυρκαγιά
	Σεισμός
	Πλημμύρα
ΥΛΙΚΟ	Διακυμάνσεις Ηλεκτρικής Ισχύος
	Τεχνικές Βλάβες
	Ηλεκτρονικές Παρεμβολές
ΑΓΑΘΑ ΛΟΓΙΣΜΙΚΟΥ	Μη εξουσιοδοτημένες αλλαγές σε λογισμικό
	Κακόβουλο Λογισμικό
	Άρνηση Υπηρεσίας
ΑΓΑΘΑ ΔΕΔΟΜΕΝΩΝ	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα
	Σφάλμα χειρισμού
	Κακόβουλη καταστροφή δεδομένων
ΔΙΚΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	Σφάλματα μετάδοσης
	Μη ορθή δρομολόγηση επικοινωνιών
	Εξαπάτηση διεύθυνσης δικτύου (IP Spoofing)

4.4.3.2 Βήμα 3.2: Αποτίμηση απειλών

Προκειμένου να πραγματοποιηθεί η αποτίμηση των απειλών για κάθε αγαθό, κάθε συμμετέχοντας στο βήμα αυτό, θα κληθεί να εκτελέσει μια σειρά ανά δύο συγκρίσεων (με την βοήθεια του πίνακα συγκρίσεων AHP) για τις απειλές που αντιστοιχούν σε ένα αγαθό, ώστε να προκύψουν τελικά οι πιο πιθανές απειλές. Σαν αποτέλεσμα, κάθε χρήστης θα ιεραρχήσει τις πιθανές απειλές που αντιμετωπίζει κάθε αγαθό ως προς τα κριτήρια Κίνητρο και Συχνότητα Εμφάνισης.

Οι προτεραιότητες του κάθε χρήστη για κάθε αγαθό θα υπολογιστούν με την AHP και θα προκύψουν οι ατομικοί βαθμοί Απειλών (Ατομική Αποτίμηση Απειλών) σύμφωνα με την κλίμακα του Πίνακα 26.

Πίνακας 26: Κλίμακα αποτίμησης Απειλών

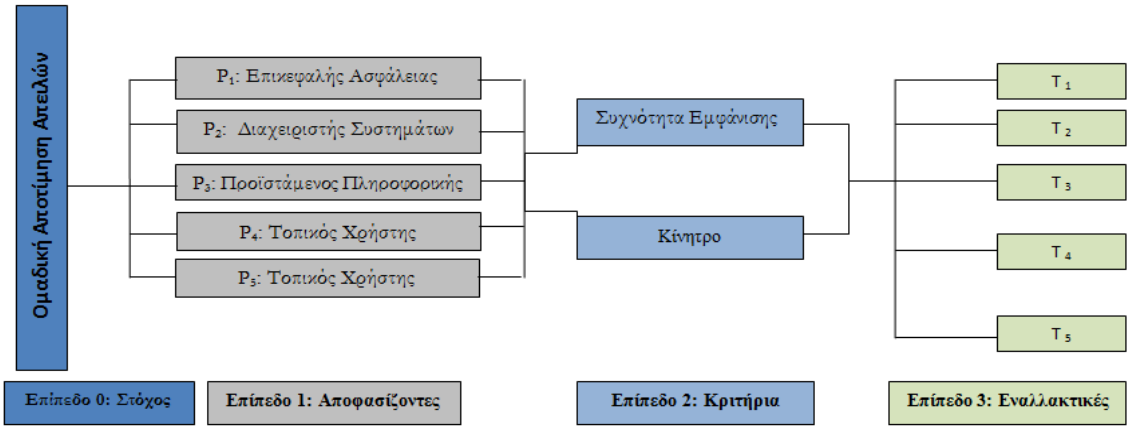
Συνολική αποτίμηση απειλών	Επίπεδο Απειλής	Βαθμός Αποτίμησης Απειλής
≥ 80	Πολύ Υψηλό (ΠΥ)	1
60-79	Υψηλό (Υ)	0,33
40-59	Μέτριο (Μ)	0,1
20-39	Χαμηλό (Χ)	0,034
≤ 19	Πολύ Χαμηλό (ΠΧ)	0,01

Για παράδειγμα, στον Πίνακα 27 φαίνεται η ατομική αποτίμηση του χρήστη P_2 για τις 5 απειλές (T_1,.. T_5) που αντιστοιχούν στο αγαθού A_1

Πίνακας 27: Ατομική αποτίμηση απειλών (χρήστης P_2)

Κριτήρια (Criteria)	Συχνότητα Εμφάνισης	Κίνητρο			
Προτεραιότητες Κριτηρίων (Criteria Priorities)	0,8333	0,1667	Προτεραιότητες	Κανονικοποιημένες Προτεραιότητες	Ποσοστό Προτεραιότητας
T_1	0,5497	0,4884	0,5395	1,0000	100,0%
T_2	0,2118	0,2173	0,2127	0,3943	39,4%
T_3	0,0977	0,0886	0,0962	0,1783	17,8%
T_4	0,0860	0,0778	0,0846	0,1569	15,7%
T_5	0,0548	0,1278	0,0670	0,1242	12,4%

Η ομαδική αποτίμηση των απειλών του κάθε αγαθού θα υπολογιστεί λαμβάνοντας υπόψη τα βάρη των συμμετεχόντων και την ατομική αποτίμηση (ιεράρχηση) των απειλών για κάθε αγαθό. Στην Εικόνα 12 φαίνεται το δένδρο απόφασης που χρησιμοποιείται για την ομαδική αποτίμηση των απειλών που αντιστοιχούν στο αγαθό A_1, με συμμετέχοντες τους P_1, P_2, P_3, P_4, P_5.



Εικόνα 12: Δένδρο Απόφασης-Ομαδικής Αποτίμησης Απειλών

Στον Πίνακα 28 παρουσιάζονται τα ομαδικά αποτελέσματα με τις προτεραιότητες κάθε απειλής.

Πίνακας 28: Ομαδικά Αποτελέσματα

Συμμετέχοντες	**P_1**	**P_2**	**P_3**	**P_4**	**P_5**			
Βάρη Συμμετεχόντων	0,3236	0,3116	0,2700	0,0654	0,0294	Συνολικές Προτεραιότητες	Κανονικοποιημένες Προτεραιότητες	Ποσοστό Προτεραιότητας
T_1	0,5420	0,5395	0,5436	0,5344	0,5292	0,5408	1,0000	100,0%
T_2	0,2125	0,2127	0,2123	0,2132	0,2136	0,2126	0,3931	39,3%
T_3	0,0966	0,0962	0,0968	0,0955	0,0947	0,0964	0,1783	17,8%
T_4	0,0850	0,0846	0,0852	0,0840	0,0833	0,0848	0,1568	15,7%
T_5	0,0639	0,0670	0,0621	0,0731	0,0792	0,0654	0,1210	12,1%

Αφού ολοκληρωθεί η παραπάνω διαδικασία, για την απειλή με την μεγαλύτερη προτεραιότητα γίνεται εκτίμηση της πιθανότητας εμφάνισής της από την Ομάδα Ασφάλειας. Στην συνέχεια οι κανονικοποιημένες προτεραιότητες των απειλών πολλαπλασιάζονται με την πιθανότητα εμφάνισης της απειλής που έχει την μεγαλύτερη προτεραιότητα (ποσοστό 100%), δηλαδή υπερίσχυσε στην προηγούμενη ομαδική αξιολόγηση. Πιο συγκεκριμένα για το παράδειγμα του προηγούμενου πίνακα, η απειλή T_1 έχει την υψηλότερη συνολική προτεραιότητα (0,5408) και επομένως ποσοστό 100%. Έτσι αν υποθέσουμε ότι η εκτίμηση της πιθανότητας εμφάνισης της απειλής T_1 είναι για παράδειγμα 30%, τότε πολλαπλασιάζοντας τις ποσοστιαίες κανονικοποιημένες προτεραιότητες των 5 πιθανών απειλών με την πιθανότητα εμφάνισης της απειλής T_1 προκύπτουν τα αποτελέσματα της συνολικής αποτίμησης των απειλών που φαίνονται στον Πίνακα 29.

Πίνακας 29: Υπολογισμός επιπέδου απειλής για το αγαθό A_1

Απειλές	**Ποσοστό Προτεραιότητας**	**Πιθανότητα σημαντικότερης απειλής**	**Συνολική αποτίμηση απειλών**	**Επίπεδο Απειλής**
T_1	100,00%	30%	30,00%	Χαμηλό (Χ)
T_2	39,30%	30%	11,79%	Πολύ Χαμηλό (ΠΧ)
T_3	17,80%	30%	5,34%	Πολύ Χαμηλό (ΠΧ)
T_4	15,70%	30%	4,71%	Πολύ Χαμηλό (ΠΧ)
T_5	12,10%	30%	3,63%	Πολύ Χαμηλό (ΠΧ)

Φαίνεται, λοιπόν, ότι οι ομαδικές απαντήσεις των 5 χρηστών δίνουν σαν αποτέλεσμα ότι η Απειλή T_1 αποτιμήθηκε σαν **Χ** και οι Απειλές T_2, T_3,T_4,T_5 σαν **ΠΧ**, σύμφωνα με την κλίμακα του Πίνακα 26.

4.4.4 Φάση 4: Αποτίμηση αδυναμιών

4.4.4.1 Βήμα 4.1: Προσδιορισμός αδυναμιών

Η μεθοδολογία STORM-RM εξετάζει τις αδυναμίες σε κατηγορίες ανάλογα με την απειλή και το είδος του αγαθού. Πιο συγκεκριμένα, για κάθε απειλή γίνεται αντιστοίχιση των αδυναμιών ασφάλειας που σχετίζονται με αυτή την απειλή. Επιπλέον, κάθε κατηγορία αγαθών σχετίζεται μόνο με εκείνες τις απειλές που αφορούν στη συγκεκριμένη κατηγορία αγαθών, όπως περιγράφηκε στο Βήμα 3.1. Στον Πίνακα 30 παρουσιάζεται ένα αντιπροσωπευτικό παράδειγμα της αντιστοίχισης αγαθών-απειλών-αδυναμιών, ενώ στο Παράρτημα ΙΙ παρουσιάζονται αναλυτικά οι αντιστοιχίσεις.

Πίνακας 30: Παράδειγμα αντιστοίχισης Είδους αγαθού/Απειλών/Αδυναμιών

Είδος Αγαθού	Απειλές- (T_i)	Αδυναμίες - (V_i)
Φυσικό Αγαθό	$T_{1:}$ Φωτιά	V_{11}: Ύπαρξη εύφλεκτων υλικών V_{12} : Αστοχία συστημάτων ανίχνευσης φωτιάς V_{13} : Αστοχία φυσικής ασφάλειας $V_{1\ n}$: Αδυναμία - (για T_1)
	T_m	V_{m1}....V_{mn}
Υλικό	$T_{2:}$ Αστοχία Υλικού	V_{21} : Λανθασμένη συντήρηση V_{22}: Έλλειψη συντήρησης V_{2n}: Αδυναμία - (για T_2)
	T_m	V_{m1}...V_{mn}
Λογισμικό	T3: Κακόβουλος κώδικας	V_{31}: Απουσία σντι-ικού λογισμικού V_{32}: Αποτυχημένη ενημέρωση σντι-ικού λογισμικού V_{33}: Ανεπαρκής εκπαίδευση του προσωπικού για τους ιούς V_{3n}: Αδυναμία - (για T_3)
	T_m	V_{m1}....V_{mn}

Σύμφωνα με την κατηγοριοποίηση αυτή θα εξεταστούν στο Βήμα 4.3 τα αγαθά ως προς τις αδυναμίες για τις πιθανές απειλές που αντιστοιχούν στο συγκεκριμένο αγαθό.

4.4.4.1.1 Ορισμός κλίμακας αδυναμιών

Η μεθοδολογία χρησιμοποιεί την παρακάτω κλίμακα αποτίμησης αδυναμιών (Πίνακας 31), η οποία περιλαμβάνει τρεις ισοκατανεμημένες πιθανότητες εκδήλωσης του χειρότερου σεναρίου από την εκδήλωση μιας απειλής. Για παράδειγμα, σε περίπτωση εκδήλωσης μιας απειλής, αν το επίπεδο αδυναμίας του υπό εξέταση αγαθού ως προς την απειλή αυτή είναι Υψηλό, τότε αυτό σημαίνει ότι η πιθανότητα να συμβεί το χειρότερο σενάριο (δηλαδή να έχουμε την μεγαλύτερη ζημιά - απώλεια) είναι μεγαλύτερη του 66%.

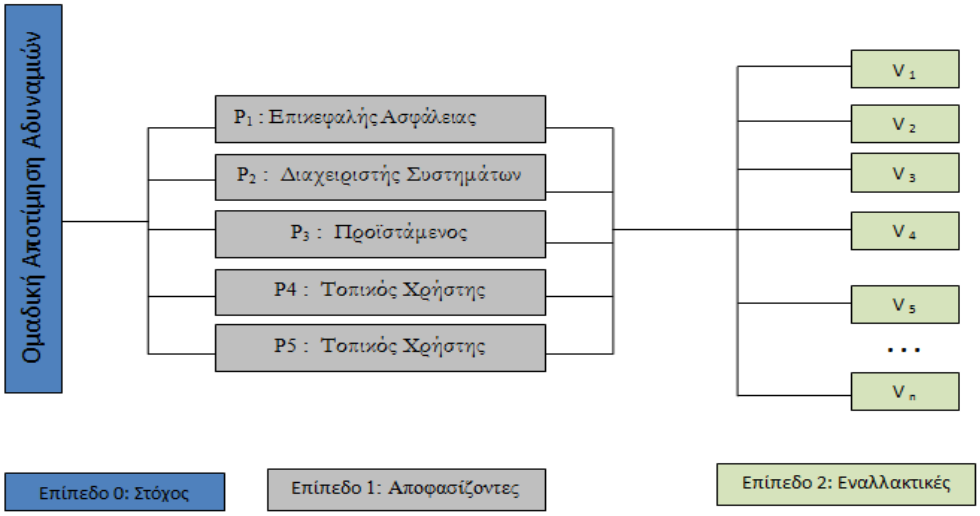
Πίνακας 31: Κλίμακα Αποτίμησης Αδυναμιών

Προτεραιότητα αδυναμιών	Επίπεδο Αδυναμιών	Βαθμός Αποτίμησης Αδυναμιών	Περιγραφή (Πιθανότητα να συμβεί το χειρότερο σενάριο)
>66 %	Υψηλό (Υ)	1	>66%
33-66 %	Μέτριο (Μ)	0,66	33% - 66%
<33 %	Χαμηλό (Χ)	0,33	< 33%

Με βάση την κλίμακα αυτή γίνεται τόσο η θεωρητική όσο και η πρακτική ανάλυση των αδυναμιών των αγαθών του υπό εξέταση οργανισμού με τρόπο ο οποίος περιγράφεται αναλυτικά στα βήματα που ακολουθούν. Με σκοπό να γίνει πιο αντικειμενική η αποτίμηση των αδυναμιών και να ανακαλυφθούν τυχόν νέες αδυναμίες, εκτός από την θεωρητική γίνεται και πρακτική αποτίμηση αδυναμιών.

4.4.4.2 Βήμα 4.2: Θεωρητική Αποτίμηση Αδυναμιών

Στην θεωρητική αποτίμηση αδυναμιών, κάθε χρήστης που συμμετέχει στο βήμα αυτό καλείται να ιεραρχήσει τις αδυναμίες που αντιστοιχούν στο υπό εξέταση αγαθό, για κάθε απειλή. Η ιεράρχηση αυτή γίνεται με χρήση του δένδρου απόφασης AHP που φαίνεται στο παράδειγμα της Εικόνας 13.



Εικόνα 13: Ομαδική Θεωρητική Αποτίμηση Αδυναμιών

Πιο συγκεκριμένα, οι χρήστες *P_1: Επικεφαλής Ασφάλειας, P_2: Διαχειριστής Συστημάτων, P_3: Προϊστάμενος Τμήματος Πληροφορικής* και οι *δύο τοπικοί χρήστες* P_4, P_5 καλούνται να αξιολογήσουν τις πέντε (5) αδυναμίες που αντιστοιχούν στο αγαθό A_i για μία συγκεκριμένη απειλή (Παράρτημα ΙΙ). Ο κάθε χρήστης (συμμετέχων) αξιολογεί την σημαντικότητα των αδυναμιών που αντιμετωπίζει το υπό εξέταση αγαθό με την βοήθεια της ανά δύο σύγκρισης της μεθοδολογίας AHP. Στην συνέχεια, λαμβάνοντας υπόψη τα βάρη του κάθε συμμετέχοντα υπολογίζεται ο ομαδικός θεωρητικός βαθμός Αποτίμησης Αδυναμιών, των αδυναμιών του αγαθού A_i, ως προς μία συγκεκριμένη απειλή. Στον Πίνακα 32 φαίνεται η ατομική αξιολόγηση πέντε (5) αδυναμιών ενός αγαθού, τα βάρη των συμμετεχόντων καθώς και οι ομαδικοί θεωρητικοί βαθμοί αποτίμησης αδυναμιών.

Πίνακας 32: Ομαδική Θεωρητική Αποτίμηση Αδυναμιών

Συμμετέχοντες	P_1	P_2	P_3	P_4	P_5		
Βάρη Συμμετεχόντων	0,3236	0,3116	0,2700	0,0654	0,0294	Συνολικές Προτεραιότητες	Συνολικές Προτεραιότητες (Ποσοστό)
V_1	0,5420	0,5395	0,5436	0,5344	0,5292	0,5408	54,08 %
V_2	0,2125	0,2127	0,2123	0,2132	0,2136	0,2126	21,26 %
V_3	0,0966	0,0962	0,0968	0,0955	0,0947	0,0964	9,64 %
V_4	0,0850	0,0846	0,0852	0,0840	0,0833	0,0848	8,48 %
V_5	0,0639	0,0670	0,0621	0,0731	0,0792	0,0654	6,54 %

Έτσι, από τον προηγούμενο πίνακα και σύμφωνα με την κλίμακα του Πίνακα 31 οι ομαδικοί Θεωρητικοί Βαθμοί Αποτίμησης Αδυναμιών είναι:

V_1=M, αφού η προτεραιότητα αδυναμιών ανάμεσα από 33-66

V_2=X, αφού η προτεραιότητα αδυναμιών ανάμεσα από 33

V_3=X, αφού η προτεραιότητα αδυναμιών < 33

V_4=X, αφού η προτεραιότητα αδυναμιών < 33

V_5=X, αφού η προτεραιότητα αδυναμιών < 33

Για τον υπολογισμό του τελικού Θεωρητικού Επιπέδου Αποτίμησης Αδυναμιών (Theoretical Vulnerability Level), $TV(A_i)$, ενός αγαθού A_i, ως προς μία συγκεκριμένη απειλή, υπολογίζεται ως ο μέγιστος των ομαδικών βαθμών. Έτσι για το παραπάνω παράδειγμα το τελικό Θεωρητικό Επίπεδο Αποτίμησης Αδυναμιών είναι:

$$TV(A_i)= \max\left(V_1, V_2, V_3, V_4, V_5\right) = M \quad (4.21)$$

4.4.4.3 Βήμα 4.3: Πρακτική Αποτίμηση Αδυναμιών

Η προτεινόμενη πρακτική αποτίμηση αδυναμιών των αγαθών στηρίζεται σε υπάρχουσες μεθοδολογίες ανίχνευσης ευπαθειών, όπως είναι οι ISSAF [11], OSSTMM [24], OWASP [29] και WASC-TC [31], λαμβάνοντας υπόψη της ελέγχους και τεχνικές οι οποίες προδιαγράφονται και καθορίζονται από τα συγκεκριμένα πλαίσια.

Η πρακτική αποτίμηση αδυναμιών της μεθοδολογίας STORM-RM εξετάζει κατηγορίες αγαθών οι οποίες έχουν καθοριστεί στο Βήμα 1.2. Πιο συγκεκριμένα, οι κατηγορίες που εξετάζονται είναι τα Υλικά αγαθά (Hardware), το Λογισμικό (Software), οι Υπηρεσίες (Services) και οι Χρήστες (Users).

Τα αποτελέσματα των εργαλείων αυτών αξιολογούνται και στη συνέχεια προκύπτει για κάθε αδυναμία και για κάθε αγαθό το επίπεδο της πρακτικής αποτίμησης αδυναμιών, Practical Vulnerability Assessment $PV(A_i)$. Στη συνέχεια, παρουσιάζονται αναλυτικά τα στάδια της πρακτικής αποτίμησης αδυναμιών για τη μεθοδολογία STORM-RM.

Στάδιο 1ο: Εφαρμογή Κοινωνικής Μηχανικής (Social Engineering)

Σκοπός του συγκεκριμένου σταδίου είναι η αποτίμηση και ο έλεγχος του βαθμού ευαισθητοποίησης και γνώσης σε επιθέσεις που έχουν ως στόχο τον ανθρώπινο παράγοντα. Οι έλεγχοι που μπορεί να εκτελεστούν είναι οι ακόλουθοι:

- ✓ Αναζήτηση γενικών πληροφοριών (π.χ. τηλέφωνα, φαξ, e-mail) που αφορούν στους χρήστες του οργανισμού με χρήση ευρέως διαδεδομένων μηχανών/εργαλείων αναζήτησης.
- ✓ Εκμετάλλευση των συλλεχθεισών πληροφοριών (π.χ. τηλέφωνα) με απώτερο στόχο τη συλλογή περαιτέρω πληροφοριών που αφορούν τους χρήστες και τα εξεταζόμενα αγαθά. Τεχνικές που μπορούν να χρησιμοποιηθούν για το σκοπό αυτό είναι οι ακόλουθες:
    - Φυσική Παρουσία στο χώρο (Physical)
    - Πλαστοπροσωπία (Impersonation)
    - Παρακολούθηση (Tailgating)
    - Τηλεφωνικά (Telephonically)
    - Αλληλογραφία (Mail)
    - Κλασική (Paper)
    - Ηλεκτρονική (Electronic)
    - Ηλεκτρονική Αλληλογραφία (E-Mail)
    - Σύνδεσμος (Link)
    - Επισύναψη Αρχείου (Attachment)

Στάδιο 2ο: Τεχνική Σκιαγράφηση Αγαθών

Στόχος του συγκεκριμένου σταδίου είναι ο προσδιορισμός των τεχνικών χαρακτηριστικών των αγαθών του οργανισμού. Οι ενέργειες που θα εκτελεστούν σε αυτό το στάδιο είναι οι παρακάτω.

- ✓ Εξερεύνηση των ορίων των δικτύων (Network Mapping)
- ✓ Απαρίθμηση και σκιαγράφηση συστημάτων.
- ✓ Προσδιορισμός των Λειτουργικών Συστημάτων (OS fingerprinting)
- ✓ Ανίχνευση διαθέσιμων θυρών (Port Scanning)
- ✓ Αναγνώριση και σκιαγράφηση υπηρεσιών.
- ✓ Πληροφορίες δρομολόγησης και υποστηριζόμενα πρωτόκολλα.
- ✓ Καταγραφή υποστηριζόμενων τεχνολογιών.

Στάδιο 3ο: Εντοπισμός Αδυναμιών

Σε αυτό το στάδιο, οι πληροφορίες από την τεχνική σκιαγράφηση χρησιμοποιούνται για την ανίχνευση αδυναμιών στα Υλικά Αγαθά (Hardware), στο Λογισμικό (Software) και τις Υπηρεσίες (Services) ενός ΠΣ. Η διαδικασία για τον εντοπισμό των αδυναμιών ακολουθεί τα εξής βήματα:

<u>Βήμα 1: Αναζήτηση γνωστών αδυναμιών</u>

Αναζήτηση σε ευρέως διαδεδομένες «βάσεις γνώσεις» (π.χ. Security Focus [28], BugTraq [2], ISS' Xforce [10], NIST's National Vulnerability Database [18], Common Vulnerability and Exposures [5]) για τον εντοπισμό νέων αδυναμιών.

Βήμα 2: Εντοπισμός αδυναμιών

Για τον εντοπισμό των αδυναμιών χρησιμοποιούνται ένα σύνολο αυτοματοποιημένων ή μη εργαλείων που θέτουν ως στόχο να επαληθεύσουν (non-intrusively) την ύπαρξη συγκεκριμένων αδυναμιών χωρίς να προχωρούν σε περαιτέρω εκμετάλλευσή τους. Η φύση του υπό ελέγχου αγαθού καθορίζει την υιοθέτηση και την εφαρμογή μια σειράς ελέγχων οι οποίοι πρέπει να εκτελεστούν για την αξιολόγησή του. Τέτοιου είδους έλεγχοι είναι οι ακόλουθοι:

- ✓ **Έλεγχος Μηχανισμών Ελέγχου Πρόσβασης:** στο πλαίσιο του συγκεκριμένου ελέγχου διαπιστώνεται η ορθότητα και η αποτελεσματικότητα των εφαρμοζόμενων μηχανισμών ελέγχου πρόσβασης στο υπό έλεγχο αγαθό.
- ✓ **Έλεγχος Μηχανισμών Ανίχνευσης Εισβολών**: οι συγκεκριμένοι έλεγχοι επικεντρώνονται στην απόδοση και στην ευαισθησία των μηχανισμών ανίχνευσης εισβολών.
- ✓ **Έλεγχος Μηχανισμών Αντιμετώπισης Κακόβουλου Λογισμικού:** οι έλεγχοι αυτοί έχουν ως απώτερο στόχο να διαπιστωθεί η αποτελεσματικότητα των εγκαταστημένων μηχανισμών καταπολέμησης κακόβουλου λογισμικού.
- ✓ **Έλεγχος Ισχύος κωδικών πρόσβασης:** σκοπός των ελέγχων αυτών είναι να διαπιστωθεί η ισχύς των κωδικών πρόσβασης στα εξεταζόμενα αγαθά.
- ✓ **Έλεγχος Ασφάλειας Ασύρματου Δικτύου:** σκοπός των ελέγχων αυτών ο εντοπισμός πιθανών αδυναμιών ασφάλειας στην υπάρχουσα υποδομή του ασύρματου δικτύου.
- ✓ **Έλεγχος Ασφάλειας Τείχους Προστασίας(Firewall):** στόχος των ελέγχων αυτών είναι να γίνει σωστή εγκατάσταση και παραμετροποίηση του τείχους προστασίας ώστε να διασφαλιστεί ότι ελέγχεται η πρόσβαση μεταξύ δικτύων.
- ✓ **Έλεγχος Ασφάλειας Δικτυακού Εξοπλισμού (Router/Switch):** οι συγκεκριμένοι έλεγχοι έχουν ως στόχο να διαπιστωθεί κατά πόσο είναι ευπαθείς οι δρομολογητές που είναι συνδεδεμένοι στο δίκτυο του οργανισμού, καθώς αν έστω και ένας να κινδυνεύει μέσω αυτού μπορεί να δεχτεί επίθεση όλο το δίκτυο.
- ✓ **Έλεγχος Ασφάλειας Εξυπηρετητών (Servers):** σκοπός είναι η εξέταση των χρησιμοποιούμενων εξυπηρετητών για τον εντοπισμό ενδεχόμενων ευπαθειών.

- ✓ **Έλεγχος Ασφάλειας Διαδικτυακών Εφαρμογών:** αξιολόγηση της ασφάλειας της υπό εξέτασης εφαρμογής για την εύρεση γνωστών αδυναμιών που μπορεί να οδηγήσουν στη διακύβευση της ασφάλειάς τους. Κατά την αξιολόγηση εκτελούνται οι παρακάτω ενέργειες:
    - **Εξέταση Μηχανισμών Αυθεντικοποίησης:** κατανόηση και εξέταση της διαδικασίας αυθεντικοποίησης η οποία έχει υιοθετηθεί από την εξεταζόμενη εφαρμογή**.**
    - **Διαχείριση Συνόδων:** εξετάζεται ο τρόπος με τον οποίο πραγματοποιείται η διαχείριση των συνόδων στην εξεταζόμενη εφαρμογή.
    - **Εξέταση Μηχανισμών Εξουσιοδότησης:** κατανόηση και έλεγχος των μηχανισμών εξουσιοδότησης που υλοποιούνται από την εφαρμογή.
    - **Επιχειρησιακή Λογική:** Εξέταση της εφαρμογής για τον εντοπισμό αδυναμιών στην επιχειρηματικής της λογική.
    - **Έλεγχος και Επικύρωση Δεδομένων:** έλεγχοι οι οποίοι απαιτούνται ώστε να διαπιστωθεί ότι τα δεδομένα τα οποία δέχεται σαν είσοδο η εξεταζόμενη εφαρμογή ελέγχονται και επικυρώνονται προτού ξεκινήσει η διαδικασία της επεξεργασίας τους. Τέτοιου είδους έλεγχοι είναι οι παρακάτω:
        - **Cross Site Scripting (XSS) Έλεγχοι:** εντοπισμός αδυναμιών τύπου XSS ώστε να διαπιστωθεί αν η τροποποίηση των παραμέτρων που δέχεται ως είσοδο η εφαρμογή μπορεί να οδηγήσει σε αποκάλυψη ευαίσθητων πληροφοριών.
        - **SQL Injection Έλεγχοι:** οι έλεγχοι που θα πραγματοποιηθούν στο συγκεκριμένο βήμα εστιάζονται στην εξέταση της πιθανότητας να εισαχθούν δεδομένα στην εφαρμογή με απώτερο στόχο την εκτέλεση ερωτημάτων SQL στη Βάση Δεδομένων (ΒΔ).
        - **LDAP Injection Έλεγχοι:** εφαρμογή ελέγχων με στόχο να διαπιστωθεί η δυνατότητα αποκάλυψης, τροποποίησης ή εισαγωγής ευαίσθητων πληροφοριών οι οποίες βρίσκονται σε υποδομές LDAP.
        - **XML Injection Έλεγχοι:** οι έλεγχοι που εκτελούνται εξετάζουν τη δυνατότητα εισαγωγής ενός εγγράφου XML με σκοπό την παραποίηση δεδομένων στην εφαρμογή.
        - **SSI Injection Έλεγχοι:** οι έλεγχοι αφορούν στην εξέταση του κώδικα των σελίδων HTML με σκοπό να διαπιστωθεί η δυνατότητα εισαγωγής κώδικα μέσα σε αυτές καθώς και η δυνατότητα εκτέλεσης του κώδικα από απόσταση.
        - **XPATH Injection Έλεγχοι:** οι έλεγχοι που πραγματοποιούνται επικεντρώνονται στο να εξετάσουν τη δυνατότητα εισαγωγής δεδομένων στην

εφαρμογή με σκοπό την εκτέλεση κατάλληλα διαμορφωμένων από τους χρήστες ερωτημάτων XPath.

- **IMAP/SMTP Injection Έλεγχοι:** εφαρμογή ελέγχων που αφορούν στην εξέταση της εφαρμογής ώστε να διαπιστωθεί η δυνατότητα εισαγωγής εντολών IMAP/SMTP και εκτέλεσής τους στους εξυπηρετητές ηλεκτρονικού ταχυδρομείου (mail servers).
- **Code Injection**: Εξέταση της εφαρμογής ώστε να διαπιστωθεί η δυνατότητα να δεχθεί ως δεδομένα εισόδου κάποιο τμήμα κώδικα το οποίο θα εκτελεστεί στον εξυπηρετητή.

- **Operation System (OS) Commanding Έλεγχοι:** εξέταση για να διαπιστωθεί η δυνατότητα εκτέλεσης τεχνικών οι οποίες επιτρέπουν την εισαγωγή εντολών λειτουργικού συστήματος ως δεδομένα εισόδου και την εκτέλεση τους στον εξυπηρετητή που φιλοξενεί το "server-side" της εφαρμογής
- **Buffer overflow Έλεγχοι:** έλεγχος ως προς διαφορετικούς τύπους αδυναμιών που σχετίζονται με απειλές buffer overflow (Heap overflow αδυναμίες, Stack overflow αδυναμίες, Format string αδυναμίες).
- **Έλεγχοι Υπηρεσιών Ιστού (Web Services)**
  - **Έλεγχος Συμμόρφωσης YI:** έλεγχος συμμόρφωσης των τεχνολογιών και των προτύπων των YI ως προς τις αντίστοιχες προδιαγραφές.
  - **Έλεγχος εγγράφων XML:** εξέταση των μηχανισμών διαχείρισης των εγγράφων XML (π.χ. μηχανισμοί δημιουργίας και επεξεργασίας) της εξεταζόμενης εφαρμογής ώστε να διαπιστωθεί ότι οι μηχανισμοί αυτοί σέβονται τόσο τη σημασιολογία του περιεχομένου όσο και τη δομή των εγγράφων.
  - **Έλεγχος Επιθέσεων Επανάληψης (Replay Attacks):** Εξέταση της εφαρμογής για να διαπιστωθεί η ανθεκτικότητά της σε επιθέσεις τύπου Επανάληψης (Replay Attacks).

✓ **Έλεγχος Ασφάλειας Βάσεων Δεδομένων:** οι συγκεκριμένοι έλεγχοι πραγματοποιούνται για την εξέταση της εξασφάλισης της ασφάλειας/διαθεσιμότητας των Β.Δ.

Βήμα 3: Δημιουργία λίστας με όλες τις αδυναμίες που εντοπίστηκαν

Σε αυτό το βήμα δημιουργείται μία λίστα με όλες τις αδυναμίες που εντοπίστηκαν από τα προηγούμενα βήματα.

Βήμα 4: Επισκόπηση των εντοπισμένων αδυναμιών για την εύρεση ψευδώς θετικών αδυναμιών

Ο βασικός σκοπός του συγκεκριμένου βήματος αποτελεί η αναλυτική επισκόπηση των αδυναμιών οι οποίες έχουν εντοπιστεί στο πλαίσιο των προηγούμενων βημάτων με στόχο τον προσδιορισμό ψευδώς θετικών ευρημάτων. Πρόκειται δηλαδή για ευρήματα τα οποία χαρακτηρίστηκαν λανθασμένα ως αδυναμίες εξαιτίας του γεγονότος ότι δεν λήφθηκαν υπόψη κάποιοι σημαντικοί παράμετροι του εξεταζόμενου αγαθού.

Βήμα 5: Δημιουργία της τελικής λίστας με τις αδυναμίες που εντοπίστηκαν

Στο συγκεκριμένο βήμα γίνεται ανασκόπηση των αδυναμιών που έχουν εντοπιστεί από τα εργαλεία ανίχνευσης, αναλύονται τα αποτελέσματα, αφαιρούνται τυχόν ψευδώς θετικές αδυναμίες που έχουν εντοπιστεί και δημιουργείται η τελική λίστα βασισμένη στην σημαντικότητα των αδυναμιών και την κρισιμότητα του κάθε αγαθού.

Βήμα 6: Προσδιορισμός σεναρίων

Σε αυτό το βήμα προσδιορίζονται τα σενάρια που περιγράφουν ενδεχόμενες περιπτώσεις εκμετάλλευσης των εντοπισμένων αδυναμιών.

Στάδιο 4ο: Δοκιμές Διείσδυσης

Το συγκεκριμένο στάδιο περιλαμβάνει μία σειρά δοκιμών διείσδυσης οι οποίες έχουν ως βασικό στόχο την επιβεβαίωση των αδυναμιών που εντοπίστηκαν στο προηγούμενο στάδιο[3]. Οι δοκιμές διείσδυσης εκτελούνται με βάση τα σενάρια που έχουν προσδιοριστεί στο τέλος του προηγούμενου σταδίου και περιλαμβάνουν τις εξής μεθόδους:

- ✓ Επιβεβαίωση των ευρημάτων με την απευθείας εξέταση των αγαθών που βρίσκονται υπό έλεγχο (δικτυακή αρχιτεκτονική, παρεχόμενες υπηρεσίες, τύποι λειτουργικών συστημάτων, καταγεγραμμένα γεγονότα στα συστήματα ασφάλειας κ.τ.λ.) για τη διασταύρωση των αποτελεσμάτων.
- ✓ Προσομοίωση επιθέσεων σε επίπεδο δικτύου, λειτουργικών συστημάτων, εξυπηρετητών κ.τ.λ. ώστε να διαπιστωθεί ότι οι αδυναμίες είναι εκμεταλλεύσιμες. Η πραγματοποίηση των επιθέσεων μπορεί να πραγματοποιηθεί με τους ακόλουθους τρόπους:

[3] Θα πρέπει να σημειωθεί ότι οι αδυναμίες που εντοπίστηκαν στο Στάδιο 2 δεν είναι στο σύνολό τους εκμεταλλεύσιμες.

- Με χρήση αυτοματοποιημένων εργαλείων εκτέλεσης επιθέσεων.
- Με την εκτέλεση κακόβουλου scripting κώδικα που μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των συστημάτων.

Στάδιο 5ο: Αξιολόγηση Ευρημάτων – Αποτίμηση Αδυναμιών

Η πρακτική αποτίμηση αδυναμιών ολοκληρώνεται με την καταγραφή των αποτελεσμάτων των δοκιμών διείσδυσης αξιολογώντας και παρουσιάζοντας τις πιθανές επιπτώσεις που μπορεί να έχει στον οργανισμό η εκμετάλλευση των εξεταζόμενων αδυναμιών.

Ο τρόπος που ακολουθείται για την αποτίμηση των αδυναμιών χωρίζεται στις παρακάτω ενέργειες:

- ✓ Καταγραφή των ευρημάτων / αποτελεσμάτων από τα εργαλεία πρακτικής αξιολόγησης.
- ✓ Επικοινωνία των άμεσα εμπλεκόμενων χρηστών (επικεφαλής ασφάλειας και διαχειριστές συστημάτων) για την αξιολόγηση των ευρημάτων / αποτελεσμάτων.
- ✓ Αντιστοίχιση των αδυναμιών με τα εξεταζόμενα αγαθά (Παράρτημα ΙΙ) και ανάθεση ενός βαθμού της κάθε αδυναμίας με βάση την κλίμακα του Πίνακα 31.
- ✓ Από την ανάθεση του βαθμού αποτίμησης αδυναμίας προκύπτει για κάθε αδυναμία και κάθε αγαθό το Επίπεδο της Πρακτικής Αποτίμησης Αδυναμιών, Practical Vulnerability Level $PV(A_i)$.

Μετά τον καθορισμό του $PV(A_i)$ και πριν τη συνολική αποτίμηση των αδυναμιών, θεωρητικής και πρακτικής, γίνεται επικοινωνία των αποτελεσμάτων με τις εμπλεκόμενες οντότητες για τον προσδιορισμό των αδυναμιών που απαιτούν άμεση διευθέτηση. Βασικό στόχο αποτελεί η πρόταση και υιοθέτηση συγκεκριμένων λύσεων για την άμεση αντιμετώπισή τους.

4.4.4.4 Βήμα 4.4: Συνολική Αποτίμηση Αδυναμιών

Το τελικό Επίπεδο Αποτίμησης Αδυναμιών (Final Vulnerability Level) των αγαθών υπολογίζεται με την βοήθεια του παρακάτω τύπου:

$$FV(A_i) = \max\left(TV(A_i), PV(A_i)\right) \quad (4.22)$$

δηλαδή το τελικό επίπεδο $FV(A_i)$ θα είναι το μέγιστο μεταξύ του Θεωρητικού, $TV(A_i)$, και του Πρακτικού Επιπέδου Αποτίμησης Αδυναμιών, $PV(A_i)$.

4.4.5 Φάση 5: Αποτίμηση επικινδυνότητας

Η αποτίμηση επικινδυνότητας των αγαθών του υπό εξέταση Πληροφοριακού Συστήματος, γίνεται με την βοήθεια του Βήματος 5.1 στην οποία υπολογίζεται το επίπεδο κινδύνου για κάθε αγαθό και του Βήματος 5.2 στην οποία προσδιορίζεται η επικινδυνότητα των αγαθών.

4.4.5.1 Βήμα 5.1: Υπολογισμός επιπέδων κινδύνου

Αφού έχουν ολοκληρωθεί οι προηγούμενες φάσεις και έχουν συλλεχθεί για όλα τα αγαθά, A_i, οι τιμές του επιπέδου αποτίμησης Επίπτωσης $I(A_i)$, Απειλής $T(A_i)$ και Αδυναμίας $FV(A_i)$, στο βήμα αυτό υπολογίζεται η τιμή του κινδύνου $R(A_i)$ του κάθε αγαθού. Πιο αναλυτικά, για κάθε τελικό βαθμό αποτίμησης επίπτωσης ενός αγαθού A_i, ως προς απώλεια Διαθεσιμότητας I_{un}, Εμπιστευτικότητας I_{dis} , και Ακεραιότητας I_{mod} υπολογίζονται οι τιμές των κινδύνων με την βοήθεια των παρακάτω τύπων:

Κίνδυνος ως προς απώλεια Διαθεσιμότητας:

$$R_{un}(A_i) = I_{un}(A_i) * T(A_i) * FV(A_i) \quad (4.23)$$

Κίνδυνος ως προς απώλεια Εμπιστευτικότητας:

$$R_{dis}(A_i) = I_{dis}(A_i) * T(A_i) * FV(A_i) \quad (4.24)$$

Κίνδυνος ως προς απώλεια Ακεραιότητας:

$$R_{mod}(A_i) = I_{mod}(A_i) * T(A_i) * FV(A_i) \quad (4.25)$$

Συνολικός Κίνδυνος:

$$R(A_i) = I(A_i) * T(A_i) * FV(A_i), \text{ όπου } I(A_i) = \max (I_{un}(A_i) , I_{dis}(A_i) , I_{mod}(A_i)) \quad (4.26)$$

Οι τιμές του $R(A_i)$ εξαρτώνται από τις διαφορετικές τιμές του επιπέδου αποτίμησης Επίπτωσης, Απειλής και Αδυναμίας. Όλες οι δυνατές τιμές του $R(A_i)$ αντιπροσωπεύουν την *Ετήσια Εκτιμώμενη Απώλεια (Annual Loss Expectancy)*, όπως φαίνονται στον Πίνακα 33.

Πίνακας 33: Πίνακας Επικινδυνότητας (Risk Level Evaluation Matrix)

ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ			ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Μ	Μ	Μ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ
			0,01	0,01	0,01	0,034	0,034	0,034	0,1	0,1	0,1	0,33	0,33	0,33	1	1	1
ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ			Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ
			0,33	0,66	1	0,33	0,66	1	0,33	0,66	1	0,33	0,66	1	0,33	0,66	1
ΕΠΙΠΤΩΣΗ	ΠΧ	10.000	33	66	100	112	224	340	330	660	1.000	1.089	2.178	3.300	3.300	6.600	10.000
	Χ	100.000	330	660	1.000	1.122	2.244	3.400	3.300	6.600	10.000	10.890	21.780	33.000	33.000	66.000	100.000
	Μ	1.000.000	3.300	6.600	10.000	11.220	22.440	34.000	33.000	66.000	100.000	108.900	217.800	330.000	330.000	660.000	1.000.000
	Υ	10.000.000	33.000	66.000	100.000	112.200	224.400	340.000	330.000	660.000	1.000.000	1.089.000	2.178.000	3.300.000	3.300.000	6.600.000	10.000.000
	ΠΥ	[4]100.000.000	330.000	660.000	1.000.000	1.122.000	2.244.000	3.400.000	3.300.000	6.600.000	10.000.000	10.890.000	21.780.000	33.000.000	33.000.000	66.000.000	100.000.000

[4] Για όλες τις τιμές χρησιμοποιείται το πάνω όριο. Για την τιμή "ΠΥ" του επιπέδου επίπτωσης, εφόσον δεν υπάρχει άνω όριο, χρησιμοποιείται η τιμή 100.000.000.

4.4.5.2 Βήμα 5.2: Προσδιορισμός Επικινδυνότητας

Στο Βήμα αυτό προσδιορίζεται η Επικινδυνότητα του κάθε αγαθού με βάση το αποτέλεσμα του προηγούμενου Βήματος και της κλίμακας Αποτίμησης Επικινδυνότητας του Πίνακα 34.

Πίνακας 34: Κλίμακα Αποτίμησης Επικινδυνότητας

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

Με χρήση λοιπόν της κλίμακας αυτής η τιμή του κινδύνου του κάθε αγαθού $R(A_i)$ μετατρέπεται σε Επικινδυνότητα, με όλες τις δυνατές τιμές όπως φαίνονται στον Πίνακα 35.

Πίνακας 35: Πίνακας Επικινδυνότητας (Risk Level Evaluation Matrix)

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

Με το βήμα αυτό ολοκληρώνεται η Φάση της Ανάλυσης Επικινδυνότητας των αγαθών του υπό εξέταση οργανισμού. Στην επόμενη Φάση προτείνονται μέτρα ασφάλειας και επιλέγονται τα μέτρα εκείνα τα οποία τελικά θα υλοποιηθούν από τη διοίκηση.

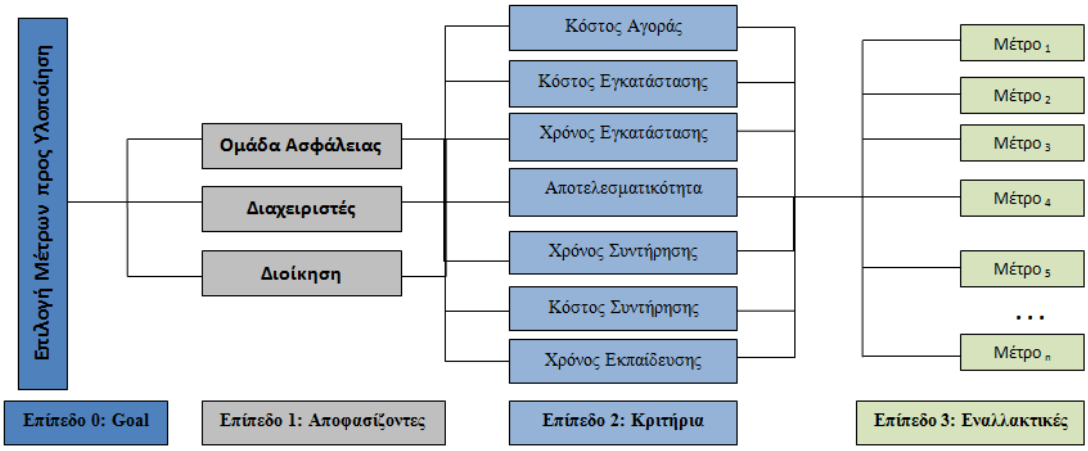
4.4.6 Φάση 6: Μέτρα προστασίας - Σχέδιο Ασφάλειας

4.4.6.1 Βήμα 6.1: Προτεινόμενα μέτρα ασφάλειας

Στην Φάση αυτή η μεθοδολογία προτείνει μια σειρά από μέτρα προστασίας για όλα τα αγαθά τα οποία προέκυψαν ως κρίσιμα από το προηγούμενο βήμα (Βήμα 5.2). Πιο συγκεκριμένα, λαμβάνοντας υπόψη τα υπάρχοντα μέτρα προστασίας (Βήμα 1.4 Υπάρχουσα Κατάσταση), η μεθοδολογία προτείνει για τα αγαθά που έχουν χαρακτηριστεί ως κρίσιμα (Επικινδυνότητα = ΠΥ), μια σειρά από μέτρα προστασίας βασισμένα στο ISO 27001 [16], τα οποία είναι τεχνικά, διοικητικά και οργανωτικά μέτρα προστασίας. Τα μέτρα προστασίας χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των αγαθών που καλούνται να προστατέψουν. Ενδεικτικά αναφέρεται ότι προτείνονται διάφορα μέτρα προστασίας κτιριακών εγκαταστάσεων, μέτρα σχετικά με τη διαθεσιμότητα, μέτρα σχετικά με την εμπιστευτικότητα, μέτρα σχετικά με την ακεραιότητα καθώς και μέτρα εκπαίδευσης προσωπικού.

4.4.6.2 Βήμα 6.2: Επιλογή κατάλληλων μέτρων ασφάλειας

Στην φάση αυτή, θα επιλεγούν ποια από τα προτεινόμενα μέτρα προστασίας θα υλοποιηθούν. Για την επιλογή των μέτρων θα χρησιμοποιηθεί ο αλγόριθμος της AHP όπου θα συμμετέχουν χρήστες από τις ομάδες *Ομάδα Ασφάλειας, Διαχειριστές* και *Διοίκηση* (όπως φαίνεται στην Εικόνα 14).



Εικόνα 14: Δένδρο Απόφασης AHP για την επιλογή των μέτρων προς υλοποίηση

Τα κριτήρια αξιολόγησης, K_i , των προτεινόμενων μέτρων για κάθε αγαθό είναι:

- ✓ K_1: κόστος αγοράς,
- ✓ K_2: κόστος εγκατάστασης,

- ✓ K_3: χρόνος εγκατάστασης,
- ✓ K_4: αποτελεσματικότητα,
- ✓ K_5: χρόνος συντήρησης,
- ✓ K_6: κόστος συντήρησης,
- ✓ K_7: χρόνος εκπαίδευσης.

Κάθε χρήστης θα μπορεί να ιεραρχήσει τα προτεινόμενα μέτρα για κάθε αγαθό. Οι ατομικές αυτές προτιμήσεις λαμβάνονται υπόψη στο ομαδικό δένδρο απόφασης ώστε τελικά να προκύψουν τα μέτρα που θα υλοποιηθούν. Με τον τρόπο αυτό λαμβάνονται υπόψη οι γνώμες των συμμετεχόντων, οι οποίες μπορεί να είναι διαφορετικές τόσο ως προς την βαρύτητα των κριτηρίων, όσο και ως προς τις τελικές τους επιλογές. Για παράδειγμα, τα μέλη της ομάδας *Διοίκηση* μπορεί να δίνουν μεγαλύτερη βαρύτητα στα κριτήρια *Κόστος Αγοράς, Κόστος Εγκατάστασης* και *Χρόνος Εκπαίδευσης,* τα μέλη της *Ομάδας Ασφάλειας* να ενδιαφέρονται περισσότερο για την *Αποτελεσματικότητα* των μέτρων και τον *Χρόνο Εγκατάστασης* και, τέλος, τα μέλη της ομάδας *Διαχειριστές* να δίνουν προτεραιότητα στον *Χρόνο Εγκατάστασης* και *Συντήρησης*. Έτσι, με την χρήση του δένδρου απόφασης της AHP (Εικόνα 14), οδηγούμαστε σε ομαδική απόφαση για την επιλογή των προτεινόμενων μέτρων προς υλοποίηση, καθώς γίνεται η ιεράρχηση των εναλλακτικών μέτρων για κάθε αγαθό λαμβάνοντας υπόψη διαφορετικά κριτήρια και ατομικές προτεραιότητες.

Τα αποτελέσματα της παραπάνω διαδικασίας οδηγούν σε μια λίστα με όλα τα μέτρα ανάλογα με τον *βαθμό υλοποίησής* τους ως εξής:

- ✓ άμεση υλοποίηση,
- ✓ προτεινόμενο για υλοποίηση,
- ✓ υπό συζήτηση,
- ✓ μη εφαρμόσιμο.

Η λίστα αυτή συμπεριλαμβάνεται στην αναφορά κατάλληλων μέτρων προστασίας (Φάση 7) σύμφωνα με το υπόδειγμα του βρίσκεται στο Παράρτημα V.

4.4.7 Φάση 7: Αναφορές Ανάλυσης Επικινδυνότητας

Στην τελευταία αυτή Φάση υπάρχει η δυνατότητα δημιουργίας όλων των αποτελεσμάτων από κάθε φάση και επιμέρους βήμα της μεθοδολογίας με μορφή αναφοράς. Πιο συγκεκριμένα, εδώ δημιουργούνται:

- ✓ Η λίστα αγαθών και των αλληλεξαρτήσεων.

- ✓ Η Αναφορά Ανάλυσης Επικινδυνότητας.
- ✓ Η Αναφορά κατάλληλων μέτρων προστασίας.

Όλες οι αναφορές δημιουργούνται σύμφωνα με το υπόδειγμα του βρίσκεται στο Παράρτημα V.

4.5 Συμπεράσματα κεφαλαίου

Στο συγκεκριμένο κεφάλαιο παρουσιάστηκε η προτεινόμενη μεθοδολογία STORM-RM, οι φάσεις οι οποίες την υλοποιούν καθώς και τα επιμέρους βήματά τους. Πρόκειται για μια μεθοδολογία η οποία έχει στόχο την μείωση των ερωτηματολογίων με την χρήση του μοντέλου αγαθών το οποίο χρησιμοποιεί (κάθε χρήστης καλείται να αποτιμήσει τα αγαθά με τα οποία συνδέεται) και ταυτόχρονα με την συλλογή γνώσης από όλους τους εμπλεκόμενους χρήστες, μεθοδολογία η οποία οδηγεί σε αποτελέσματα προσδιορισμού και αντιμετώπισης κινδύνου τα οποία ανταποκρίνονται στην πραγματική κατάσταση του υπό εξέταση ΠΣ.

Επίσης, ο τρόπος με τον οποίο είναι δομημένες οι φάσεις και τα βήματα της μεθοδολογίας επιτρέπουν την εύκολη υλοποίησή της σε αυτοματοποιημένο εργαλείο το οποίο θα διευκολύνει ακόμη περισσότερο τους χρήστες των υπό εξέταση οργανισμών. Προς την κατεύθυνση αυτή κινείται το κεφάλαιο που ακολουθεί, το οποίο περιγράφει το συνεργατικό περιβάλλον διαχείρισης ασφάλειας STORM-RM και τον τρόπο με τον οποίο η προτεινόμενη μεθοδολογία θα παρέχεται σαν υπηρεσία μέσα από αυτό.

4.6 Βιβλιογραφία 4ου Κεφαλαίου

[1] AS/NZS 4360. Risk management standards australia. Strathfield, 1999.

[2] BugTraq, http://seclists.org/ (accessed August 2012).

[3] Business Process Modeling Notation (BPMN), http://www.bpmn.org/ (accessed August 2012).

[4] Club de la Securite de L' information Francais Methods Commision, Mehari 2010 Risk analysis and treatment Guide, France, August 2010, http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk- Analysis-and-Treatment-Guide.pdf (accessed December 2011)

[5] Common Vulnerability and Exposures, http://cve.mitre.org/ (accessed August 2012).

[6] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Books I – The Method", Ministerio de Administraciones Publicas, June 2006.

[7] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Book II – Catalogue of Elements", Ministerio de Administraciones Publicas, June 2006.

[8] Crespo F., Gomez M., Candau J., and Manas J.A., "MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Book III – Techniques", Ministerio de Administraciones Publicas, June 2006.

[9] Green Paper on a European Programme for Critical Infrastructure Protection, Commission of the European Communities, COM (2005) 576 final, Brussels, November 17, 2005.

[10] IBM Internet Security Systems (ISS X Force), http://www.iss.net/ (accessed August 2012).

[11] Information Systems Security Assessment Framework, Open Information Systems Security Group (OISSG), http://www.oissg.org/issaf (accessed August 2012).

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

[13] ISO/IEC 27004:2009: Information Technology - Security techniques - Information security management - Measurement, 2009.

[14] ISO/IEC 15408-1:2009: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 2009.

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

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

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

[18] NIST's National Vulnerability Database, http://nvd.nist.gov/ (accessed August 2012).

[19] Ntouskas, T. and Polemi, N. (2012) 'STORM-RM: a collaborative and multicriteria risk management methodology', Int. J. Multicriteria Decision Making, Vol. 2, No. 2, pp.159–177.

[20] Ntouskas T., Kotzanikolaou P., Polemi N., "Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach", in Proc. of the 1st International Symposium & 10th Balkan Conference on Operational Research, Thessaloniki, Greece, September 2011.

[21] OCTAVE. http://www.gnu.org/software/octave/(accessed December 2011).

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

[23] OMG (Object Management Group), http://www.omg.org/, (accessed August 2012).

[24] Open Source Security Testing Methodology Manual, Institute for Security and Open Methodologies (ISECOM), http://www.isecom.org/osstmm/**,** (accessed August 2012).

[25] Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, National Institute for Standards and Technology, USA, July 2002.

[26] Saaty, T. L. "Decision making with the analytic hierarchy process", Int. J. Service Sciences, Vol. 1, No I, pp. 83-98, 2008.

[27] Saaty, T. L. "The Analytic Hierarchy Process", McGraw-Hill, New York, 1980

[28] Security focus, http://www.securityfocus.com/ (accessed August 2012).

[29] The Open Web Application Security Project, https://www.owasp.org (accessed August 2012).

[30] Unified Modeling Language (UML), http://www.uml.org/ (accessed August 2012).

[31] Web Application Security Consortium (WASC), Wasc Threat Classification, http://www.webappsec.org/ (accessed August 2012).

Κεφάλαιο 5ο

5 Συνεργατικό περιβάλλον διαχείρισης ασφάλειας (STORM)

5.1 Εισαγωγή

Η αποτελεσματικότερη διαχείριση της ασφάλειας πληροφοριακών συστημάτων μπορεί να πραγματοποιηθεί με την σχεδίαση και την ανάπτυξη καινοτόμων εφαρμογών οι οποίες βασίζονται σε νέα διαδραστικά πλαίσια. Τα πλαίσια αυτά έχουν την δυνατότητα να ικανοποιήσουν καινούριες προκλήσεις και να ανταπεξέλθουν αποφασιστικά στις αυξανόμενες ανάγκες των σημερινών πολυδιάστατων ως προς την υποκείμενη τεχνολογική υποδομή οργανισμών.

Η πρώτη βασική πτυχή που τα πλαίσια αυτά καλούνται να διευθετήσουν είναι η απαίτηση για ουσιαστική διαχείριση και για αποτελεσματικό συνδυασμό της γνώσης και της πληροφορίας που οι οργανισμοί διαθέτουν με στόχο τη διαμόρφωση ενός ολοκληρωμένου πλαισίου ασφάλειας και διαχείρισης της επικινδυνότητας. Η κατανεμημένη όμως φύση των συγκεκριμένων οργανισμών, η οποία χαρακτηρίζεται από στοιχεία όπως είναι το πλήθος και η πολυπλοκότητα των διαθέσιμων συστημάτων και υπηρεσιών, η χωρογραφική τους διασπορά αλλά και ο σημαντικά μεγάλος αριθμός χρηστών και διαχειριστών, καθιστά τη συλλογή και την επεξεργασία της διαθέσιμης γνώσης μια διαδικασία εξαιρετικά επίπονη και χρονοβόρα. Η χρήση πλαισίων που βασίζονται σε τεχνολογίες που προάγουν την συνεργατικότητα, όπως για παράδειγμα οι τεχνολογίες Ιστού 2.0, αποτελεί την βέλτιστη συνεισφορά στην συγκεκριμένη πρόκληση.

Η συνεργατικότητα αποτελεί μια παράμετρο η οποία πρέπει να διευθετηθεί στα νέα γενιάς περιβάλλοντα διαχείρισης ασφάλειας. Βασικός της στόχος είναι η ενίσχυση και η διευκόλυνση της επικοινωνίας μεταξύ των εμπλεκόμενων οντοτήτων που επιτρέπει την υπερπήδηση εμποδίων που προκύπτουν από την εφαρμογή χρονοβόρων διαδικασιών. Το στοιχείο αυτό ευνοεί σημαντικά τη βελτίωση του χρόνου απόκρισης και αντιμετώπισης ζητημάτων με τρόπο γρήγορο και αποτελεσματικό. Παράλληλα, επιτρέπει την δημιουργία ευέλικτων συνεργατικών ομάδων εργασίας επιτρέποντάς τους να λειτουργήσουν μεθοδικά και συστηματικά. Στο πλαίσιο αυτό, οι συγκεκριμένες ομάδες μπορεί να αποτελέσουν ένα κρίσιμο παράγοντα για την διαμόρφωση ενός αποδεκτού επιπέδου ασφάλειας και αξιοπιστίας.

Η δεύτερη πτυχή την οποία τα πλαίσια πρέπει να αντιμετωπίσουν σχετίζεται με την αποτελεσματική αναπαράσταση των επιχειρησιακών διαδικασιών των οργανισμών. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό για οργανισμούς οι οποίοι εξαιτίας του μεγέθους και της πολυπλοκότητας της υποδομής τους είναι εξαιρετικά δύσκολο να προσδιορίσουν και να οριοθετήσουν τα κρισιμότερα συστατικά της τα οποία σχετίζονται άμεσα με την σημαντικότητα των επιχειρησιακών διαδικασιών που αυτά υποστηρίζουν. Για τον λόγο αυτό, η οπτικοποίηση των διαθέσιμων διαδικασιών των οργανισμών προσφέρει ένα εύχρηστο και φιλικό εννοιολογικό περιβάλλον που επιτρέπει την καλύτερη κατανόηση τόσο της λογικής της ίδιας της διαδικασίας όσο και των συστατικών από τα οποία αυτή απαρτίζεται. Με τον τρόπο αυτό, διευρύνεται η αντίληψη των χρηστών όσον αφορά στα σημεία της διαδικασίας αλλά και αντίστοιχα της υποδομής τους στα οποία πρέπει να δοθεί ιδιαίτερη έμφαση.

Η υιοθέτηση από μέρους των οργανισμών μίας εφαρμογής διαχείρισης της ασφάλειας και της επικινδυνότητας, η οποία θα ικανοποιεί τις προαναφερόμενες απαιτήσεις, προσφέρει στους οργανισμούς αυτούς μια σειρά πλεονεκτημάτων τα οποία συνοψίζονται στα ακόλουθα:

- ✓ αποτελεσματικότερη αποτύπωση και καταγραφή των κρίσιμων υπηρεσιών της υποκείμενης υποδομής, των εξαρτώμενων αγαθών όπως, επίσης, και των εφαρμοζόμενων μέτρων ασφάλειας,
- ✓ ευέλικτη αποτίμηση των επιπτώσεων που επιφέρει η παραβίαση της ασφάλειας των επιμέρους συστατικών της υποδομής,
- ✓ ακριβέστερη αποτίμηση της τρωτότητας των σύνθετων συστημάτων και υποδομών,
- ✓ σαφή καθορισμό των απειλών που αντιμετωπίζουν οι υποδομές,
- ✓ καθορισμό της επικινδυνότητας και της κρισιμότητας των επιμέρους συστατικών μιας υποδομής με αντικειμενικότερα κριτήρια, και
- ✓ προσδιορισμό των μέτρων ασφάλειας που ικανοποιούν σε μεγαλύτερο βαθμό τις απαιτήσεις ασφάλειας των συστημάτων, ενώ, παράλληλα, αντιμετωπίζουν με αποτελεσματικότερο τρόπο τους κινδύνους που αυτά αντιμετωπίζουν.

Το προτεινόμενο συνεργατικό περιβάλλον STORM (Secure Tool for Risk Management) θέτει ως πρωταρχικό του στόχο την διευθέτηση των απαιτήσεων αυτών με τη χρήση συνεργατικών πλαισίων που βασίζονται σε τεχνολογίες Ιστού 2.0 (Web 2.0), αλλά και την υιοθέτηση σύγχρονων αυτοματοποιημένων, ανοιχτών, διαδραστικών και αξιόπιστων τεχνολογικών εργαλείων όπως είναι τα συστήματα διαχείρισης επιχειρησιακών διαδικασιών.

Στο κεφάλαιο αυτό παρουσιάζονται οι δυνατότητες των συνεργατικών περιβαλλόντων, καταγράφονται οι απαιτήσεις τις οποίες καλείται το προτεινόμενο περιβάλλον διαχείρισης

ασφάλειας STORM να ικανοποιήσει και, στην συνέχεια, παρουσιάζεται η αρχιτεκτονική η οποία επιλέχθηκε καθώς και οι υπηρεσίες οι οποίες παρέχονται από το STORM.

5.2 Συνεργατική Διαχείριση Κινδύνων (ΔΚ)

Το περιβάλλον STORM πρόκειται να αποτελέσει ένα πρότυπο εργαλείο για την διαχείριση ασφάλειας των Πληροφοριακών Συστημάτων προσφέροντας υπηρεσίες οι οποίες θα διευκολύνουν την συνεργατική διαχείριση της ασφάλειας στα υπό εξέταση Πληροφοριακά Συστήματα. Για το λόγο αυτό, κρίνεται αναγκαίο να χρησιμοποιηθούν συνεργατικές τεχνολογίες Ιστού 2.0. Πιο συγκεκριμένα, το STORM θα πρέπει να παρέχει υπηρεσίες όπως forum, chat rooms οι οποίες θα διευκολύνουν την συνεργατικότητα και την ανταλλαγή απόψεων και ιδεών σε θέματα ασφάλειας ΠΣ, ενώ ταυτόχρονα θα είναι σε θέση να βοηθήσουν τους χρήστες στην άμεση εύρεση λύσεων τυχόν καθημερινών προβλημάτων ασφάλειας. Ταυτόχρονα, απαραίτητη είναι η ύπαρξη wikis και ηλεκτρονικής βιβλιοθήκης ώστε να ενημερώνονται οι χρήστες του συστήματος πάνω σε θέματα ασφάλειας ΠΣ ενώ παράλληλα να βρίσκουν πληροφορίες και οδηγίες για την αντιμετώπιση κινδύνων, για διαδικασίες ασφάλειας και για εργαλεία καθώς και αναλυτικές οδηγίες για την πρακτική ανάλυση των ευπαθειών των αγαθών του υπό εξέταση Πληροφοριακού Συστήματος. Τέλος, απαραίτητη κρίνεται και η ύπαρξη υπηρεσίας καταγραφής-σχεδίασης επιχειρησιακών διαδικασιών για την αποτύπωση των επιχειρησιακών διαδικασιών του υπό εξέταση οργανισμού.

5.3 Απαιτήσεις συνεργατικού περιβάλλοντος STORM

Για την αποτελεσματική επιλογή των τεχνολογιών υλοποίησης του περιβάλλοντος STORM απαιτείται ο σαφής καθορισμός των απαιτήσεων που καλείται να ικανοποιεί. Μεταξύ άλλων, θα πρέπει να καλύπτονται και οι απαιτήσεις του προτύπου ISO / IEC 9126-1:2001 [5] για την ποιότητα του λογισμικού, οι οποίες περιγράφονται στις ενότητες που ακολουθούν.

5.3.1 Ασφάλεια

Είναι πολύ σημαντικό να υποστηρίζονται βασικές και προηγμένες υπηρεσίες ασφάλειας κατά την πρόσβαση και την χρήση των υπηρεσιών, εφόσον μέσω της εφαρμογής θα υπάρχει πρόσβαση σε πολύ σημαντική πληροφορία. Για παράδειγμα, στην υπηρεσία μέσω της οποίας θα αποτιμάται η επίπτωση των κρίσιμων υπηρεσιών των ΠΣ θα είναι απαραίτητη η καταγραφή των υπηρεσιών, των αγαθών και των δεδομένων τα οποία διαχειρίζεται, τα οποία μπορεί να είναι δεδομένα εμπορικά,

μισθολογικά κτλ. Σε πρώτο επίπεδο θα πρέπει οι υπηρεσίες να επιβάλλουν την εγγραφή του χρήστη και την αναλυτική καταγραφή υπηρεσιών και των συστατικών τους. Θα πρέπει επιπλέον να δοθεί μεγάλη προσοχή τόσο σε τεχνικά όσο και σε νομοθετικά ζητήματα ασφάλειας που αφορούν:

- ✓ Στον τρόπο αναγνώρισης, ταυτοποίησης και αυθεντικοποίησης των χρηστών.
- ✓ Στον έλεγχο πρόσβασης των ήδη αυθεντικοποιημένων χρηστών σε διαφορετικά υποσυστήματα ή δεδομένα, με δικαιώματα πρόσβασης ανάλογα με το ρόλο του κάθε χρήστη και την ανάγκη γνώσης.
- ✓ Στην ανταλλαγή και διατήρηση κρίσιμων για τον οργανισμό δεδομένων, με τρόπο ο οποίος εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων.
- ✓ Στην προστασία των αποτελεσμάτων της διαχείρισης ασφάλειας των ΠΣ.
- ✓ Στην προστασία της ιδιωτικότητας της πληροφορίας που ανταλλάσσουν οι χρήστες μέσω των συνεργατικών υπηρεσιών (Forum, Wiki, Chat Room), οι οποίες μπορεί να περιέχουν στοιχεία για την εσωτερική λειτουργία του οργανισμού.

5.3.2 Επεκτασιμότητα

Το περιβάλλον STORM θα ήταν αναγκαίο να μπορεί να επεκταθεί και παραμετροποιηθεί ώστε να εφοδιαστεί με τυχόν νέες υπηρεσίες και να μπορέσει να χρησιμοποιηθεί από διαφορετικού είδους και πολυπλοκότητας οργανισμούς.

5.3.3 Διαλειτουργικότητα

Το συνεργατικό περιβάλλον STORM θα πρέπει να υποστηρίζει την διαλειτουργικότητα και την διασυνδεσιμότητα με άλλα περιβάλλοντα, εργαλεία (π.χ. εργαλεία ανάλυσης επιχειρησιακών διαδικασιών, εργαλεία ανίχνευσης εισβολών) και υπηρεσίες άλλων φορέων ή οργανισμών σχετικών με τον τομέα της ασφάλειας πληροφοριακών συστημάτων.

5.3.4 Απλότητα στην χρήση

Θα πρέπει να σχεδιαστεί λαμβάνοντας υπόψη το επίπεδο γνώσης των χρηστών. Οι τεχνικές που θα χρησιμοποιηθούν πρέπει να αποσκοπούν στην όσο το δυνατόν πιο εύκολη αντίληψη και ερμηνεία των ενεργειών του κάθε συστατικού. Αντίστοιχα, οι οθόνες εργασίας θα πρέπει να είναι εύχρηστες, και με μηνύματα καθοδήγησης των χρηστών όπου χρειάζεται, ώστε να επιτυγχάνεται η ανταλλαγή της απαραίτητης πληροφορίας με όσο το δυνατό πιο κατανοητό τρόπο.

5.3.5 Εικονοποίηση

Γραφικές αναπαραστάσεις θα χρησιμοποιούνται όσο είναι εφικτό για να διευκολύνουν τον χρήστη στην ταχύτερη απεικόνιση αποτελεσμάτων (π.χ. ροές υπηρεσιών, στατιστικά αποτελέσματα).

5.3.6 Αισθητική

Θα πρέπει να επιλεχθούν γραμματοσειρές και χρώματα με στόχο να ξεκουράζουν και να παροτρύνουν τον χρήστη να παραμείνει στο σύστημα όσο χρειάζεται, προκειμένου να ολοκληρώσει τις τυχόν διεργασίες στις οποίες εμπλέκεται αλλά και να αποκτήσει την απαραίτητη πληροφορία που θα προσφέρουν οι υπηρεσίες του STORM .

5.3.7 Ευκολία στην εκμάθηση

Το συνεργατικό περιβάλλον STORM θα πρέπει να υποστηρίζεται από τις εξής βασικές γενικές αρχές :

- ✓ **Προβλεψιμότητα (predictability):** Όλες οι σελίδες θα πρέπει να σχεδιαστούν ακολουθώντας τα ίδια λογικά βήματα ώστε από τη στιγμή που ο χρήστης ασχοληθεί με μία από αυτές και κατανοήσει τη λογική της να είναι σε θέση να την εφαρμόσει και στις υπόλοιπες.
- ✓ **Συνέπεια (consistency):** Σε όλα τα συστατικά του συστήματος θα πρέπει να χρησιμοποιούνται οι ίδιες συμβάσεις (ομοιομορφία στην εμφάνιση των δεδομένων του συστήματος). Σε όλες τις σελίδες θα πρέπει να χρησιμοποιηθούν οι ίδιες αναπαραστάσεις για το ίδιο συστατικό. Δεν θα ήταν εύχρηστο να αλλάζουν θέση στην οθόνη ή να αλλάζουν τα ίδια τα κουμπιά.

5.3.8 Αποφυγή σύγχυσης του χρήστη

Θα πρέπει να δίνονται αρκετές επιλογές στο χρήστη ώστε να χρησιμοποιήσει όλες τις δυνατότητες του συστήματος. Η σύγχυση του χρήστη πρέπει να αποφεύγεται ακολουθώντας τις τακτικές οι οποίες έχουν εφαρμοστεί διεθνώς στην ανάπτυξη ιστοσελίδων, με τη χρήση δηλαδή μεγάλων γραμμάτων, απλών εννοιών και πολλαπλών μενού για βοήθεια στην περιήγηση.

5.3.9 Δυνατότητα αποφυγής λαθών και εύκολης διαχείρισης λαθών

Θα πρέπει να έχουν προβλεφθεί όλοι οι απαραίτητοι έλεγχοι αποφυγής λαθών των χρηστών οι οποίοι παραβιάζουν το σχεδιασμό του συστήματος. Με κατάλληλα μηνύματα λαθών θα πρέπει να ειδοποιείται ο χρήστης για την σωστή διεκπεραίωση της διεργασίας.

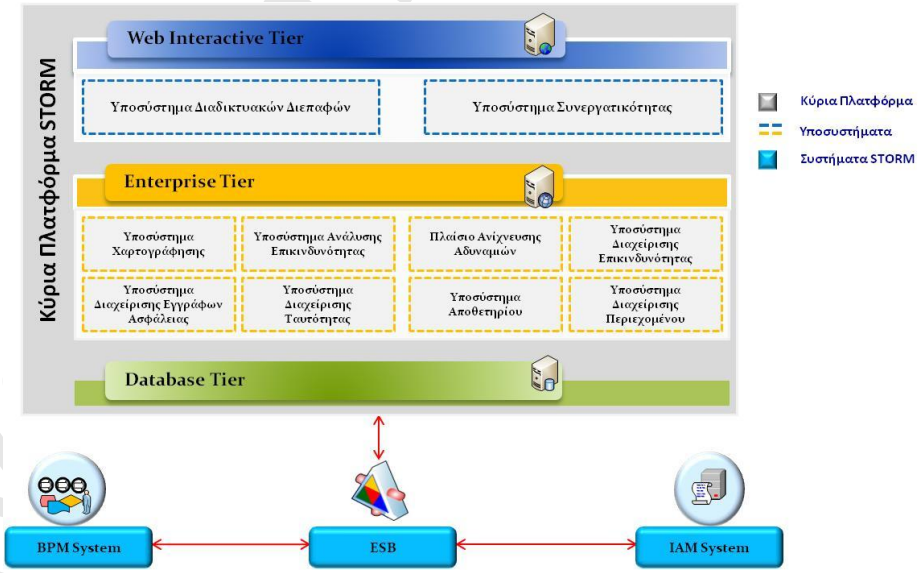
5.4 Αρχιτεκτονική και Τεχνολογίες του STORM

Λαμβάνοντας υπόψη τις απαιτήσεις της προηγούμενης ενότητας, έγινε η επιλογή των τεχνολογιών και της αρχιτεκτονικής του STORM [7], η οποία παρουσιάζεται στις ενότητες που ακολουθούν βάσει του προτύπου RM-ODP [3][9][12]. Συγκεκριμένα, η αρχιτεκτονική η οποία επιλέχθηκε για την υλοποίηση του συνεργατικού περιβάλλοντος STORM (Εικόνα 15) αποτελείται από τέσσερις (4) βασικές οντότητες:

- ✓ την *Κύρια Πλατφόρμα***,**
- ✓ τον *Δίαυλο Επιχειρησιακών Υπηρεσιών (ESB),*
- ✓ το *Σύστημα Διαχείρισης Ταυτοτήτων (Identity & Access Management System - IAM)* και
- ✓ το *Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών (BPM System).*

Η Κύρια Πλατφόρμα είναι υπεύθυνη για την παροχή των βασικών υπηρεσιών STORM (5.6 Υπηρεσίες STORM), ενώ τα συστήματα **Δ**ιαχείρισης Ταυτοτήτων και Διαχείρισης Επιχειρησιακών Διαδικασιών λειτουργούν υποστηρικτικά και η επικοινωνία τους με την Κύρια Πλατφόρμα γίνεται μέσω του Δίαυλου Επιχειρησιακών Υπηρεσιών.

Με την επιλογή της συγκεκριμένης αρχιτεκτονικής (κάνοντας χρήση ενδιάμεσου επιπέδου - Δίαυλος Επιχειρησιακών Υπηρεσιών) επιτυγχάνεται η διαλειτουργικότητα και η ασφαλής επικοινωνία των εξωτερικών συστημάτων με την Κύρια Πλατφόρμα ενώ, ταυτόχρονα, δίνεται η δυνατότητα σύνδεσης οποιοδήποτε άλλου εξωτερικού συστήματος χρειαστεί σε μελλοντικές επεκτάσεις του συνεργατικού περιβάλλοντος STORM.



Εικόνα 15: Αρχιτεκτονική συνεργατικού περιβάλλοντος STORM

Στις ενότητες που ακολουθούν περιγράφονται οι κύριες οντότητες καθώς και τα επιμέρους υποσυστήματα από τα οποία αποτελείται κάθε οντότητα του περιβάλλοντος STORM.

5.4.1 Κύρια Πλατφόρμα

Η βασική οντότητα του συνεργατικού περιβάλλοντος είναι η Κύρια Πλατφόρμα, η οποία βασίζεται σε αρχιτεκτονική τριών επιπέδων (three tier) και αποτελείται από:

- ✓ το Δικτυακό-Διαδραστικό Επίπεδο (Web Interactive Tier),
- ✓ το Επιχειρησιακό Επίπεδο (Enterprise Tier), και
- ✓ το Επίπεδο Βάσης Δεδομένων (Database Tier).

Η Κύρια Πλατφόρμα είναι υλοποιημένη στο πλαίσιο PHP Symfony 1.0 Framework [11] και απαιτεί εξυπηρετητή Apache [1].

Στις ενότητες που ακολουθούν παρουσιάζεται κάθε ένα από τα επίπεδα αυτά, καθώς και τα υποσυστήματα από τα οποία αποτελούνται.

5.4.1.1 Δικτυακό-Διαδραστικό Επίπεδο (Web Interactive Tier)

Το *Δικτυακό - Διαδραστικό Επίπεδο* είναι υπεύθυνο για το γραφικό περιβάλλον των τελικών χρηστών του συνεργατικού περιβάλλοντος και την προβολή του STORM περιεχομένου με φιλικό και εύχρηστο τρόπο. Το επίπεδο αυτό (Εικόνα 16) αποτελείται από δύο υποσυστήματα: το *Υποσύστημα Διαδικτυακών Διεπαφών* και το *Υποσύστημα Συνεργατικότητας* τα οποία περιγράφονται αναλυτικά στις επόμενες ενότητες.

Εικόνα 16: Δικτυακό - Διαδραστικό Επίπεδο

5.4.1.1.1 Υποσύστημα Διαδικτυακών Διεπαφών

Το *Υποσύστημα Διαδικτυακών Διεπαφών* είναι υπεύθυνο για την παρουσίαση της λειτουργικότητας όλων των υποσυστημάτων προς τις ομάδες των χρηστών. Συγκεκριμένα, περιλαμβάνει διαδραστικά εργαλεία όπως δυναμικές ιστοσελίδες και φόρμες αναζήτησης, τα οποία εξυπηρετούν τον χρήστη να εισάγει δεδομένα και να αναζητήσει πληροφορίες στο σύστημα STORM. Αυτό το υποσύστημα αναλαμβάνει την κατάλληλη προώθηση της πληροφορίας που εισάγεται από το χρήστη, μέσω

ανταλλαγής των απαραίτητων μηνυμάτων προς τα υπόλοιπα υποσυστήματα, ώστε να εξασφαλίζεται η εξουσιοδοτημένη και συνεπής λειτουργία του συστήματος STORM.

5.4.1.1.2 Υποσύστημα Συνεργατικότητας

Το *Υποσύστημα Συνεργατικότητας* είναι υπεύθυνο για την ενίσχυση της επικοινωνίας, της ενημέρωσης και της ενασχόλησης με την ασφάλεια ΠΣ των διαφορετικών ομάδων χρηστών (5.5 Ομάδες Χρηστών STORM). Το υποσύστημα αυτό παρέχει τις συνεργατικές υπηρεσίες (5.6.3 Συνεργατικές Υπηρεσίες STORM) αξιοποιώντας τις τεχνολογίες Web 2.0 και απαρτίζεται από forum, wiki, chat rooms και blogs, τα οποία αποτελούν και τα 4 διαφορετικά υποσυστήματα συνεργατικότητας.

Υποσύστημα Φόρουμ. Το Υποσύστημα Φόρουμ (message board/forum) είναι μια διαδικτυακή ιστοσελίδα συζητήσεων όπου οι χρήστες μπορούν να επικοινωνούν για διάφορα θέματα υπό τη μορφή δημοσιεύσεων ή αναρτήσεων για θέματα ασφάλειας των ΠΣ. Πιο συγκεκριμένα, τα χαρακτηρηστικά του υποσυστήματος είναι:

- ✓ Οι διάφορες θεματικές ενότητες είναι ομαδοποιημένες σε τόπους συζήτησης οι οποίοι, με την σειρά τους, είναι ομαδοποιημένοι σε κατηγορίες.
- ✓ Εύκολη πλοήγηση μεταξύ των θεματικών ενοτήτων.
- ✓ Ειδοποίηση των χρηστών μέσω RSS για την ύπαρξη νέων θεμάτων ή συζητήσεων.
- ✓ Δυνατότητα διαγραφής μηνυμάτων και κλειδώματος συζητήσεων από τον διαχειριστή.

Υποσύστημα Wiki. Το Υποσύστημα Wiki επιτρέπει στις διάφορες ομάδες χρηστών να δημιουργήσουν και να επεξεργαστούν ιστοσελίδες με στόχο την ενημέρωση και την εκπαίδευση πάνω σε θέματα ασφάλειας ΠΣ. Πιο αναλυτικά, το υποσύστημα αυτό είναι υπεύθυνο για:

- ✓ Δημιουργία / Επεξεργασία σελίδων με αυτόματη διαχείριση εκδόσεων.
- ✓ Διατήρηση ολόκληρου του ιστορικού επεξεργασίας των σελίδων.
- ✓ Γραφική αναπαράσταση των διαφορών μεταξύ διαφορετικών εκδόσεων μιας σελίδας.
- ✓ Προεπισκόπηση αλλαγών πριν την τελική αποθήκευση.
- ✓ Αυτόματη δημιουργία πίνακα περιεχομένων.

Υποσύστημα Chat Rooms. Το Υποσύστημα Chat Rooms επιτρέπει την επικοινωνία των ομάδων χρηστών με τη χρήση μηνυμάτων κειμένου (text-based chat) σε πραγματικό χρόνο. Το υποσύστημα αυτό χρησιμοποιείται για την πραγματοποίηση συζητήσεων σε θέματα ασφάλειας και την επίλυση προβλημάτων. Για το σύστημα αυτό χρησιμοποιείται το AJAX Chat – Open Source Web Chat [8].

Το AJAX Chat είναι ένα ελεύθερο και πλήρως παραμετροποιήσιμο λογισμικό για web chat και είναι υλοποιημένο σε JavaScript και PHP. Τα χαρακτηριστικά του υποσυστήματος είναι:

- ✓ Πολλαπλά Κανάλια.
- ✓ Προσωπικά Μηνύματα.
- ✓ Ιδιωτικά Κανάλια.
- ✓ Σύστημα Πρόσκλησης σε ιδιωτικό κανάλι.
- ✓ Δυνατότητα διαγραφής μηνυμάτων.
- ✓ Δυνατότητα ορισμού ωρών λειτουργίας.

Υποσύστημα Blog. Το Υποσύστημα Blog επιτρέπει σε εξουσιοδοτημένους χρήστες να αναρτούν περιεχόμενο σχετικό με την ασφάλεια ΠΣ. Το Blog ενημερώνεται από τον χρήστη με τακτικές αναρτήσεις, περιγραφές γεγονότων, ειδήσεων ή άλλο υλικό, όπως εικόνες και βίντεο. Οι αναρτήσεις εμφανίζονται σε αντίστροφη χρονολογική σειρά, ενώ υπάρχει και δυνατότητα αναζήτησης. Επιπλέον, οι υπόλοιποι χρήστες μπορούν να αφήνουν σχόλια στην εκάστοτε ανάρτηση, αν αυτό κρίνεται σκόπιμο από το διαχειριστή του blog. Το υποσύστημα Blog έχει τις παρακάτω δυνατότητες:

- ✓ Εμφάνιση λίστας δημοσιεύσεων.
- ✓ Λεπτομέρειες δημοσίευσης.
- ✓ Προσθήκη σχολίων.
- ✓ Ειδοποίηση ηλεκτρονικού ταχυδρομείου (e-mail) για νέα σχόλια.
- ✓ Κατηγοριοποίηση δημοσιεύσεων με βάση λέξεις-κλειδιά.
- ✓ Ειδοποιήσεις RSS για νέες δημοσιεύσεις.
- ✓ Διαχείριση σχολίων και δημοσιεύσεων.

Μέσω του Υποσυστήματος Συνεργατικότητας καθίσταται εφικτή η επικοινωνία διαφορετικών ομάδων χρηστών μεταξύ τους ώστε να επιτυγχάνεται ταχύτερα η επίλυση προβλημάτων που προκύπτουν. Επίσης, η συνεργατική φύση των εργαλείων από τα οποία απαρτίζεται το εν λόγω υποσύστημα είναι σε θέση να βοηθήσει στην ταχύτερη λήψη αποφάσεων από τις αρμόδιες ομάδες χρηστών, αλλά και να συνεισφέρει συνολικά στη δημιουργία συνεργατικής κουλτούρας μεταξύ των χρηστών του συνεργατικού περιβάλλοντος STORM.

5.4.1.2 Επιχειρησιακό Επίπεδο (Enterprise Tier)

Το *Επιχειρησιακό Επίπεδο* (Εικόνα 17) είναι υπεύθυνο για την υλοποίηση της επιχειρησιακής λογικής της Κύριας Πλατφόρμας ενώ ταυτόχρονα λειτουργεί και ως ενδιάμεσο επίπεδο μεταξύ του

Δικτυακού-Διαδραστικού Επιπέδου και του Επιπέδου Βάσης Δεδομένων. Το Επιχειρησιακό Επίπεδο αποτελείται από οκτώ (8) αλληλοεξαρτώμενα υποσυστήματα:

- ✓ το υποσύστημα Χαρτογράφησης,
- ✓ το υποσύστημα Ανάλυσης Επικινδυνότητας,
- ✓ το Πλαίσιο Ανίχνευσης Αδυναμιών,
- ✓ το υποσύστημα Διαχείρισης Επικινδυνότητας,
- ✓ το υποσύστημα Διαχείρισης Εγγράφων Ασφάλειας,
- ✓ το υποσύστημα Διαχείρισης Ταυτότητας,
- ✓ το υποσύστημα Αποθετηρίου, και
- ✓ το υποσύστημα Διαχείρισης Περιεχομένου,

τα οποία αναλαμβάνουν να φέρουν εις πέρας τις απαραίτητες επιχειρησιακές λειτουργίες της Κύριας Πλατφόρμας.

Εικόνα 17: Επιχειρησιακό Επίπεδο

Στις Ενότητες που ακολουθούν παρουσιάζονται όλα τα υποσυστήματα του *Επιχειρησιακού Επιπέδου*.

5.4.1.2.1 Υποσύστημα Χαρτογράφησης

Το *Υποσύστημα Χαρτογράφησης*, είναι υπεύθυνο για την συλλογή και την επεξεργασία του απαραίτητου πληροφοριακού υλικού για την καταγραφή των κρίσιμων ηλεκτρονικών υπηρεσιών, την καταγραφή των αγαθών (αγαθών δεδομένων, συστημάτων, υλικού, λογισμικού και χρηστών ανά ηλεκτρονική υπηρεσία) και των αλληλεξαρτήσεών τους, καθώς και την αποτύπωση της υφιστάμενης κατάστασης. Το υποσύστημα Χαρτογράφησης είναι ταυτόχρονα υπεύθυνο για την διασύνδεση και την ανταλλαγή μηνυμάτων με το υποσύστημα Ανάλυσης Επικινδυνότητας.

5.4.1.2.2 Υποσύστημα Ανάλυσης Επικινδυνότητας

Το *Υποσύστημα Ανάλυσης Επικινδυνότητας* είναι υπεύθυνο για την υλοποίηση των βημάτων της μεθοδολογίας (Κεφάλαιο 4) για την Ανάλυση Επικινδυνότητας. Πιο συγκεκριμένα, για τη

δημιουργία, επεξεργασία και διαχείριση της απαραίτητης πληροφορίας που απαιτείται από τα βήματα της μεθοδολογίας, το υποσύστημα Ανάλυσης Επικινδυνότητας είναι εφοδιασμένο με επιμέρους υποσυστήματα τα οποία είναι αλληλένδετα και περιγράφονται παρακάτω:

Το *Υποσύστημα Αποτίμησης Επιπτώσεων Ασφάλειας*, το οποίο αναλαμβάνει όλες τις διαδικασίες που περιγράφει η μεθοδολογία του Κεφαλαίου 4 στο αντίστοιχο βήμα της. Είναι υπεύθυνο για τους απαραίτητους υπολογισμούς των ατομικών, των ομαδικών και των τελικών βαθμών αποτιμήσεων ασφάλειας κάθε αγαθού.

Το *Υποσύστημα Αποτίμησης Απειλών*, αναλαμβάνει να εκτελέσει τις διαδικασίες του αντίστοιχου βήματος της μεθοδολογίας του Κεφαλαίου 4. Συγκεκριμένα, πραγματοποιεί τις αντιστοιχίσεις των απειλών με τις ομάδες αγαθών και αναλαμβάνει την επεξεργασία και τον υπολογισμό των ατομικών, στην συνέχεια των ομαδικών και, τέλος, των τελικών βαθμών αποτίμησης απειλών για κάθε αγαθό.

Το *Υποσύστημα Αποτίμησης Αδυναμιών* είναι υπεύθυνο για την καταγραφή, ανάλυση, αξιολόγηση και υπολογισμό των θεωρητικών και πρακτικών βαθμών αποτίμησης των αδυναμιών. Ταυτόχρονα, είναι υπεύθυνο για τον υπολογισμό των συνολικών βαθμών αποτίμησης αδυναμιών των αγαθών, όπως ορίζει το αντίστοιχο βήμα της μεθοδολογίας του Κεφαλαίου 4.

Τέλος, το *Υποσύστημα Αποτίμησης Επικινδυνότητας* είναι υπεύθυνο για τη διασύνδεση με όλα τα προηγούμενα υποσυστήματα και την ανταλλαγή των απαραίτητων μηνυμάτων με στόχο τόσο την επεξεργασία των επιμέρους αποτελεσμάτων των βαθμών αποτίμησης επίπτωσης ασφάλειας, απειλών και αδυναμιών, όσο και τον υπολογισμό των βαθμών επικινδυνότητας κάθε αγαθού.

5.4.1.2.3 Πλαίσιο Ανίχνευσης Αδυναμιών

Το *Πλαίσιο Ανίχνευσης Αδυναμιών* αναλαμβάνει την πρακτική αποτίμηση αδυναμιών των υπό εξέταση αγαθών. Πιο συγκεκριμένα, πρόκειται για μια ειδικά διαμορφωμένη πλατφόρμα, εφοδιασμένη από ανοιχτού κώδικα εργαλεία, τα οποία είναι υπεύθυνα για την πρακτική ανάλυση αδυναμιών, όπως αυτή περιγράφεται στο Κεφάλαιο 4.

5.4.1.2.4 Υποσύστημα Διαχείρισης Επικινδυνότητας

Το *Υποσύστημα Διαχείρισης Επικινδυνότητας* αναλαμβάνει όλες εκείνες τις λειτουργίες που απαιτούνται από την Φάση 6: Μέτρα Προστασίας - Σχέδιο Ασφάλειας της μεθοδολογίας του Κεφαλαίου 4. Το συγκεκριμένο υποσύστημα λαμβάνει ως είσοδο τα αποτελέσματα του υποσυστήματος Ανάλυσης Επικινδυνότητας, εκτελεί τον έλεγχο αυτών των αποτελεσμάτων ώστε να

είναι σε θέση να προτείνει τα μέτρα ασφάλειας. Ταυτόχρονα, εκτελεί όλες τις απαραίτητες διαδικασίες και υπολογισμούς για την τελική επιλογή των κατάλληλων μέτρων ασφάλειας.

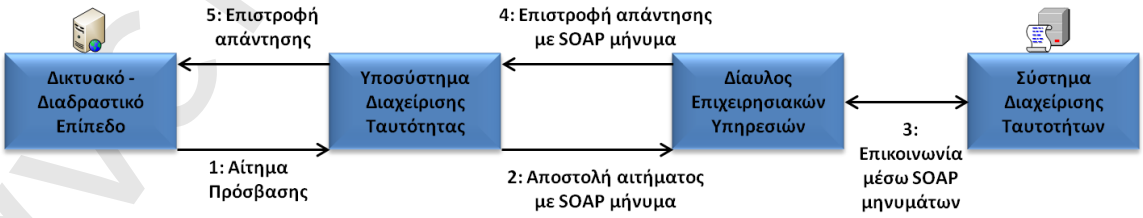
5.4.1.2.5 Υποσύστημα Διαχείρισης Εγγράφων Ασφάλειας

Το *Υποσύστημα Διαχείρισης Εγγράφων Ασφάλειας* είναι υπεύθυνο για την παροχή της Υπηρεσίας Διαχείρισης Εγγράφων Ασφάλειας. Το συγκεκριμένο υποσύστημα παρέχει την αναγκαία διαλειτουργικότητα με το *Υποσύστημα Χαρτογράφησης, το Υποσύστημα Ανάλυσης Επικινδυνότητας* και το *Υποσύστημα Διαχείρισης Επικινδυνότητας* έτσι ώστε να λαμβάνει όλη την αναγκαία πληροφορία μέσω της οποίας θα παρέχονται, δημιουργούνται και διαχειρίζονται τα αναγκαία Έγγραφα Ασφάλειας (Πολιτική Ασφάλειας, Σχέδιο Αποκατάστασης Καταστροφών). Πιο αναλυτικά αναλαμβάνει τους απαραίτητους μηχανισμούς και ελέγχους για την απαραίτητη επεξεργασία των αποτελεσμάτων της Χαρτογράφησης (η συλλογή των πληροφοριακών αγαθών όπως ορίζεται από το συγκεκριμένο βήμα της μεθοδολογίας - Κεφάλαιο 4) ώστε να δημιουργηθούν οι απαραίτητες ενότητες της Πολιτικής Ασφάλειας και του Σχεδίου Αποκατάστασης Καταστροφών.

Ταυτόχρονα αναλαμβάνει και την αντιστοίχιση των αποτελεσμάτων της Ανάλυσης και Διαχείρισης Επικινδυνότητας με τις κατάλληλες ενότητες του ISO 27001:2005 [4], ώστε να δημιουργηθούν / ενημερωθούν οι διαδικασίες τις Πολιτικής Ασφάλειας και του Σχεδίου Αποκατάστασης Καταστροφών (οι οποίες εμφανίζονται / παρέχονται από την υπηρεσία Διαχείρισης Εγγράφων Ασφάλειας).

5.4.1.2.6 Υποσύστημα Διαχείρισης Ταυτότητας

Το *Υποσύστημα Διαχείρισης Ταυτότητας* είναι υπεύθυνο για τη διασύνδεση με τον Δίαυλο Επιχειρησιακών Υπηρεσιών. Πιο συγκεκριμένα, αναλαμβάνει τη δημιουργία και την ανταλλαγή μηνυμάτων των επιμέρους υποσυστημάτων (της Κύριας Πλατφόρμας) με τον Δίαυλο Επιχειρησιακών Υπηρεσιών ώστε να επιτευχθεί η επικοινωνία με το Σύστημα Διαχείρισης Ταυτοτήτων (Εικόνα 18).



Εικόνα 18: Ανταλλαγή μηνυμάτων αυθεντικοποίησης χρηστών

Το Υποσύστημα Διαχείρισης Ταυτότητας ανταλλάσσει SOAP μηνύματα [10] με τον Δίαυλο Επιχειρησιακών Υπηρεσιών και αυτός με την σειρά του επικοινωνεί με το Σύστημα Διαχείρισης Ταυτοτήτων προκειμένου να επιτευχθεί ή όχι η πρόσβαση ενός χρήστη στην Κύρια Πλατφόρμα.

5.4.1.2.7 Υποσύστημα Αποθετηρίου

Το *Υποσύστημα Αποθετηρίου* είναι υπεύθυνο για τη διασύνδεση όλων των υποσυστημάτων με το Επίπεδο Βάσης Δεδομένων και αναλαμβάνει να φέρει εις πέρας όλα τα απαραίτητα ερωτήματα - μηνύματα των επιμέρους υποσυστημάτων προς το Επίπεδο Βάσης Δεδομένων του STORM. Συγκεκριμένα είναι υπεύθυνο για όλες τις ανταλλαγές μηνυμάτων από και προς το Επίπεδο Βάσεως Δεδομένων για τη δημιουργία, επεξεργασία και ανανέωση του απαραίτητου πληροφοριακού υλικού όπως:

- ✓ λίστες αγαθών/ απειλών / αδυναμιών,
- ✓ αλληλεξαρτήσεις αγαθών,
- ✓ κατηγορίες επιπτώσεων,
- ✓ κλίμακες επιπτώσεων ασφάλειας / αποτίμησης απειλών / αποτίμησης αδυναμιών / επικινδυνότητας,
- ✓ αποτελέσματα αποτίμησης αγαθών / απειλών / αδυναμιών / επικινδυνότητας,
- ✓ μέτρα προστασίας, κλπ.,

τα οποία αποτελούν είτε είσοδο είτε έξοδο όλων των υποσυστημάτων του περιβάλλοντος STORM.

5.4.1.2.8 Υποσύστημα Διαχείρισης Περιεχομένου

Το *Υποσύστημα Διαχείρισης Περιεχομένου* (Content Management System, CMS) είναι υπεύθυνο για τη δημιουργία, επεξεργασία, διαχείριση και δημοσίευση όλου του βασικού επεξεργασμένου και μη πληροφοριακού περιεχομένου με ένα συνεπή και οργανωμένο τρόπο. Ταυτόχρονα, το συγκεκριμένο υποσύστημα αναλαμβάνει όλους εκείνους του μηχανισμούς για την αποθήκευση, αναζήτηση και ανάκτηση των εγγράφων της Υπηρεσίας Ηλεκτρονικής Βιβλιοθήκης.

5.4.1.3 Επίπεδο Βάσης Δεδομένων (Database Tier)

Το *Επίπεδο Βάσης Δεδομένων* αναλαμβάνει την διαχείριση, επεξεργασία και αποθήκευση όλου του πληροφοριακού περιεχομένου του συνεργατικού περιβάλλοντος STORM. Το Επιχειρησιακό Επίπεδο προκειμένου να έχει πρόσβαση στα δεδομένα του STORM επικοινωνεί με το Επίπεδο Βάσης

Δεδομένων μέσω του Υποσυστήματος Αποθετηρίου. Σε περίπτωση, όμως, που κάποιο από τα συστήματα Διαχείρισης Ταυτοτήτων ή Διαχείρισης Επιχειρησιακών Διαδικασιών χρειαστεί να συνδεθεί με το Επίπεδο Βάσης Δεδομένων**,** η επικοινωνία τους γίνεται μόνο μέσω του Διαύλου Επιχειρησιακών Υπηρεσιών**.**

Με τον τρόπο αυτό επιτυγχάνεται ο κεντρικός έλεγχος και η ασφαλής πρόσβαση στα δεδομένα του STORM, ενώ ταυτόχρονα αν κάποια άλλη εξωτερική οντότητα (σε τυχόν μελλοντική επέκταση του περιβάλλοντος STORM) επιθυμήσει να συνδεθεί και να εισαγάγει ή να διαβάσει δεδομένα από το Επίπεδο Βάσης Δεδομένων θα πρέπει να προσαρμοστεί κατάλληλα με τις προδιαγραφές (μέσω του πρωτοκόλλου WSDL) του Διαύλου Επιχειρησιακών Υπηρεσιών.

5.4.2 Συστήματα STORM

Στις ενότητες που ακολουθούν περιγράφονται οι λειτουργίες των περιφερειακών συστημάτων του συνεργατικού περιβάλλοντος διαχείρισης ασφάλειας STORM, του Διαύλου Επιχειρησιακών Υπηρεσιών, του Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών και του Συστήματος Διαχείρισης Ταυτοτήτων.

5.4.2.1 Δίαυλος Επιχειρησιακών Υπηρεσιών

Με στόχο την ασφαλή και άμεση σύνδεση των εξωτερικών συστημάτων (Σύστημα Διαχείρισης Ταυτοτήτων και Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών) και της Κύριας Πλατφόρμας επιλέξαμε να ενσωματώσουμε στην αρχιτεκτονική του συνεργατικού περιβάλλοντος STORM τον *Δίαυλο Επιχειρησιακών Υπηρεσιών (Enterprise Service Bus)*. Ο Δίαυλος Επιχειρησιακών Υπηρεσιών είναι βασισμένος στην βιβλιοθήκη Mule version 3 [6] και χρησιμοποιεί τον εξυπηρετητή Apache Tomcat.

Το βασικό πλεονέκτημα του Δίαυλου Επιχειρησιακών Υπηρεσιών είναι ότι επιτρέπει σε διαφορετικά συστήματα / εφαρμογές να επικοινωνούν με ασφάλεια μεταξύ τους, λειτουργώντας ως ένας κοινός δίαυλος ανταλλαγής μηνυμάτων. Συγκεκριμένα, οι κύριες αρμοδιότητες του Δίαυλου Επιχειρησιακών Υπηρεσιών είναι:

- ✓ η διασύνδεση της Κύριας Πλατφόρμας με τα εξωτερικά συστήματα,
- ✓ η παρακολούθηση και ο έλεγχος της δρομολόγησης της ανταλλαγής μηνυμάτων μεταξύ της Κύριας Πλατφόρμας και των εξωτερικών συστημάτων, και

- ✓ η διαχείριση των απαραίτητων Υπηρεσιών Ιστού (Web Services) που είναι υπεύθυνες για τη διασύνδεση όλων των εξωτερικών συστημάτων με την Κύρια Πλατφόρμα.

Ο Δίαυλος Επιχειρησιακών Υπηρεσιών αποτελείται από τρία (3) υποσυστήματα:

- ✓ το Υποσύστημα Μετατροπής Δεδομένων (Data Transformation Module), το οποίο διαβεβαιώνει ότι τα δεδομένα τα οποία ανταλλάσσονται (όποτε και αν χρειαστεί) από τα εξωτερικά συστήματα στην Κύρια Πλατφόρμα βρίσκονται σε συγκεκριμένη δομή (προκαθορισμένη μορφή),
- ✓ το Υποσύστημα Διαμεσολάβησης (Message Broker Module), το οποίο αναλαμβάνει τη σωστή μεταφορά δεδομένων, και
- ✓ το Υποσύστημα Δρομολόγησης (Message Routing Module), το οποίο αναλαμβάνει τη δρομολόγηση και το φιλτράρισμα των μηνυμάτων που ανταλλάσσονται βάση συγκεκριμένων κανόνων.

Τα μηνύματα SOAP [10] που ανταλλάσσονται μέσω του Δίαυλου Επιχειρησιακών Υπηρεσιών μπορεί να είναι:

- ✓ είτε *Μηνύματα υπηρεσίας* (service messages) τα οποία περιέχουν πληροφορίες για την επικοινωνία μεταξύ διαφορετικών συστημάτων,
- ✓ είτε *Μηνύματα Δρομολόγησης* (routing messages) τα οποία περιέχουν πληροφορίες δρομολόγησης,
- ✓ είτε και των δύο ειδών μηνύματα.

Ο Δίαυλος Επιχειρησιακών Υπηρεσιών διαβεβαιώνει την ομαλή ενορχήστρωση και διαλειτουργικότητα των εξωτερικών συστημάτων και της Κύρια Πλατφόρμας, ενώ ταυτόχρονα δίνει την δυνατότητα αναβάθμισης/επέκτασης και σύνδεσης με οποιαδήποτε άλλη εξωτερική οντότητα (υπηρεσία ή σύστημα) εάν αυτό κριθεί αναγκαίο από μελλοντικές αναβαθμίσεις του περιβάλλοντος STORM.

5.4.2.2 Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών

Το *Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών* (Business Process Management System - BPMS) είναι υπεύθυνο για την καταγραφή, επεξεργασία και απεικόνιση των αγαθών των Πληροφοριακών Συστημάτων που σχετίζονται με τις κρίσιμες ηλεκτρονικές υπηρεσίες του υπό εξέταση οργανισμού. Όπως ορίζεται στο βήμα της Χαρτογράφησης της STORM-RM μεθοδολογίας (Κεφάλαιο 4), με αυτό το σύστημα οι αρμόδιες ομάδες χρηστών (π.χ. στελέχη διοίκησης) θα

μπορούν να προβούν στην παραγωγή διαγραμμάτων επιχειρησιακών διαδικασιών. Η πληροφορία η οποία θα αποτυπώνεται και θα αποθηκεύεται σε αυτά τα διαγράμματα θα αποτελεί είσοδο για άλλα υποσυστήματα της Κύριας Πλατφόρμας STORM, με βασικότερο αυτό της Ανάλυσης Επικινδυνότητας.

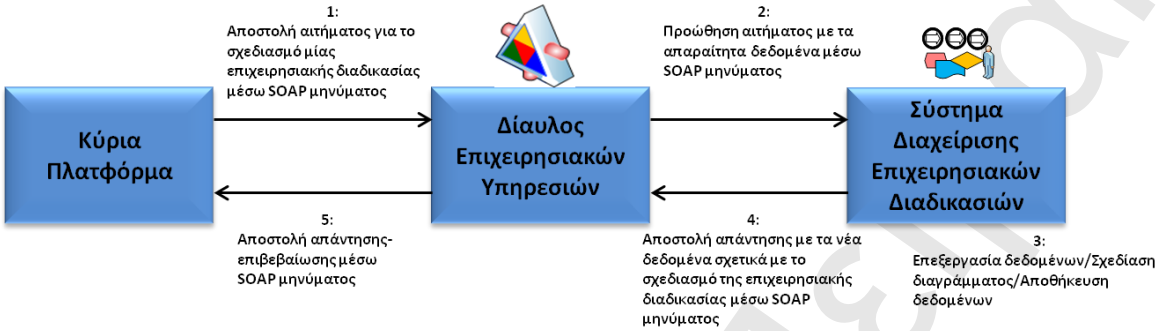
Το Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών είναι βασισμένο στο Signavio Web Designer, το οποίο είναι ένα ανοιχτού κώδικα εργαλείο αποτύπωσης επιχειρησιακών διαδικασιών και χρησιμοποιεί το πρότυπο BPMN [2]. Για τις ανάγκες της Φάσης Χαρτογράφησης της μεθοδολογίας STORM-RM έχουν γίνει οι κατάλληλες παραμετροποιήσεις του εργαλείου. Συγκεκριμένα, έχουν δημιουργηθεί νέα αντικείμενα (objects) σχεδίασης (Πίνακας 36) ώστε κατά την αποτύπωση των επιχειρησιακών διαδικασιών μιας ηλεκτρονικής υπηρεσίας να αποθηκεύονται τα *Δεδομένα* τα οποία χρησιμοποιεί η υπηρεσία αλλά και τα *Συστήματα* τα οποία εμπλέκονται για την παροχή της εν λόγω η-υπηρεσίας.

Πίνακας 36: Νέα Αντικείμενα Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών

Αντικείμενο (Object)	**Γνωρίσματα (Attributes)**
Δεδομένα (Data)	Όνομα (name) Περιγραφή (description) Κατηγορία Δεδομένων (data_asset_category)
Σύστημα (System)	Όνομα (name) Περιγραφή (description) Κατηγορία Συστήματος (system_category)

Κατά την διάρκεια σχεδίασης, αποτύπωσης και αποθήκευσης ενός διαγράμματος μεταφέρεται η απαραίτητη πληροφορία (π.χ. λίστα υλικών αγαθών που σχετίζονται με μία συγκεκριμένη η-υπηρεσία) στην Κύρια Πλατφόρμα μέσω του Διαύλου Επιχειρησιακών Υπηρεσιών. Συγκεκριμένα, για να ενεργοποιηθεί το Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών, ώστε να σχεδιαστεί το κατάλληλο διάγραμμα μίας η-υπηρεσίας, η Κύρια Πλατφόρμα επικοινωνεί με τον Δίαυλο Επιχειρησιακών Υπηρεσιών, ο οποίος με τη σειρά του επικοινωνεί με το Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών. Στη συνέχεια, ο χρήστης αναλαμβάνει μέσω του Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών τη σχεδίαση / αποτύπωση / αποθήκευση του διαγράμματος μίας η-υπηρεσίας. Τα δεδομένα αποθηκεύονται σε αντικείμενα όπως αυτά περιγράφονται στον Πίνακας 36. Μετά το πέρας της εν λόγω διαδικασίας, τα νέα δεδομένα που έχουν προκύψει αποστέλλονται ως απάντηση στον Δίαυλο Επιχειρησιακών Υπηρεσιών και αυτός, με τη σειρά του, τα προωθεί στην Κύρια Πλατφόρμα. Η επικοινωνία μεταξύ των εμπλεκόμενων μερών

βασίζεται στο μοντέλο των Υπηρεσιών Ιστού και οι απαραίτητες πληροφορίες μεταδίδονται μέσω αιτημάτων και απαντήσεων μηνυμάτων SOAP [10] (Εικόνα 19).



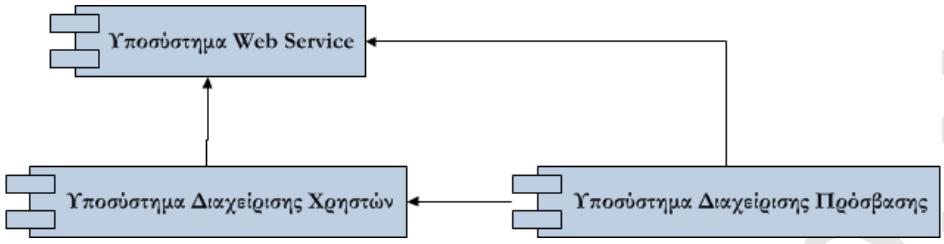
Εικόνα 19: Επικοινωνία Κύριας Πλατφόρμας - Δίαυλος Επ. Υπηρεσιών - Σύστημα Δ. Επ. Διαδικασιών

Το Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών είναι βασισμένο σε Java Servlets και χρειάζεται συγκεκριμένο τύπο web server, κατάλληλο για εφαρμογές Java EE (πχ Tomcat). Οι διαφορετικές αυτές πλατφόρμες θα πρέπει, με κάποιον τρόπο, να συνδυαστούν ώστε το περιβάλλον διεπαφής να είναι ομοιογενές και ενοποιημένο για τους τελικούς χρήστες.

Η ενσωμάτωση του Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών στο περιβάλλον του STORM γίνεται με χρήση των HTML iframe. Πιο συγκεκριμένα, όταν ένας τελικός χρήστης κάνει την επιλογή (μέσω των μενού πλοήγησης) για αποτύπωση των επιχειρησιακών διαδικασιών μιας συγκεκριμένης υπηρεσίας, ανοίγει το γραφικό περιβάλλον με όλες τις απαραίτητες γραμμές εργαλείων για την σχεδίαση και την αποθήκευση των διαγραμμάτων BPM.

5.4.2.3 Σύστημα Διαχείρισης Ταυτοτήτων

Το *Σύστημα Διαχείρισης Ταυτότητας και Δικαιωμάτων Προσπέλασης* (Identity and Access Management, IAM System), καθορίζει και εφαρμόζει με τον πλέον κατάλληλο τρόπο ειδικά σχεδιασμένες πολιτικές ταυτοποίησης, αυθεντικοποίησης και εξουσιοδότησης, οι οποίες θα χρησιμοποιούνται για τον έλεγχο προσπέλασης στις υπηρεσίες του STORM. Το Σύστημα Διαχείρισης Ταυτότητας και Δικαιωμάτων Προσπέλασης είναι υλοποιημένο σε Java και χρειάζεται συγκεκριμένο τύπο web server, κατάλληλο για εφαρμογές Java EE (πχ Tomcat).



Εικόνα 20: Σύστημα Διαχείρισης Ταυτοτήτων

Το Σύστημα Διαχείρισης Ταυτοτήτων (IAM System) αποτελείται από τρία (3) βασικά υποσυστήματα (Εικόνα 20) τα οποία περιγράφονται στις παραγράφους που ακολουθούν:

- ✓ Το Υποσύστημα Διαχείρισης Χρηστών (Profile Management Module), το οποίο είναι υπεύθυνο για την διαχείριση του προφίλ των χρηστών του περιβάλλοντος STORM. Συγκεκριμένα είναι υπεύθυνο για την δημιουργία / επεξεργασία / διαγραφή των χρηστών και των ομάδων χρηστών.
- ✓ Το Υποσύστημα Διαχείρισης Πρόσβασης (Access Control Module), το οποίο αναλαμβάνει την διαχείριση των δικαιωμάτων πρόσβασης των χρηστών ανάλογα με την ομάδα χρηστών στην οποία ανήκουν.
- ✓ Το Υποσύστημα Web Service (Web Service Module), το οποίο διαχειρίζεται την επικοινωνία του συστήματος IAM και των υπόλοιπων οντοτήτων του περιβάλλοντος STORM. Παρέχει Υπηρεσίες Ιστού οι οποίες βασίζονται στις πληροφορίες που απαιτούνται από τα υπόλοιπα δύο υποσυστήματα (*Διαχείρισης Χρηστών και Διαχείρισης Πρόσβασης*) με στόχο την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών, ενώ ταυτόχρονα αναλαμβάνει και την επικοινωνία με τις εξωτερικές οντότητες του περιβάλλοντος STORM, σε περίπτωση που κάποια από αυτές χρειάζεται δικαιώματα πρόσβασης ώστε να χρησιμοποιηθεί από τους χρήστες του STORM.

5.5 Ομάδες Χρηστών STORM

Στην ενότητα αυτή περιγράφονται οι προτεινόμενες ομάδες χρηστών του συνεργατικού περιβάλλοντος διαχείρισης ασφάλειας STORM. Οι ομάδες οι οποίες περιγράφονται είναι ενδεικτικές καθώς το περιβάλλον STORM δίνει την δυνατότητα παραμετροποίησης και προσαρμογής των δυνατοτήτων του ώστε να καλύπτει τις ανάγκες οποιουδήποτε οργανισμού. Οι προτεινόμενες ομάδες οι οποίες θα είναι σε θέση να κάνουν χρήση των υπηρεσιών STORM είναι οι παρακάτω.

Ο Νόμιμος εκπρόσωπος του υπό εξέταση οργανισμού αντιπροσωπεύει ένα χρήστη ο οποίος έχει πολύ υψηλή διοικητική θέση στον οργανισμό και ευρεία γνώση της δομής, λειτουργίας και των στόχων του οργανισμού. Η συμμετοχή του είναι πολύ σημαντική και αφορά: (1) στον καθορισμό του

εύρους της μελέτης ασφάλειας (ποιες οργανωτικές μονάδες, υπηρεσίες και συστήματα πρέπει να μελετηθούν), (2) στον προσδιορισμό των διοικητικών υπευθύνων του οργανισμού που πρέπει να εμπλακούν στη μελέτη και (3) στην αρχική αξιολόγηση της κρισιμότητας των υπό μελέτη υπηρεσιών, από μία επιχειρησιακή ματιά. Το ρόλο του νόμιμου εκπροσώπου θα μπορούσε να αναλάβει κάποιο μέλος της Ανώτατης Διοίκησης όπως ο Γενικός Διευθυντής του οργανισμού ή κάποιο πρόσωπο που δρα με την εξουσιοδότηση της Ανώτατης Διοίκησης.

Τα μέλη της Ομάδας Ασφάλειας του υπό εξέταση οργανισμού αντιπροσωπεύουν τη διοικητική δομή του οργανισμού και έχουν υψηλή γνώση θεμάτων ασφάλειας συστημάτων και δικτύων μέσα στον οργανισμό. Συνήθως η Ομάδα Ασφάλειας αποτελεί ανεξάρτητη διοικητική οντότητα υπό την επίβλεψη της ανώτατης διοίκησης ή υπό την επίβλεψη της διεύθυνσης πληροφορικής. Σημειώνεται ότι ο ρόλος της ομάδας ασφάλειας αποτελεί οργανωτική απαίτηση όλων των γνωστών προτύπων ασφάλειας όπως το ISO 27001. Την ομάδα ασφάλειας ενδέχεται να εκπροσωπεί στις διάφορες λειτουργίες ο Υπεύθυνος Ασφάλειας Συστημάτων και Δικτύων, ο οποίος αποτελεί ουσιαστικά τον επικεφαλής της ομάδας ασφάλειας. Τα μέλη της συγκεκριμένης ομάδας χρηστών είναι σε θέση να κάνουν αξιολόγηση της κρισιμότητας των υπηρεσιών, ανάλυση και αποτίμηση επικινδυνότητας, διαχείριση κινδύνου με χρήση των κατάλληλων αντιμέτρων και υλοποίηση όλων των διαδικασιών της πολιτικής ασφάλειας σύμφωνα με τις Φάσεις τις μεθοδολογίας STORM-RM. Μπορούν να παρακολουθούν και να ενημερώνονται διαρκώς για τα νέα πρότυπα και βέλτιστες πρακτικές και να τις εφαρμόζουν άμεσα στο σύστημά τους. Ως αποτέλεσμα, θα είναι διαθέσιμο σε όλους τους χρήστες επικαιροποιημένα σχέδια επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών, αφού θα έχουν ληφθεί υπόψη όλες οι τεχνικές και επιχειρησιακές διαδικασίες του οργανισμού.

Τα μέλη της Διοίκησης του υπό εξέταση οργανισμού τα οποία αντιπροσωπεύουν τους διοικητικούς προϊσταμένους (ή εκπροσώπους αυτών) των διοικητικών μονάδων που συμμετέχουν στη μελέτη ασφάλειας. Τα μέλη της Διοίκησης, έχουν σαφή γνώση του τρόπου λειτουργίας των υπηρεσιών των διοικητικών τους μονάδων, υψηλή γνώση των πληροφοριακών συστημάτων που χρησιμοποιούνται για την παροχή των υπηρεσιών της μονάδας του, και γνώση του προσωπικού (τελικών χρηστών) που λειτουργούν αυτές τις υπηρεσίες. Οι χρήστες αυτής της ομάδας που συμμετέχουν στη μελέτη έχουν καθοριστεί από τον Νόμιμο Εκπρόσωπο του οργανισμού, και με τη σειρά τους καθορίζουν τους τεχνικούς υπεύθυνους και τους τελικούς χρήστες που θα συμμετέχουν. Επιπλέον, έχουν σαφή γνώση των επιχειρησιακών επιπτώσεων από πιθανές παραβιάσεις ασφάλειας των συστημάτων που χρησιμοποιούνται για την παροχή υπηρεσιών από τις οργανωτικές μονάδες για

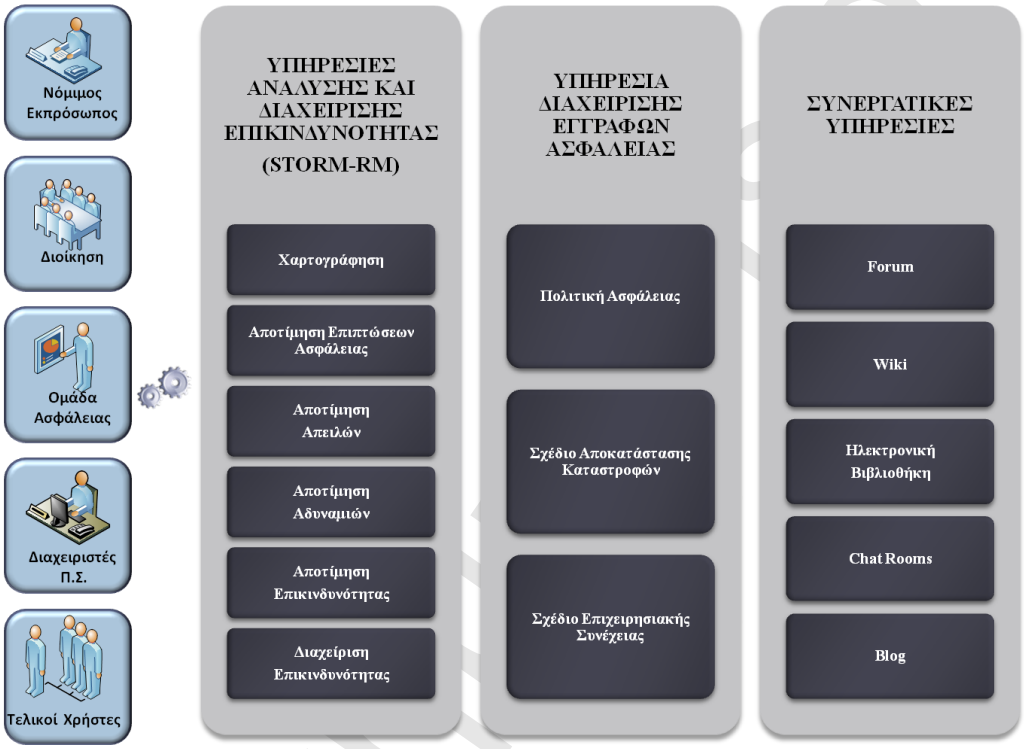
τις οποίες είναι υπεύθυνοι. Είναι σε θέση να συμμετέχουν στην διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας των ΠΣ τους, σύμφωνα με τις Φάσεις της μεθοδολογίας STORM-RM.

Οι Διαχειριστές των πληροφοριακών συστημάτων οι οποίοι θα ενημερώνουν συνεχώς το εργαλείο με όλο το απαραίτητο υλικό (τεχνικές οδηγίες, εγχειρίδια χρήσης, σχέδια επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών, διεθνή πρότυπα κτλ), θα δημιουργούν τα ερωτηματολόγια και τις απαραίτητες φόρμες, θα ορίζουν τους ρόλους των χρηστών, θα ελέγχουν και θα ανανεώνουν τις λίστες με το εγκατεστημένο λογισμικό και υλικό του πληροφοριακού συστήματος του οργανισμού και θα συμμετέχουν στην διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας σύμφωνα με τις Φάσεις της μεθοδολογίας STORM-RM.

Οι Τελικοί χρήστες οι οποίοι μπορεί να είναι ή τοπικοί, ή εξωτερικοί χρήστες του ΠΣ του υπό εξέταση οργανισμού. Πιο συγκεκριμένα, οι τοπικοί χρήστες (πχ χρήστες λογιστηρίου, χρήστες μηχανογράφησης κτλ), μπορούν μέσω του νέου εργαλείου να βρίσκουν πληροφορίες για τεχνικά θέματα και διαδικασίες ασφάλειας και, έτσι, να αντιμετωπίζονται ταχύτατα και αποτελεσματικά οι τυχόν δυσκολίες τους. Παράλληλα, θα είναι διαρκώς και πλήρως ενημερωμένοι για τις υποχρεώσεις και τον ρόλο τους σε περίπτωση που προκύψει κάποιο κακόβουλο γεγονός, ώστε αν τεθεί σε λειτουργία το σχέδιο αποκατάστασης καταστροφών ο χρόνος ανάκαμψης να είναι ο ταχύτερος δυνατός. Οι εξωτερικοί χρήστες, δηλαδή χρήστες των φορέων με τους οποίους συνεργάζεται ο υπό εξέταση οργανισμός, θα μπορούν να ενημερώνονται για τους κανόνες ασφαλείας και τους όρους ασφαλούς διασύνδεσης και επικοινωνίας με τα πληροφοριακά συστήματα του οργανισμού. Με τον τρόπο αυτό, θα υπάρχει δικλείδα ασφαλείας και θα ελαχιστοποιούνται ακόμα περισσότερο οι κίνδυνοι για αλλοίωση ή διακοπή των κρίσιμων πληροφοριών που ανταλλάσσονται μεταξύ τους. Όλοι οι χρήστες της ομάδας Τελικοί χρήστες θα συμμετέχουν στη διαδικασία ανάλυσης επικινδυνότητας σύμφωνα με τις Φάσεις της μεθοδολογίας STORM-RM.

5.6 Υπηρεσίες STORM

Στην ενότητα αυτή θα περιγραφούν οι βασικές υπηρεσίες (Εικόνα 21) του STORM, οι οποίες είναι απαραίτητες για να ικανοποιήσουν τους στόχους του συνεργατικού περιβάλλοντος.



Εικόνα 21: Υπηρεσίες συνεργατικού περιβάλλοντος STORM

5.6.1 Υπηρεσίες ανάλυσης και διαχείρισης επικινδυνότητας - STORM-RM

Στόχος της συγκεκριμένης ομάδας υπηρεσιών είναι η ανάλυση επικινδυνότητας των πληροφοριακών συστημάτων του οργανισμού χρησιμοποιώντας τα απαραίτητα βήματα της συνεργατικής μεθοδολογίας STORM-RM (Κεφάλαιο 4). Πιο συγκεκριμένα, για την πραγματοποίηση της ανάλυσης επικινδυνότητας των ΠΣ οι χρήστες του περιβάλλοντος STORM θα είναι σε θέση να χρησιμοποιούν τις παρακάτω υπηρεσίες.

5.6.1.1 Υπηρεσία Χαρτογράφησης

Μέσω της υπηρεσίας Χαρτογράφησης θα υπάρχει η δυνατότητα καταγραφής και αποτίμησης όλων των κρίσιμων η-υπηρεσιών του υπό εξέταση Π.Σ. Στην συνέχεια, για κάθε κρίσιμη ηλεκτρονική υπηρεσία υπάρχει η δυνατότητα αναλυτικής καταγραφής όλων των αγαθών (Φυσικά αγαθά, Υλικά

αγαθά, Λογισμικό, Δεδομένα, Χρήστες) που σχετίζονται με την κάθε η-υπηρεσία. Έπειτα από την καταγραφή των απαραίτητων αγαθών που σχετίζονται με την κάθε κρίσιμη η-υπηρεσία, υπάρχει η δυνατότητα αποτύπωσης των αλληλεξαρτήσεων των αγαθών αυτών σύμφωνα με το δένδρο αλληλεξαρτήσεων (Βήμα 1.3: Αλληλεξαρτήσεις αγαθών). Τέλος, στην υπηρεσία χαρτογράφησης, υπάρχει η δυνατότητα αποτύπωσης της υφιστάμενης κατάστασης των μέτρων ασφάλειας (επιλογή από μια λίστα μέτρων βασισμένα στο ISO 27001 [4]) και ο χαρακτηρισμός τους ως Πλήρως Εγκατεστημένα, Μερικώς Εγκατεστημένα, Μη Εγκατεστημένα. Επιπλέον, η υπηρεσία Χαρτογράφησης των κρίσιμων η-υπηρεσίων περιλαμβάνει την αποτύπωση των επιχειρησιακών διαδικασιών που τις στηρίζουν. Η αποτύπωση των επιχειρησιακών διαδικασιών πραγματοποιείται με την χρήση μοντέλων αναπαράστασης BPMN [2]. Η αποτύπωση των επιχειρησιακών διαδικασιών αφορά στην καταγραφή των:

- συμβάντων, δραστηριοτήτων,
- ροών μηνυμάτων, συσχετισμών,
- κατηγοριών, ομαδοποιήσεων, και
- αντικειμένων πληροφορίας, ομάδων, συμβολισμών.

Με την βοήθεια των μοντελοποιημένων επιχειρησιακών διαδικασιών παρέχεται η δυνατότητα οπτικής ανασκόπησης και αναθεώρησης από τους εμπλεκόμενους χρήστες.

Τα αποτελέσματα της υπηρεσίας Χαρτογράφησης θα χρησιμοποιηθούν ως είσοδος στις υπόλοιπες υπηρεσίες Ανάλυσης Επικινδυνότητας.

5.6.1.1.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλοι οι ρόλοι του STORM, δηλαδή ο Νόμιμος Εκπρόσωπος, τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες, με διαφορετικά σενάρια χρήσης, όπως περιγράφονται παρακάτω.

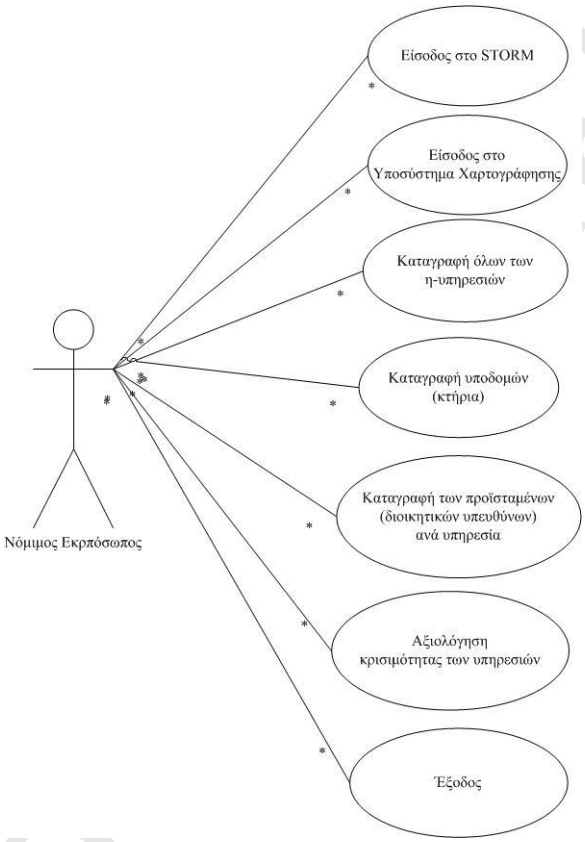
5.6.1.1.1.1 Σενάριο λειτουργίας Α: Καταγραφή των υπηρεσιών από τον Νόμιμο Εκπρόσωπο

Το σενάριο αυτό είναι το πρώτο που εκτελείται για την έναρξη μίας μελέτης ασφάλειας. Εκτελείται από τον Νόμιμο Εκπρόσωπο του οργανισμού και καθορίζει το εύρος της μελέτης, δηλαδή ποιες διοικητικές μονάδες και ποιες κύριες υπηρεσίες θα συμμετέχουν στη μελέτη ασφάλειας.

Περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 22):

1) Είσοδος στο Υποσύστημα Χαρτογράφησης.

2) Καταγραφή των η-υπηρεσιών.
3) Καταγραφή υποδομών (κτίρια).
4) Καταγραφή των προϊσταμένων (διοικητικών υπευθύνων) ανά υπηρεσία.
5) Αξιολόγηση κρισιμότητας των υπηρεσιών.
6) Έξοδος.



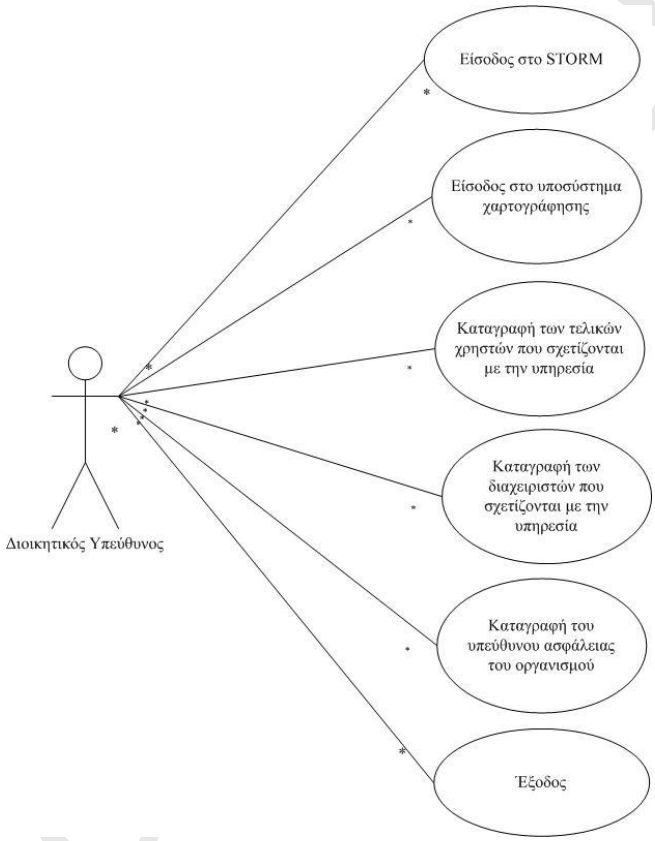
Εικόνα 22: Καταγραφή των υπηρεσιών από τον Νόμιμο Εκπρόσωπο

5.6.1.1.1.2 <u>Σενάριο λειτουργίας Β: Καταγραφή των εμπλεκόμενων χρηστών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους</u>

Το σενάριο αυτό είναι το δεύτερο που εκτελείται σε μία μελέτη ασφάλειας. Οι Διοικητικοί Υπεύθυνοι είναι εκείνοι που έχουν καταγραφεί στο προηγούμενο σενάριο από τον Νόμιμο Εκπρόσωπο του οργανισμού. Συνεπώς, το σενάριο αυτό απαιτεί την ολοκλήρωση του προηγούμενου σεναρίου λειτουργίας.

Περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 23):

1) Είσοδος στο υποσύστημα χαρτογράφησης (βλέπει μόνο τις υπηρεσίες για τις οποίες είναι υπεύθυνος).
2) Καταγραφή των τελικών χρηστών που σχετίζονται με την υπηρεσία.
3) Καταγραφή των διαχειριστών που σχετίζονται με την υπηρεσία.
4) Καταγραφή του υπεύθυνου ασφάλειας του οργανισμού.
5) Έξοδος.



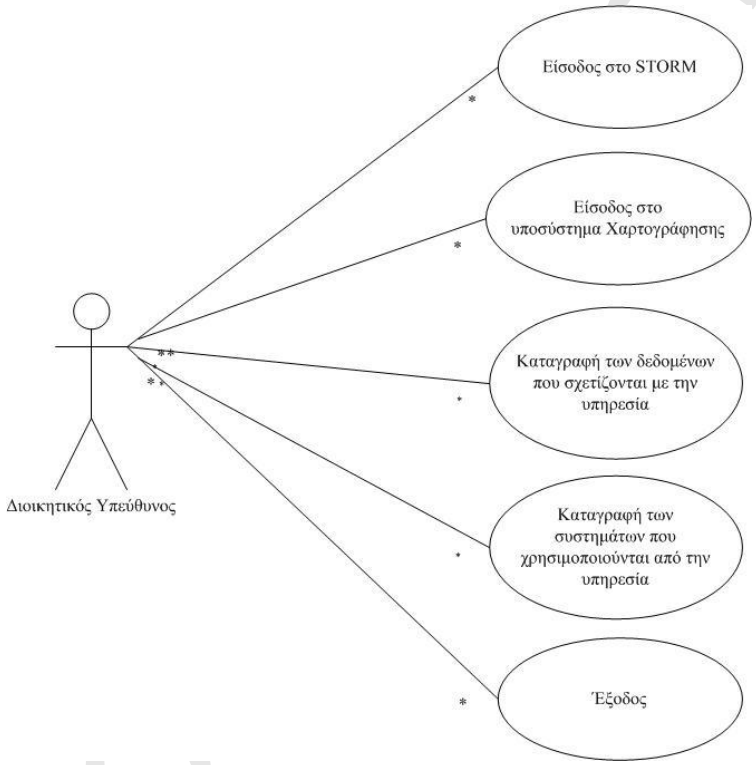
Εικόνα 23: Καταγραφή των εμπλεκόμενων χρηστών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους

5.6.1.1.1.3 Σενάριο λειτουργίας Γ: Καταγραφή των δεδομένων και των συστημάτων ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Α΄ τρόπος)

Το σενάριο αυτό είναι το τρίτο που εκτελείται σε μία μελέτη ασφάλειας και ακολουθεί το σενάριο λειτουργίας Β. Αποτελεί τη μία εναλλακτική για την καταγραφή των συστημάτων (η δεύτερη εναλλακτική παρουσιάζεται στο σενάριο λειτουργίας Δ).

Περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 24):

1) Είσοδος στο υποσύστημα χαρτογράφησης (βλέπει μόνο τις υπηρεσίες για τις οποίες είναι υπεύθυνος).
2) Καταγραφή των δεδομένων που σχετίζονται με την υπηρεσία (καταγράφει τα δεδομένα εισόδου και εξόδου που σχετίζονται με την υπηρεσία, με τη χρήση σχετικής φόρμας).
3) Καταγραφή των συστημάτων που χρησιμοποιούνται από την υπηρεσία (με τη χρήση φόρμας).
4) Έξοδος.



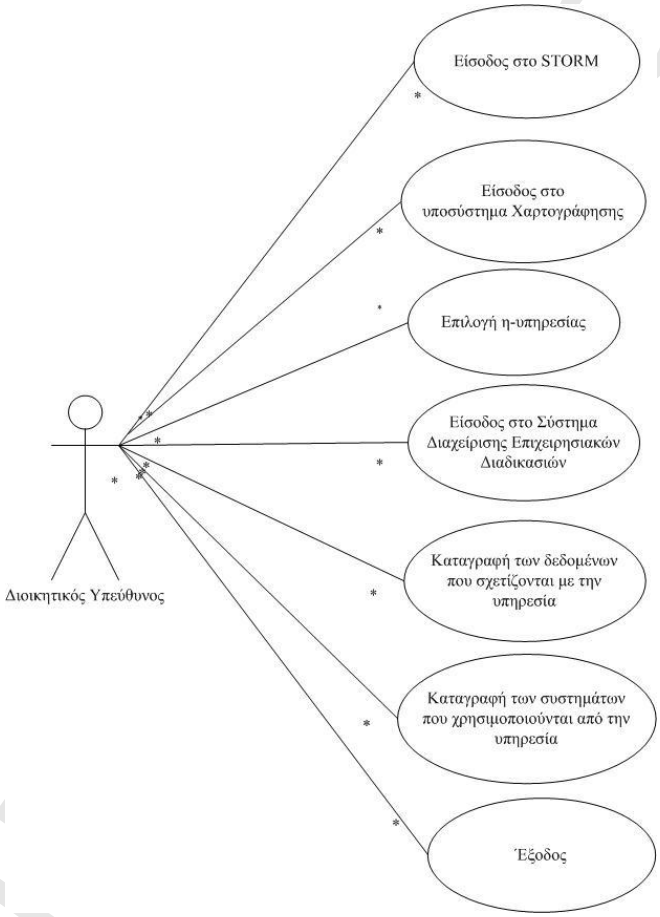
Εικόνα 24: Καταγραφή των δεδομένων και των συστημάτων ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Α΄τρόπος)

5.6.1.1.1.4 <u>Σενάριο λειτουργίας Δ: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Β΄ τρόπος)</u>

Το σενάριο αυτό αποτελεί τον δεύτερο, εναλλακτικό τρόπο καταγραφής των δεδομένων και συστημάτων ανά υπηρεσία. Για τον Β' τρόπο καταγραφής χρησιμοποιείται το γραφικό περιβάλλον του Συστήματος Διαχείρισης Επιχειρησιακών Διαδικασιών.

Το συγκεκριμένο σενάριο περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 25):

1) Είσοδος στο υποσύστημα χαρτογράφησης (βλέπει μόνο τις υπηρεσίες για τις οποίες είναι υπεύθυνος).
2) Επιλογή η-υπηρεσίας.
3) Είσοδος στο Σύστημα Διαχείρισης Επιχειρησιακών Διαδικασιών.
4) Καταγραφή των δεδομένων εισόδου και εξόδου που σχετίζονται με την υπηρεσία.
5) Καταγραφή των συστημάτων που χρησιμοποιούνται από την υπηρεσία.
6) Έξοδος.



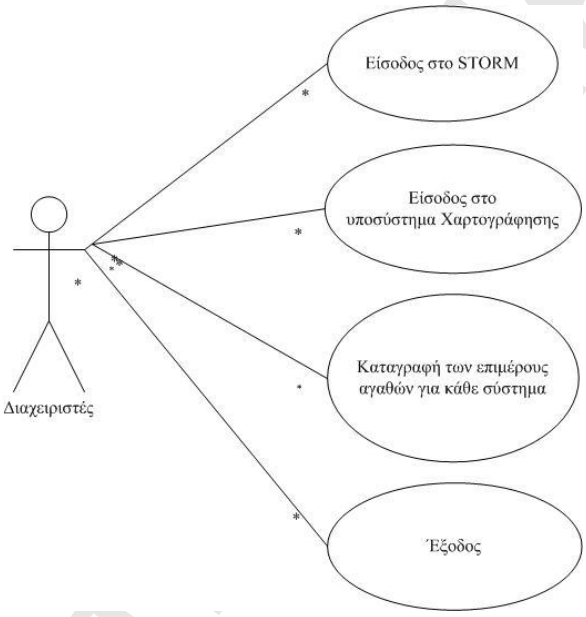
Εικόνα 25: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διοικητικούς Υπευθύνους (Β΄ τρόπος)

5.6.1.1.1.5 Σενάριο λειτουργίας Ε: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διαχειριστές

Το σενάριο αυτό εκτελείται μετά την καταγραφή των συστημάτων, ώστε οι Διαχειριστές να καταγράψουν αναλυτικά για κάθε σύστημα, σε χαμηλό επίπεδο τα επιμέρους συστατικά του (υλικό,

λογισμικό κτλ). Περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 26):

1) Είσοδος στο υποσύστημα χαρτογράφησης (κάθε διαχειριστής βλέπει μόνο τις υπηρεσίες στις οποίες έχει αντιστοιχηθεί από τους διοικητικούς υπεύθυνους).
2) Καταγραφή των επιμέρους αγαθών για κάθε σύστημα. Αυτό θα γίνεται με τη χρήση έτοιμων φορμών, οι οποίες δίνουν τη δυνατότητα αντιστοίχισης κάθε αγαθού σε έτοιμες κατηγορίες. Με τον τρόπο αυτό, κάθε σύστημα θα πρέπει να αποτελείται από συγκεκριμένα συστατικά.
3) Έξοδος.



Εικόνα 26: Καταγραφή των πληροφοριακών αγαθών ανά υπηρεσία από τους Διαχειριστές

5.6.1.2 Υπηρεσία Αποτίμησης Επιπτώσεων Ασφάλειας

Στόχος της συγκεκριμένης υπηρεσίας είναι η αποτίμηση του κάθε αγαθού σε περίπτωση απώλειας της ασφάλειας. Κάθε χρήστης και για κάθε αγαθό θα καλείται να πραγματοποιήσει την αποτίμηση των επιπτώσεων ασφάλειας επιλέγοντας τις κατηγορίες επιπτώσεων και τον βαθμό αποτίμησης σύμφωνα με την κλίμακα της μεθοδολογίας (Κεφάλαιο 4). Έπειτα από την ολοκλήρωση της αποτίμησης όλων των εμπλεκόμενων χρηστών, θα υπάρχει η δυνατότητα προβολής των αποτελεσμάτων, τόσο σε ηλεκτρονική μορφή όσο και σε εκτυπώσιμη μορφή.

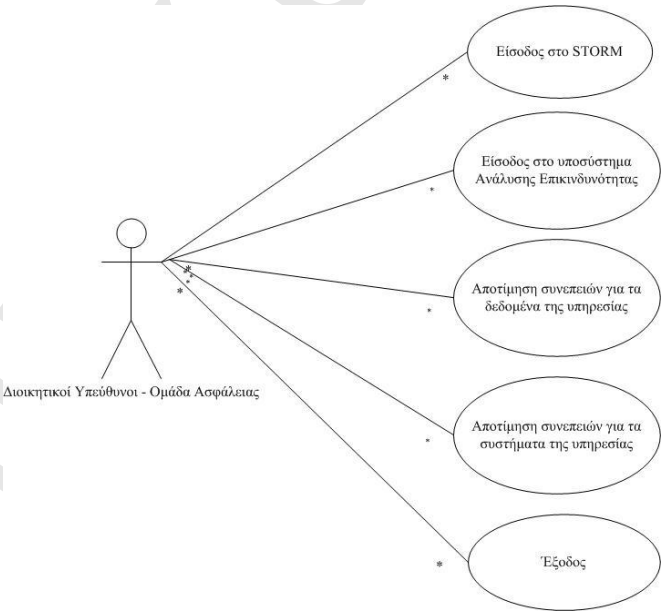
5.6.1.2.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες με διαφορετικά σενάρια χρήσης, τα οποία περιγράφονται παρακάτω.

5.6.1.2.1.1 Σενάριο λειτουργίας Α: Αποτίμηση των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 27):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας (εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο).
2) Αποτίμηση επιπτώσεων ασφάλειας για τα δεδομένα της υπηρεσίας (με τη χρήση των ηερωτηματολογίων).
3) Αποτίμηση επιπτώσεων ασφάλειας για τα συστήματα της υπηρεσίας (με τη χρήση των ηερωτηματολογίων).
4) Έξοδος.

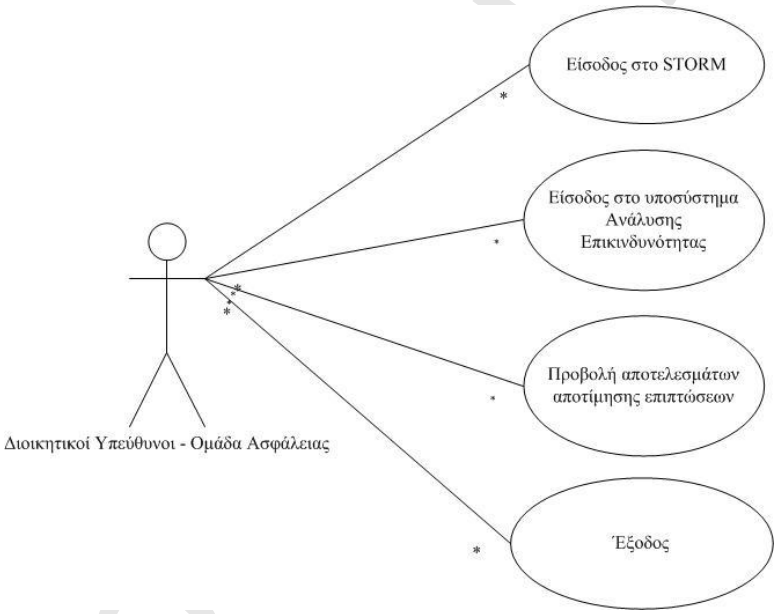


Εικόνα 27: Αποτίμηση των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας ασφάλειας και τα μέλη της Διοίκησης

5.6.1.2.1.2 Σενάριο λειτουργίας Β: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 28):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας (εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο).
2) Επιλογή προβολής αποτελεσμάτων αποτίμησης επιπτώσεων (με τη βοήθεια μενού και γραφημάτων για ατομικά / ομαδικά / τελικά αποτελέσματα).
3) Έξοδος.



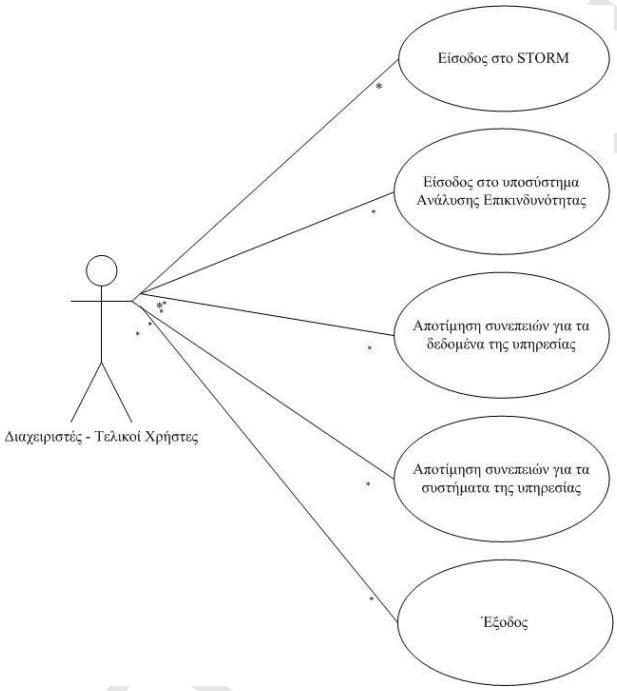
Εικόνα 28: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.2.1.3 Σενάριο λειτουργίας Γ: Αποτίμηση των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 29):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας (εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον διοικητικό υπεύθυνο).

2) Αποτίμηση επιπτώσεων ασφάλειας για τα δεδομένα της υπηρεσίας (με τη χρήση ηερωτηματολογίων).
3) Αποτίμηση επιπτώσεων ασφάλειας για τα συστήματα της υπηρεσίας (με τη χρήση ηερωτηματολογίων).
4) Έξοδος.

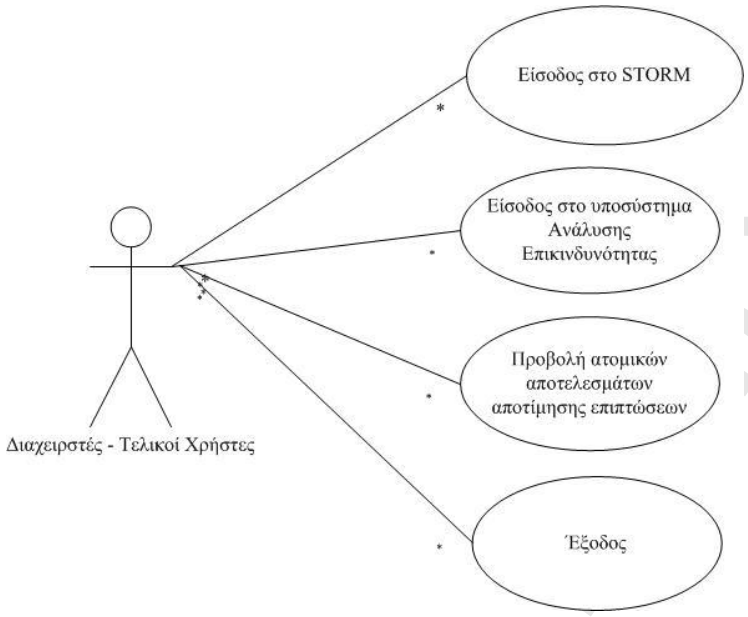


Εικόνα 29: Αποτίμηση των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες

5.6.1.2.1.4 <u>Σενάριο λειτουργίας Δ: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες</u>

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 30):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας (εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον διοικητικό υπεύθυνο).
2) Επιλογή προβολής ατομικών αποτελεσμάτων αποτίμησης επιπτώσεων (με τη βοήθεια μενού).
3) Έξοδος.



Εικόνα 30: Προβολή των αποτελεσμάτων των επιπτώσεων ασφάλειας από τους Διαχειριστές και τους Τελικούς Χρήστες

5.6.1.3 Υπηρεσία Αποτίμησης Απειλών

Με τη βοήθεια της συγκεκριμένης υπηρεσίας, οι χρήστες του συστήματος STORM θα είναι σε θέση να πραγματοποιήσουν την αποτίμηση των απειλών κάθε αγαθού. Πιο συγκεκριμένα, υπάρχει περιγραφή των βαθμών αποτίμησης απειλών καθώς και παρουσιάζεται για κάθε αγαθό η λίστα με τις πιθανές απειλές που του αντιστοιχούν (σύμφωνα με το Παράρτημα 8.2). Κάθε χρήστης για κάθε αγαθό που του αντιστοιχεί θα δίνει το βαθμό αποτίμησης για τις απειλές οι οποίες αντιστοιχούν σε αυτό. Ταυτόχρονα, υπάρχει η δυνατότητα προβολής τόσο των ατομικών όσο και των τελικών ομαδικών αποτελεσμάτων καθώς και η δυνατότητα εκτύπωσής τους.

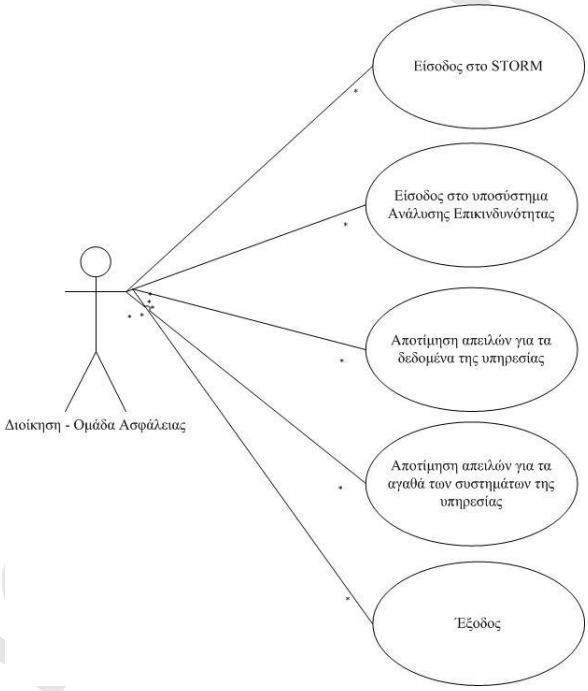
5.6.1.3.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες, με διαφορετικά σενάρια χρήσης τα οποία περιγράφονται παρακάτω.

5.6.1.3.1.1 Σενάριο λειτουργίας Α: Αποτίμηση των απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 31):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο.
2) Αποτίμηση απειλών για τα δεδομένα της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
3) Αποτίμηση απειλών για τα αγαθά των συστημάτων (δηλαδή το υλικό και λογισμικό από τα οποία αποτελούνται τα συστήματα) της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
4) Έξοδος.

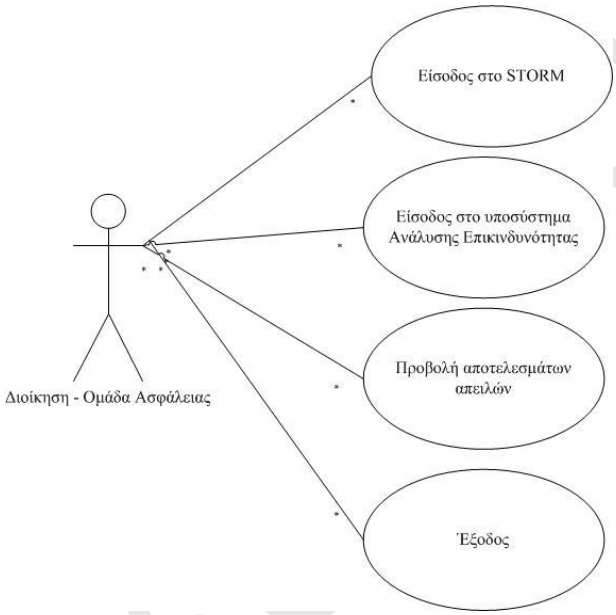


Εικόνα 31: Αποτίμηση των απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.3.1.2 Σενάριο λειτουργίας Β: Προβολή αποτελεσμάτων αποτίμησης απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 32):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο.
2) Επιλογή προβολής αποτελεσμάτων αποτίμησης απειλών (με τη βοήθεια μενού και γραφημάτων).
3) Έξοδος.

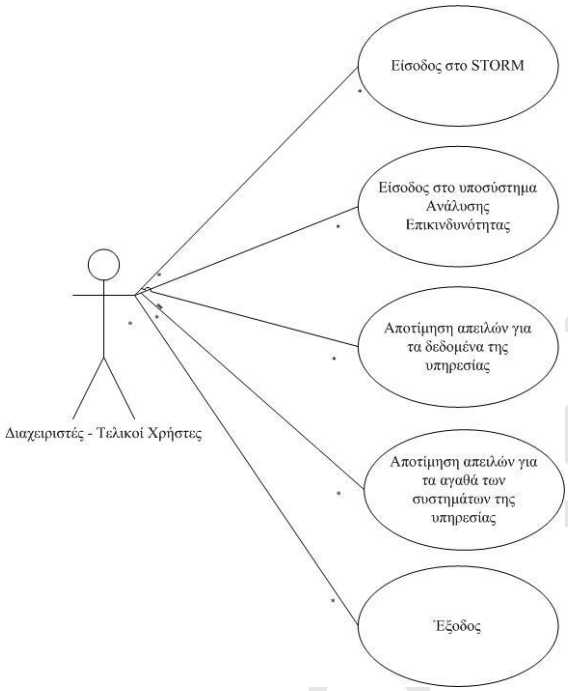


Εικόνα 32: Προβολή αποτελεσμάτων αποτίμησης απειλών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.3.1.3 Σενάριο λειτουργίας Γ: Αποτίμηση των απειλών από τους Διαχειριστές και τους Τελικούς Χρήστες

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 33):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον διοικητικό υπεύθυνο.
2) Αποτίμηση απειλών για τα δεδομένα της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
3) Αποτίμηση απειλών για τα αγαθά των συστημάτων (δηλαδή το υλικό και λογισμικό από τα οποία αποτελούνται τα συστήματα της υπηρεσίας) με τη χρήση η-ερωτηματολογίων.
4) Έξοδος.



Εικόνα 33: Αποτίμηση των απειλών από τους Διαχειριστές και τους Τελικούς Χρήστες

5.6.1.4 Υπηρεσία Αποτίμησης Αδυναμιών

Η υπηρεσία Αποτίμησης Αδυναμιών υλοποιεί το Βήμα 4.1: "Προσδιορισμός αδυναμιών", το Βήμα 4.2: Θεωρητική Αποτίμηση Αδυναμιών, μέρος του Βήματος 4.3 Πρακτική Αποτίμηση Αδυναμιών καθώς επίσης και το Βήμα 4.4 Συνολική Αποτίμηση Αδυναμιών (όπως παρουσιάστηκαν στο Κεφάλαιο 4). Πιο συγκεκριμένα υπάρχει η δυνατότητα περιγραφής της κλίμακας αδυναμιών ώστε να είναι σε θέση οι χρήστες να προχωρήσουν στην αποτίμηση των αδυναμιών. Ταυτόχρονα παρουσιάζονται οι αντιστοιχίσεις των αγαθών / απειλών / αδυναμιών ώστε οι χρήστες να πραγματοποιούν τη θεωρητική και την πρακτική αποτίμηση των αδυναμιών για κάθε αγαθό. Τέλος, σε συνδυασμό με την πληροφορία που συλλέγεται από την υπηρεσία Ανίχνευσης Αδυναμιών (όπου αυτό απαιτείται), παρουσιάζονται τα συνολικά αποτελέσματα αποτίμησης αδυναμιών των αγαθών $FV(A_i)$ τόσο σε ηλεκτρονική όσο και σε εκτυπώσιμη μορφή.

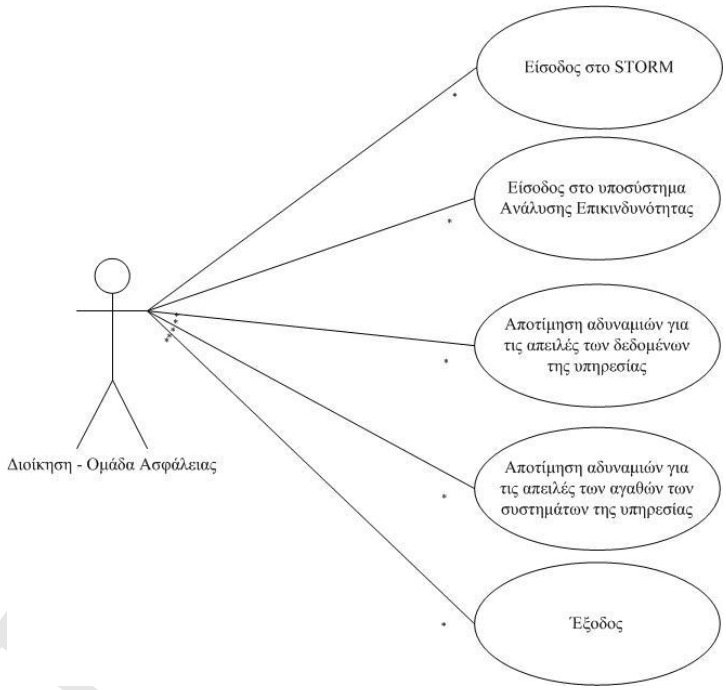
5.6.1.4.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες, με διαφορετικά σενάρια χρήσης τα οποία περιγράφονται παρακάτω.

5.6.1.4.1.1 Σενάριο λειτουργίας Α: Αποτίμηση των αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 34):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο.
2) Αποτίμηση αδυναμιών για τις απειλές των δεδομένων της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
3) Αποτίμηση αδυναμιών για τις απειλές των αγαθών των συστημάτων της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
4) Έξοδος.

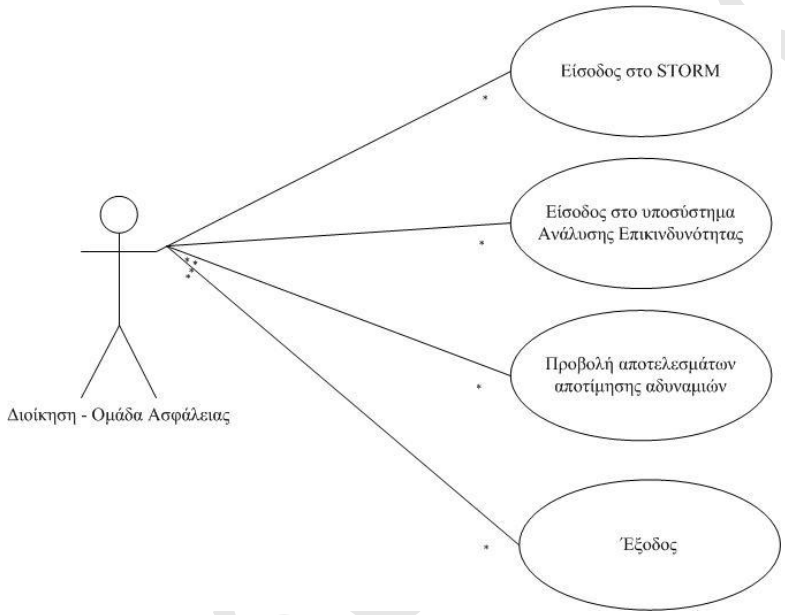


Εικόνα 34: Αποτίμηση των αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.4.1.2 Σενάριο λειτουργίας Β: Προβολή αποτελεσμάτων αποτίμησης αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 35):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο).
2) Επιλογή προβολής αποτελεσμάτων αποτίμησης αδυναμιών (με τη βοήθεια μενού και γραφημάτων).
3) Έξοδος.

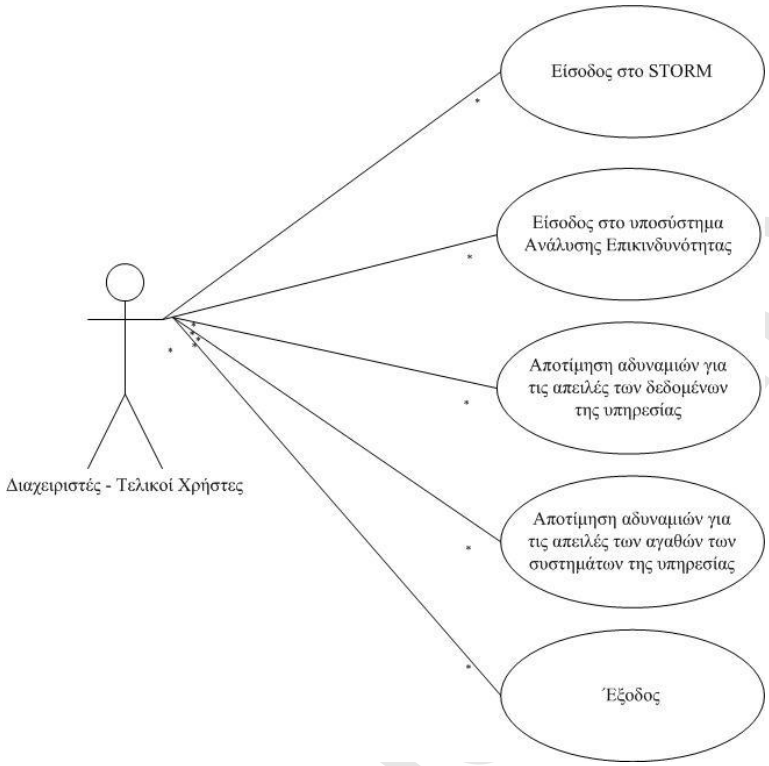


Εικόνα 35: Προβολή αποτελεσμάτων αποτίμησης αδυναμιών από τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.4.1.3 Σενάριο λειτουργίας Γ: Αποτίμηση των αδυναμιών από τους Διαχειριστές και τους Τελικούς Χρήστες

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 36):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον διοικητικό υπεύθυνο.
2) Αποτίμηση αδυναμιών για τις απειλές των δεδομένων της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
3) Αποτίμηση αδυναμιών για τις απειλές των αγαθών των συστημάτων της υπηρεσίας με τη χρήση η-ερωτηματολογίων.
4) Έξοδος.



Εικόνα 36: Αποτίμηση των αδυναμιών από τους Διαχειριστές και τους Τελικούς Χρήστες

5.6.1.5 Υπηρεσία Αποτίμησης Επικινδυνότητας

Στην υπηρεσία Αποτίμησης Επικινδυνότητας, οι χρήστες είναι σε θέση να δουν τη λίστα με τα αποτελέσματα της αποτίμησης επικινδυνότητας των αγαθών του υπό εξέταση ΠΣ ταξινομημένα με βάση το βαθμό επικινδυνότητάς τους. Τα αποτελέσματα αυτά θα χρησιμοποιηθούν ως είσοδος στην υπηρεσία Διαχείρισης Επικινδυνότητας.

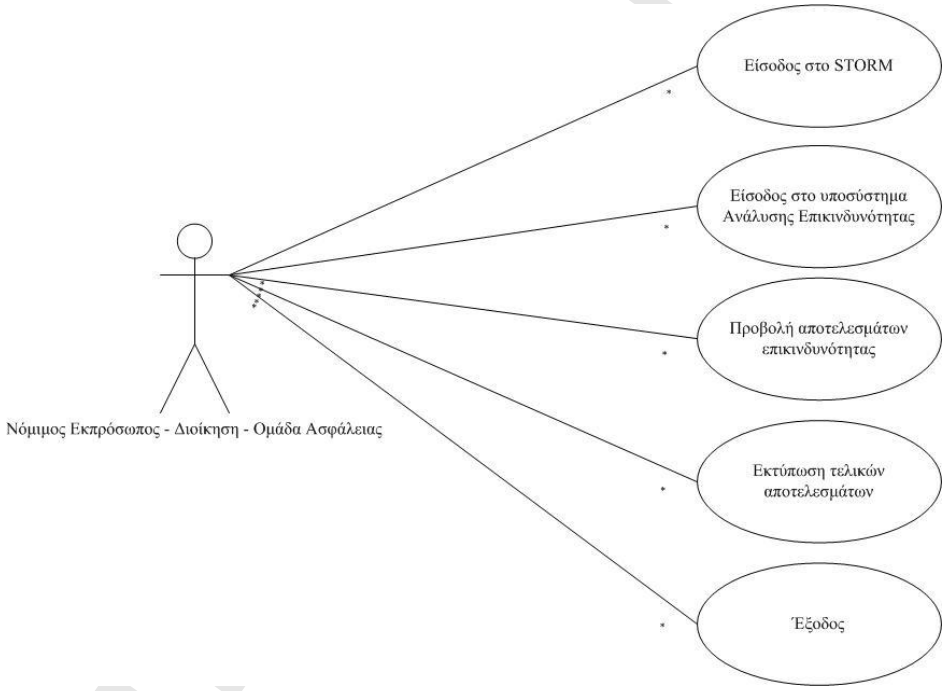
5.6.1.5.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν ο Νόμιμος Εκπρόσωπος, τα μέλη της Ομάδας Ασφάλειας και τα κατάλληλα μέλη της Διοίκησης. Σκοπός της υπηρεσίας είναι η τελική προβολή των αποτελεσμάτων επικινδυνότητας. Κρίνεται σκόπιμο να έχουν πρόσβαση σε αυτά τα δεδομένα μόνο όσοι θα πρέπει, λόγω του ρόλου τους, να γνωρίζουν αυτή την ευαίσθητη πληροφορία.

5.6.1.5.1.1 Προβολή των αποτελεσμάτων επικινδυνότητας από τον Νόμιμο Εκπρόσωπο, τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 37):

1) Είσοδος στο Υποσύστημα Ανάλυσης Επικινδυνότητας όπου εμφανίζονται μόνο οι υπηρεσίες στις οποίες έχουν αντιστοιχηθεί οι χρήστες από τον νόμιμο εκπρόσωπο.
2) Επιλογή προβολής αποτελεσμάτων αποτίμησης επικινδυνότητας (με τη βοήθεια μενού και γραφημάτων).
3) Επιλογή εκτύπωσης τελικών αποτελεσμάτων (με τη βοήθεια μενού)
4) Έξοδος.



Εικόνα 37: Προβολή των αποτελεσμάτων επικινδυνότητας από τον Νόμιμο Εκπρόσωπο, τα μέλη της Ομάδας Ασφάλειας και τα μέλη της Διοίκησης

5.6.1.6 Υπηρεσίες Διαχείρισης Επικινδυνότητας

Οι υπηρεσίες Διαχείρισης Επικινδυνότητας αποτελούνται από την υπηρεσία *Προτεινόμενα Μέτρα Ασφάλειας* και την υπηρεσία *Επιλογή Κατάλληλών Μέτρων Ασφάλειας* οι οποίες υλοποιούν τα Βήματα 6.1 και 6.2 αντίστοιχα, της Φάσης 6: "Μέτρα Προστασίας - Σχέδιο Ασφάλειας" της

μεθοδολογίας του Κεφαλαίου 4. Πιο συγκεκριμένα, στην υπηρεσία Προτεινόμενα Μέτρα Ασφάλειας παρουσιάζονται τα μέτρα τα οποία προτείνονται από τη μεθοδολογία, λαμβάνοντας υπόψη τα αποτελέσματα των προηγούμενων υπηρεσιών. Τα μέτρα αυτά είναι σε μορφή λίστας και κατηγοριοποιημένα με βάση το είδος τους και το είδος των απειλών που δύναται να αντιμετωπίσουν. Με την υπηρεσία *Επιλογή Κατάλληλών Μέτρων Ασφάλειας* οι αρμόδιοι χρήστες (σύμφωνα με τις ομάδες που καθορίστηκαν στο Κεφάλαιο 5) είναι σε θέση να πραγματοποιήσουν τις κατάλληλες συγκρίσεις (σύμφωνα με την αντίστοιχη φάση της μεθοδολογίας) ώστε να επιλέξουν τα μέτρα τα οποία είναι πιο κοντά στις δυνατότητές τους και στις απαιτήσεις τους (οικονομικές, τεχνολογικές). Και οι δύο παραπάνω υπηρεσίες διαχείρισης επικινδυνότητας διαθέτουν δυνατότητες αποτύπωσης των αποτελεσμάτων τους τόσο σε ηλεκτρονική όσο και εκτυπώσιμη μορφή.

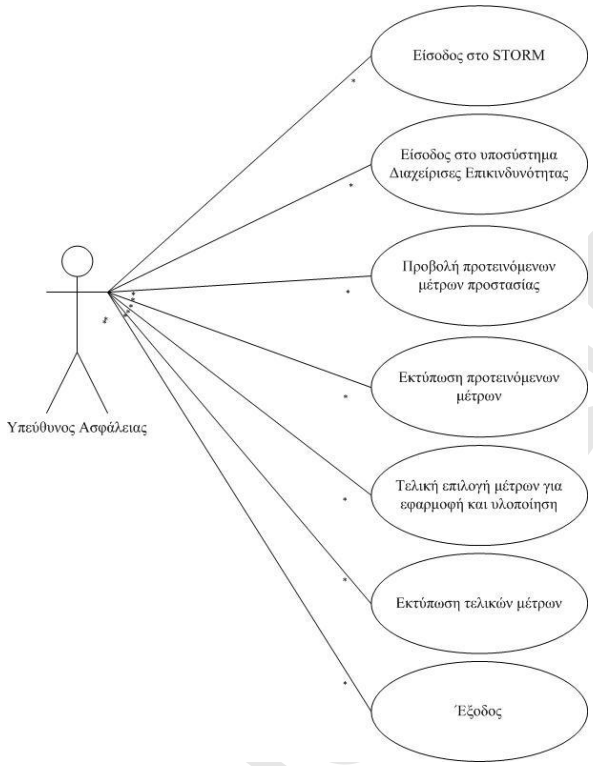
5.6.1.6.1 Λειτουργικότητα

Στις υπηρεσίες διαχείρισης επικινδυνότητας συμμετέχει μόνο ο Υπεύθυνος Ασφάλειας του οργανισμού, ο οποίος μπορεί να επιλέξει τα προτεινόμενα και τα τελικά μέτρα ασφάλειας με τη βοήθεια της Ομάδας Ασφάλειας και την τελική έγκριση του Νόμιμου Εκπροσώπου του οργανισμού. Η επιλογή των μέτρων ασφάλειας απαιτεί εξειδικευμένη γνώση σε θέματα ασφάλειας, και γι’ αυτό το λόγο, το υποσύστημα αυτό είναι προσβάσιμο μόνο από τον Υπεύθυνο Ασφάλειας.

5.6.1.6.1.1 Προβολή προτεινόμενων και επιλογή τελικών μέτρων ασφάλειας από τον Υπεύθυνο Ασφάλειας

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 38):

1) Είσοδος στο Υποσύστημα Διαχείρισης Επικινδυνότητας.
2) Προβολή προτεινόμενων μέτρων ασφάλειας, με τη βοήθεια μενού.
3) Επιλογή εκτύπωσης προτεινόμενων μέτρων, με τη βοήθεια μενού.
4) Τελική επιλογή μέτρων για εφαρμογή και υλοποίηση.
5) Επιλογή εκτύπωσης τελικών μέτρων, με τη βοήθεια μενού.
6) Έξοδος.



Εικόνα 38: Προβολή και επιλογή τελικών μέτρων ασφάλειας από τον Υπεύθυνο Ασφάλειας

5.6.2 Υπηρεσία Διαχείρισης Εγγράφων Ασφάλειας

Η συγκεκριμένη υπηρεσία έχει ως στόχο τη διαχείριση των εγγράφων ασφάλειας. Πιο συγκεκριμένα η υπηρεσία αυτή δίνει τη δυνατότητα στους χρήστες (ανάλογα με το ρόλο τους στο σύστημα) να δημιουργούν, να επεξεργάζονται και να ανανεώνουν όλα τα έγγραφα ασφάλειας όπως την πολιτική ασφάλειας, το σχέδιο αποκατάστασης καταστροφών και το σχέδιο επιχειρησιακής συνέχειας. Οι χρήστες είναι σε θέση να ενημερώνονται για τους ρόλους και τις αρμοδιότητές τους σε περίπτωση ενεργοποίησης των σχεδίων ασφάλειας, καθώς και για τις διαδικασίες που απαιτούνται για την ανάκαμψη της ομαλής λειτουργίας του Πληροφοριακού Συστήματος. Όλες οι φόρμες της υπηρεσίας είναι διαθέσιμες τόσο σε ηλεκτρονική όσο και σε εκτυπώσιμη μορφή.

5.6.2.1.1 Λειτουργικότητα

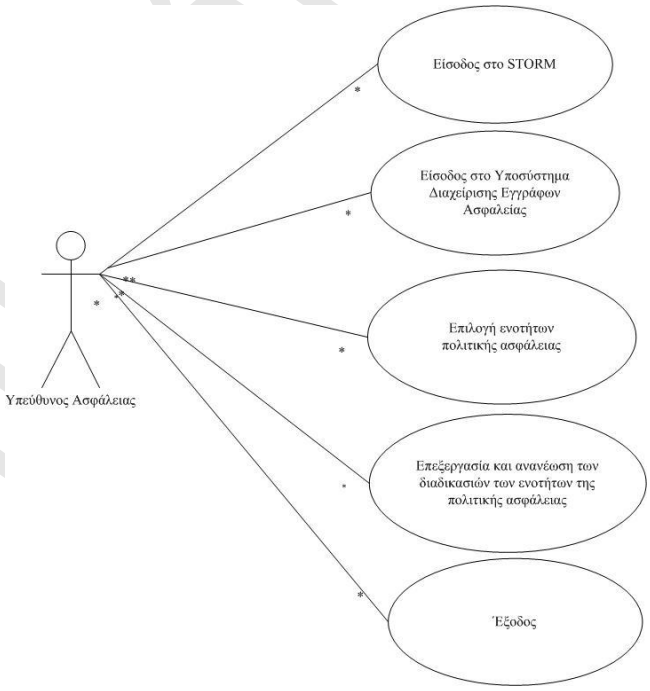
Στην υπηρεσία αυτή συμμετέχουν ο Νόμιμος Εκπρόσωπος, τα μέλη της Ομάδας Ασφάλειας, τα κατάλληλα μέλη της Διοίκησης και οι Τελικοί Χρήστες. Σκοπός της υπηρεσίας είναι η δημιουργία, η ανανέωση και η προβολή της πολιτικής ασφάλειας, των σχεδίων αποκατάστασης καταστροφών και

της επιχειρησιακής συνέχειας. Κρίνεται σκόπιμο, να έχουν πρόσβαση σε αυτά τα δεδομένα, μόνο όσοι θα πρέπει λόγω του ρόλου τους να γνωρίζουν αυτή την ευαίσθητη πληροφορία. Επίσης σημειώνεται ότι μόνο τα μέλη της Ομάδας ασφάλειας έχουν την δυνατότητα να ενημερώνουν τις διαδικασίες ασφάλειας μέσω των κατάλληλων ηλεκτρονικών φορμών οι οποίες παρέχονται από την συγκεκριμένη υπηρεσία. Οι υπόλοιπες ομάδες έχουν την δυνατότητα μόνο να δουν ποιες είναι οι διαδικασίες και να εκτυπώνουν ή να αποθηκεύνουν την δημόσια έκδοση της πολιτικής ασφάλειας και τα βήματα των σχεδίων αποκατάστασης καταστροφής και επιχειρησιακής συνέχειας που τους αφορούν / εμπλέκουν.

5.6.2.1.1.1 Σενάριο λειτουργίας Α: Δημιουργία της πολιτικής ασφάλειας από τον Υπεύθυνο Ασφάλειας

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 39):

1) Είσοδος στο Υποσύστημα Διαχείρισης Εγγράφων Ασφαλείας.
2) Επιλογή ενοτήτων πολιτικής ασφάλειας, με τη βοήθεια μενού.
3) Επεξεργασία και ανανέωση των διαδικασιών των ενοτήτων της πολιτικής ασφάλειας.
4) Έξοδος.

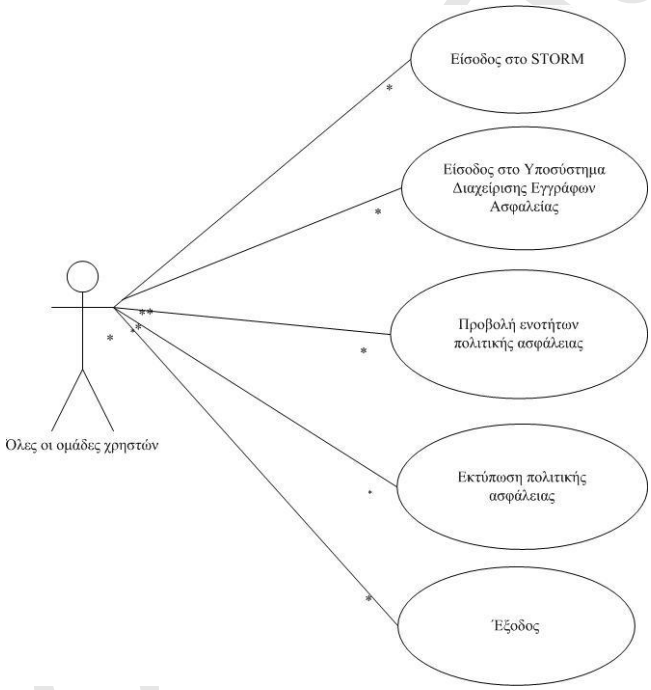


Εικόνα 39: Δημιουργία της πολιτικής ασφάλειας από τον Υπεύθυνο Ασφάλειας

5.6.2.1.1.2 Σενάριο λειτουργίας Β: Προβολή της πολιτικής ασφάλειας από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 40):

1) Είσοδος στο Υποσύστημα Διαχείρισης Εγγράφων Ασφαλείας.
2) Προβολή ενοτήτων πολιτικής ασφάλειας, με τη βοήθεια μενού.
3) Εκτύπωση πολιτικής ασφάλειας.
4) Έξοδος.



Εικόνα 40: Προβολή της πολιτικής ασφάλειας από όλες τις ομάδες χρηστών

5.6.3 Συνεργατικές Υπηρεσίες STORM

Οι Συνεργατικές Υπηρεσίες προσφέρουν τη δυνατότητα στους χρήστες να επικοινωνήσουν μέσα από το σύστημα STORM ώστε να είναι πιο άμεση και πιο παραγωγική η επίτευξη κοινών στόχων και η συνεργασία των χρηστών. Συγκεκριμένα, οι ομάδες χρηστών έχουν στη διάθεσή τους τις υπηρεσίες που περιγράφονται στις ενότητες που ακολουθούν.

5.6.3.1 Forum

Μέσω της υπηρεσίας Forum είναι δυνατή η ταυτόχρονη ενημέρωση πολλών χρηστών για θέματα ασφάλειας ΠΣ, για επίλυση καθημερινών τεχνικών προβλημάτων κλπ.. Επίσης, μέσω αυτής της υπηρεσίας δίνεται ένα βήμα επικοινωνίας στον κάθε χρήστη να υποβάλλει ερωτήσεις για τυχόν προβλήματα που αντιμετωπίζει σχετικά με το STORM ώστε να λάβει όσο το δυνατόν ταχύτερα απαντήσεις από την αρμόδια ομάδα χρηστών. Οι παραπάνω λειτουργικότητες καθιστούν αυτήν την υπηρεσία ένα πολύτιμο εργαλείο συνεργατικότητας και μαζικής ενημέρωσης.

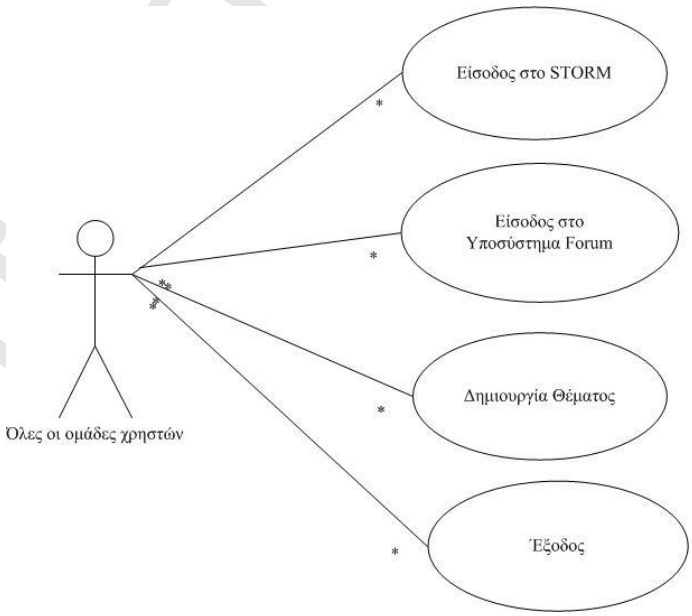
5.6.3.1.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλες οι ομάδες χρηστών του STORM, δηλαδή τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες.

5.6.3.1.1.1 Σενάριο λειτουργίας Α: Δημιουργία Θέματος από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 41):

1) Είσοδος στο υποσύστημα Forum.
2) Δημιουργία Θέματος.
3) Έξοδος.

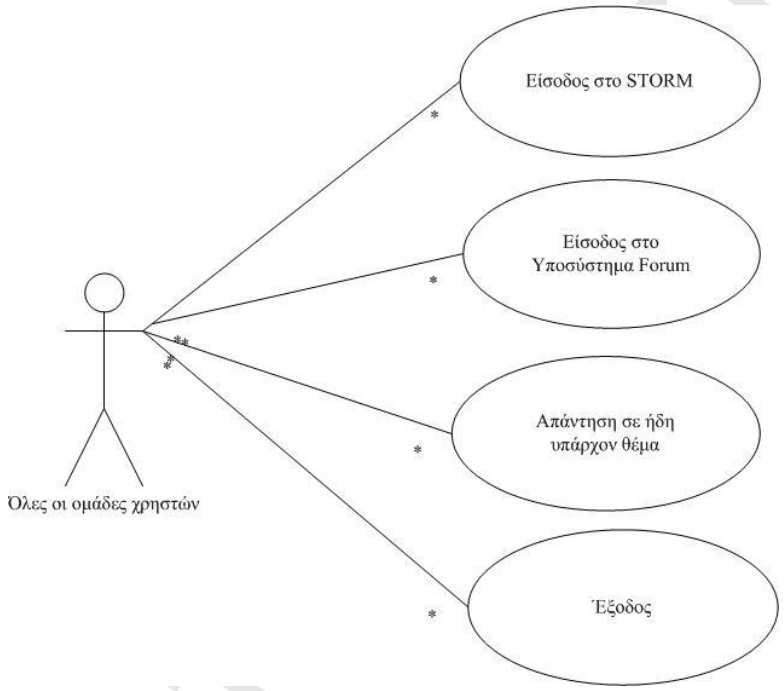


Εικόνα 41: Δημιουργία Θέματος από όλες τις ομάδες χρηστών

5.6.3.1.1.2 Σενάριο λειτουργίας Β: Απάντηση σε Θέμα του Forum από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 42):

1) Είσοδος στο υποσύστημα Forum.
2) Απάντηση σε ήδη υπάρχον θέμα.
3) Έξοδος.



Εικόνα 42: Απάντηση σε Θέμα του Forum από όλες τις ομάδες χρηστών

5.6.3.2 Wiki

Μέσω της υπηρεσίας Wiki δίνεται η δυνατότητα σε αρμόδιους χρήστες να δημιουργήσουν / επεξεργαστούν πληροφορία μέσα στο σύστημα ώστε να επεκτείνουν/ενημερώσουν τα απαραίτητα έγγραφα ασφαλείας πετυχαίνοντας τον μέγιστο βαθμό συνεργατικότητας. Πιο συγκεκριμένα η υπηρεσία wiki επιτρέπει στους χρήστες να ενημερώνονται για τον ορθό τρόπο εφαρμογής της μεθοδολογίας STORM-RM, να βρίσκουν πληροφορίες για τις διαδικασίες υλοποίησης των σχεδίων αποκατάστασης καταστροφών/επιχειρησιακής συνέχειας κτλ.

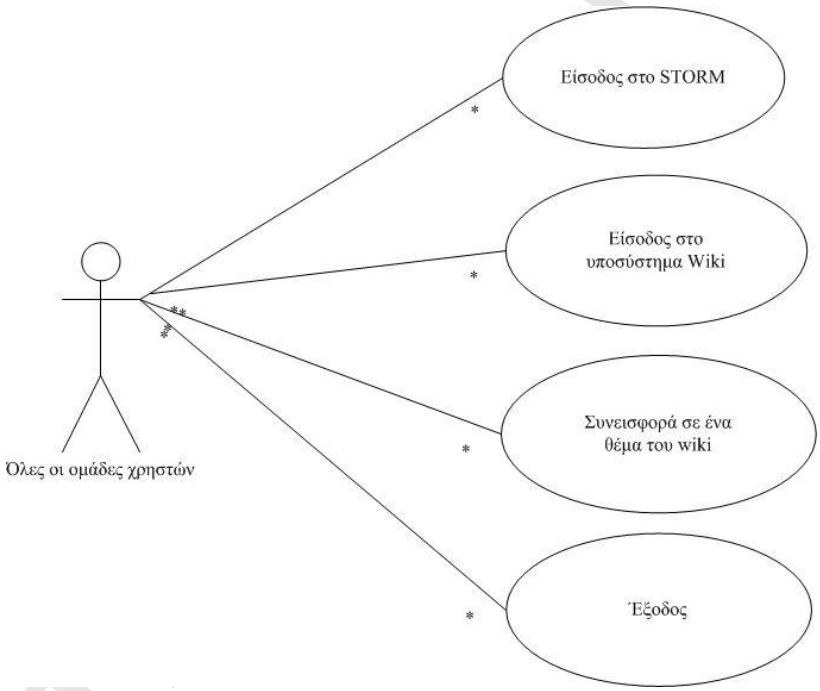
5.6.3.2.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλες οι ομάδες χρηστών του S-PORT, δηλαδή τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες.

5.6.3.2.1.1 Συνεισφορά στο wiki από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 43):

1) Είσοδος στο υποσύστημα Wiki.
2) Συνεισφορά σε ένα θέμα του wiki (π.χ. προσθήκη/επεξεργασία/διαγραφή περιεχομένου).
3) Έξοδος.



Εικόνα 43: Συνεισφορά στο wiki από όλες τις ομάδες χρηστών

5.6.3.3 Chat rooms

Η υπηρεσία Chat rooms προσφέρει τον αμεσότερο βαθμό επικοινωνίας μεταξύ των χρηστών (real-time) και είναι απαραίτητη σε καταστάσεις που απαιτούν ελάχιστο χρόνο απόκρισης. Παράλληλα, η

υπηρεσία αυτή συμβάλλει στη συνεργατική εκπόνηση των βημάτων της μεθοδολογίας STORM από τις επιμέρους ομάδες χρηστών, καθώς και τη μεταφορά τεχνογνωσίας μεταξύ τους.

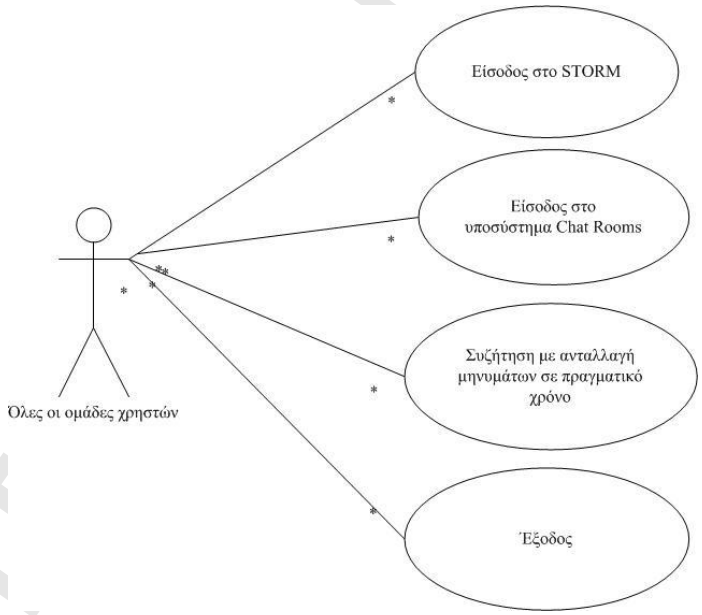
5.6.3.3.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλες οι ομάδες χρηστών του STORM, δηλαδή τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες.

5.6.3.3.1.1 Συζήτηση με ανταλλαγή μηνυμάτων σε πραγματικό χρόνο από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 44):

1) Είσοδος στο υποσύστημα Chat Rooms.
2) Συζήτηση με ανταλλαγή μηνυμάτων σε πραγματικό χρόνο.
3) Έξοδος.



Εικόνα 44: Συζήτηση με ανταλλαγή μηνυμάτων σε πραγματικό χρόνο από όλες τις ομάδες χρηστών

5.6.3.4 Blog

Με τη βοήθεια της υπηρεσίας Blog, οι χρήστες του συστήματος STORM είναι σε θέση να αναρτούν νέες δημοσιεύσεις και ενημερώσεις σχετικές με την ασφάλεια ΠΣ τη μορφή ημερολογίου. Η υπηρεσία μπορεί να χρησιμοποιηθεί για την ενίσχυση της ενασχόλησης των χρηστών με την ασφάλεια μέσω τακτικών ενημερώσεων, αλλά και για την ενημέρωσή τους για την τρέχουσα πορεία της ανάλυσης και διαχείρισης επικινδυνότητας και ενδιάμεσα αποτελέσματα.

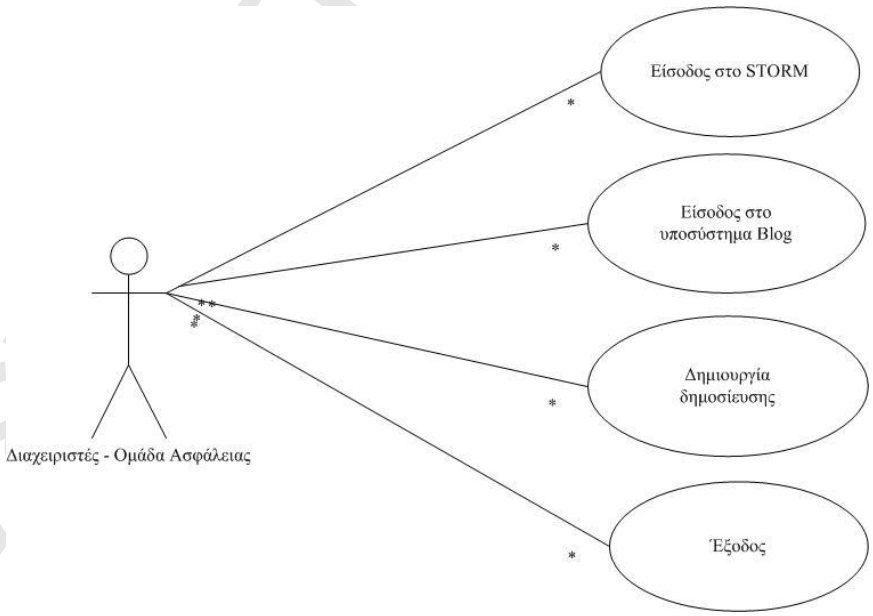
5.6.3.4.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλες οι ομάδες χρηστών του STORM, δηλαδή τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες.

5.6.3.4.1.1 Σενάριο λειτουργίας Α: Δημιουργία δημοσίευσης από τους Διαχειριστές και τα μέλη της Ομάδας ασφάλειας

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 45):

1) Είσοδος στο υποσύστημα Blog.
2) Δημιουργία Δημοσίευσης.
3) Έξοδος.

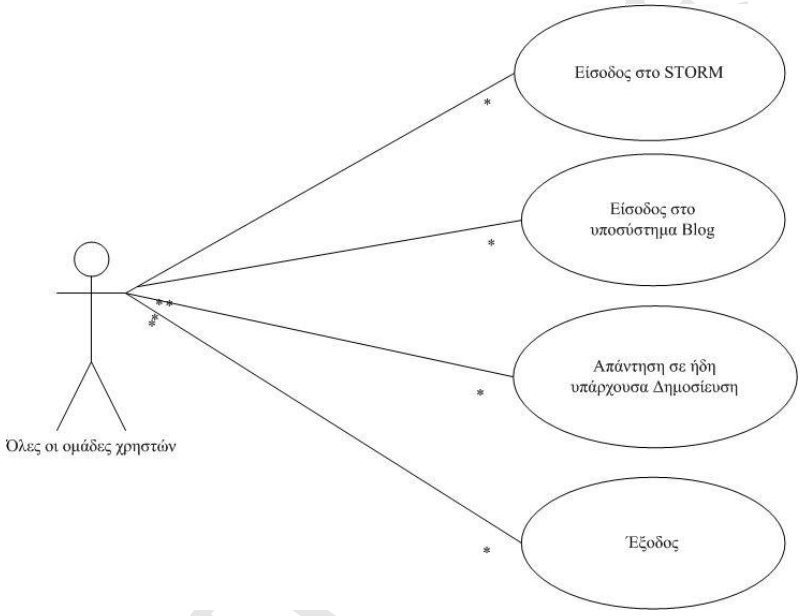


Εικόνα 45: Δημιουργία δημοσίευσης από τους Διαχειριστές και τα μέλη της Ομάδας ασφάλειας

5.6.3.4.1.2 Σενάριο λειτουργίας Β: Απάντηση σε Δημοσίευση του Blog από όλες τις ομάδες χρηστών

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 46):

1) Είσοδος στο υποσύστημα Blog.
2) Απάντηση σε ήδη υπάρχουσα Δημοσίευση.
3) Έξοδος.



Εικόνα 46: Απάντηση σε Δημοσίευση του Blog από όλες τις ομάδες χρηστών

5.6.3.5 Ηλεκτρονική Βιβλιοθήκη

Η υπηρεσία αυτή δίνει τη δυνατότητα στους χρήστες (ανάλογα με τον ρόλο τους στο σύστημα) να δημιουργούν, να επεξεργάζονται και να ανανεώνουν έγγραφα τα οποία αφορούν στην ασφάλεια Πληροφοριακών Συστημάτων (όπως βέλτιστες πρακτικές, σχετική νομοθεσία, μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας κλπ.) καθώς και άλλα έγγραφα (όπως τεχνικές οδηγίες, οδηγίες εγκατάστασης λογισμικού κλπ.) τα οποία πρόκειται να διευκολύνουν την καθημερινότητα των χρηστών του ΠΣ. Όλα τα έγγραφα της βιβλιοθήκης είναι διαθέσιμα σε ηλεκτρονική μορφή και οργανωμένα σε θεματικές κατηγορίες με βάση την ταξονομία η οποία περιγράφεται στο Παράρτημα ΙΙΙ.

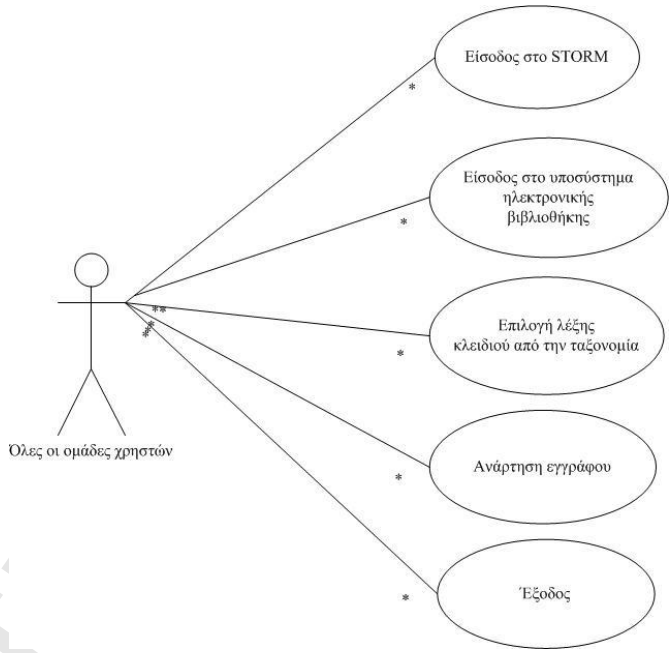
5.6.3.5.1 Λειτουργικότητα

Στην υπηρεσία αυτή συμμετέχουν όλες οι ομάδες χρηστών του STORM, δηλαδή τα μέλη της Ομάδας Ασφάλειας, τα μέλη της Διοίκησης, οι Διαχειριστές και οι Τελικοί Χρήστες.

5.6.3.5.1.1 Σενάριο λειτουργίας Α: Ανάρτηση εγγράφου

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 47):

1) Είσοδος στο υποσύστημα ηλεκτρονικής βιβλιοθήκης.
2) Επιλογή λέξης κλειδιού από την ταξονομία.
3) Ανάρτηση εγγράφου.
4) Έξοδος.



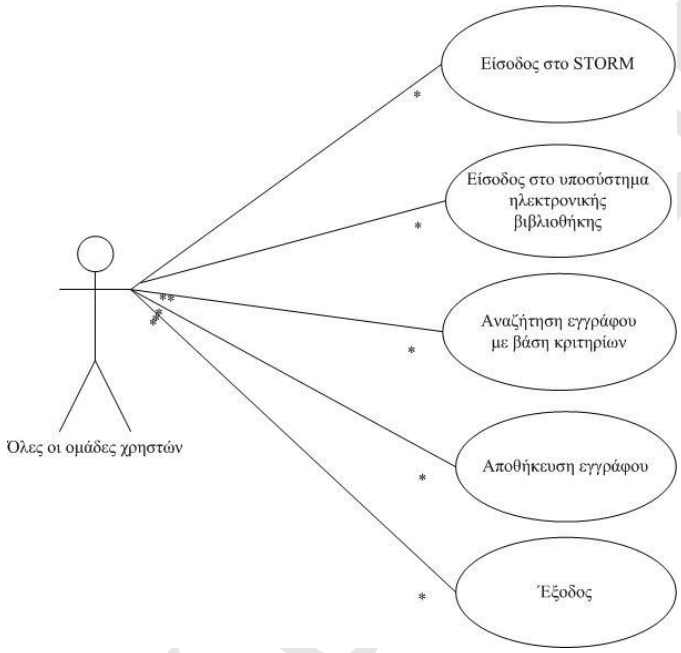
Εικόνα 47: Ανάρτηση εγγράφου στην η-βιβλιοθήκη

5.6.3.5.1.2 Σενάριο λειτουργίας Β: Αναζήτηση εγγράφου

Το σενάριο αυτό περιλαμβάνει τις ακόλουθες λειτουργίες, όπως περιγράφονται από το αντίστοιχο διάγραμμα UML (Εικόνα 48):

1) Είσοδος στο υποσύστημα ηλεκτρονικής βιβλιοθήκης.

2) Αναζήτηση εγγράφου με βάση κριτηρίων (είτε με χρήση της ταξονομίας, είτε με λέξη κλειδί, είτε με βάση την ημερομηνία ανάρτησης του εγγράφου).
3) Αποθήκευση εγγράφου.
4) Έξοδος.



Εικόνα 48: Αναζήτηση εγγράφου στην η-βιβλιοθήκη

5.7 Συμπεράσματα - Ανοιχτά θέματα

Η διαχείριση της ασφάλειας και της επικινδυνότητας τόσο σε οργανισμούς που φιλοξενούν κρίσιμες υποδομές και διαθέτουν μια πολύπλοκη και πολυδιάστατη ως προς την υποκείμενη τεχνολογική υποδομή φύση, όπως είναι οι εμπορικοί λιμένες, όσο και σε μικρότερης πολυπλοκότητας οργανισμούς, όπως οι ΜΜΕ, αποτελεί μια διαδικασία εξαιρετικά επίπονη και χρονοβόρα [7]. Το γεγονός αυτό οφείλεται κατά κύριο λόγο σε δύο βασικούς παράγοντες. Ο πρώτος αφορά στην δυσκολία συλλογής και αξιολόγησης της γνώσης η οποία βρίσκεται διανεμημένη στο πλαίσιο πολύπλοκων και κατανεμημένων οργανισμών. Η δυσκολία αυτή οφείλεται κυρίως στην απουσία διαδικασιών και μέσων που ευνοούν την επικοινωνία μεταξύ των εμπλεκόμενων οντοτήτων. Ο δεύτερος παράγοντας σχετίζεται με την δυσκολία κατανόησης της τεχνολογικής υποδομής του οργανισμού και τον ευέλικτο εντοπισμό των σημαντικότερων συστατικών της. Το στοιχείο αυτό, βέβαια, προϋποθέτει την υιοθέτηση ουσιαστικών μηχανισμών που να προάγουν την κριτική σκέψη και να διευρύνουν την αντίληψη επιτρέποντας τη δημιουργία μιας πιο ολοκληρωμένης άποψης όσον αφορά στην υποδομή του οργανισμού.

Το περιβάλλον STORM κατανοώντας πλήρως τις συγκεκριμένες προκλήσεις κινείται προς την διευθέτησή τους υιοθετώντας βέλτιστες πρακτικές και πλαίσια. Με την χρήση συνεργατικών τεχνολογιών καθώς και άλλων σύγχρονων αυτοματοποιημένων, ανοιχτών, διαδραστικών και αξιόπιστων τεχνολογικών εργαλείων, παρέχει ένα σύνολο υπηρεσιών οι οποίες στόχο έχουν την δημιουργία μιας κουλτούρας ασφάλειας στον οργανισμό και την ολιστική διαχείριση της ασφάλειας των ΠΣ τους. Η συνεισφορά του συνεργατικού περιβάλλοντος STORM είναι σημαντική τόσο στη εφαρμογή του σε μεγάλης κλίμακας οργανισμούς όσο και σε οργανισμούς όπου τα ΠΣ είναι μικρής πολυπλοκότητας. Συγκεκριμένα, η καινοτομία του περιβάλλοντος STORM να υιοθετεί τεχνολογίες Web 2.0 για την διαχείριση της ασφάλειας, επιτρέπει τη συνεργατικότητα όλων των εμπλεκόμενων χρηστών του υπό εξέταση οργανισμού και τη συλλογή της γνώσης, με σκοπό την αντικειμενικότερη ανάλυση και διαχείριση της επικινδυνότητας των σημερινών ΠΣ εξοικονομώντας ανθρώπινους πόρους, χρόνο και κόστος για τη διοίκηση των οργανισμών. Από την άλλη, στα ΠΣ μικρών, μεσαίων και μικρομεσαίων επιχειρήσεων όπου η τεχνογνωσία των χρηστών πάνω σε θέματα ασφάλειας είναι ελάχιστη, η χρήση συνεργατικών περιβαλλόντων διαχείρισης ασφάλειας όπως το περιβάλλον STORM, αποτελεί επιτακτική ανάγκη ώστε να αναπτυχθεί μια κουλτούρα ασφάλειας στους χρήστες τέτοιων οργανισμών και να διασφαλιστούν οργανωμένες ομάδες ανταλλαγής ιδεών και επίλυσης προβλημάτων ασφάλειας μέσω των υπηρεσιών του STORM.

Ως μελλοντική επέκταση του συνεργατικού περιβάλλοντος και των υπηρεσιών του μπορεί να αποτελέσει η ενσωμάτωση και άλλων γνωστών μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας (εκτός της προτεινόμενης μεθοδολογίας STORM-RM) ώστε να είναι σε θέση οι αρμόδιοι χρήστες των οργανισμών να επιλέγουν την μεθοδολογία, να συγκρίνουν τα αποτελέσματα των μεθόδων και να υλοποιούν τελικά τις διαδικασίες οι οποίες ανταποκρίνονται περισσότερο στις δικές τους ανάγκες και απαιτήσεις.

5.8 Βιβλιογραφία 5ου Κεφαλαίου

[1] Apache Software Foundation. Available at: http://www.apache.org/ (Accessed August 2012).

[2] Business Process Modeling Notation. Available at: http://www.bpmn.org/ (Accessed August 2012).

[3] Information Technology - Open Distributed Processing - Reference Model - Enterprise Language, Proposed new version, ISO/IEC JTC1/SC7/WG17 W17N0222, ITU-T X.911 ISO/IEC 15414, March 2006.

[4] ISO / IEC 27001:2005 "Information technology - Security techniques - Information Security Management System – Requirements", 2005.

[5] ISO/IEC 9126-1:2001 "Software engineering - Product quality - Part 1: Quality model", 2001.

[6] Mule version 3. Available at: http://www.mulesoft.org/ (Accessed March 2012).

[7] Ntouskas, T., Pentafronimos G., Papastergiou, S., "STORM - Collaborative Security Management Environment", C.A. Ardagna and J. Zhou (Eds.): WISTP 2011, LNCS 6633, pp. 320–335, 2011.

[8] Open Source Web Chat. Available at: http://sourceforge.net/projects/ajax-chat/ (Accessed March 2012).

[9] RM-ODP Reference Model, Sytmemic Modelling Laboratory, LAMS, Ecole Polytechnique Federale de Lausanne, http://lams.epfl.ch/reference/rm-odp (Accessed August 2012).

[10] SOAP. Available at: http://www.w3.org/TR/soap(Accessed August 2012).

[11] Symfony Framework. Available at: http://www.symfony-project.org (Accessed August 2012).

[12] Vallecillo A. "RM-ODP: The ISO Reference Model for Open Distributed Processing". DINTEL Edition on Software Engineering. No. 3. ISBN: 84-931933-2-1, pp. 69-99. March 2001.

Κεφάλαιο 6ο

6 Μελέτες περίπτωσης

6.1 Εισαγωγή

Στο κεφάλαιο αυτό θα παρουσιαστούν δύο διαφορετικές μελέτες περίπτωσης χρήσης και εφαρμογής της προτεινόμενης μεθοδολογίας ανάλυσης και διαχείρισης επικινδυνότητας STORM-RM και του συνεργατικού περιβάλλοντος STORM. Συγκεκριμένα, θα παρουσιαστούν οι μελέτες περίπτωσης στα ΠΣ εμπορικών λιμένων (ΠΣΕΛ) και στα ΠΣ μικρών και μικρομεσαίων επιχειρήσεων (ΜΜΕ). Θα αποτυπωθεί η υφιστάμενη κατάσταση στην διαχείριση ασφάλειας τέτοιων ΠΣ, θα αναδειχθούν οι ελλείψεις τους και θα παρουσιαστούν οι προτεινόμενες λύσεις καθώς και τα αναμενόμενα αποτελέσματα από την εφαρμογή τους.

6.2 Συνεργατική ΔΑ των ΠΣ εμπορικών λιμένων

6.2.1 ΠΣ εμπορικών λιμένων

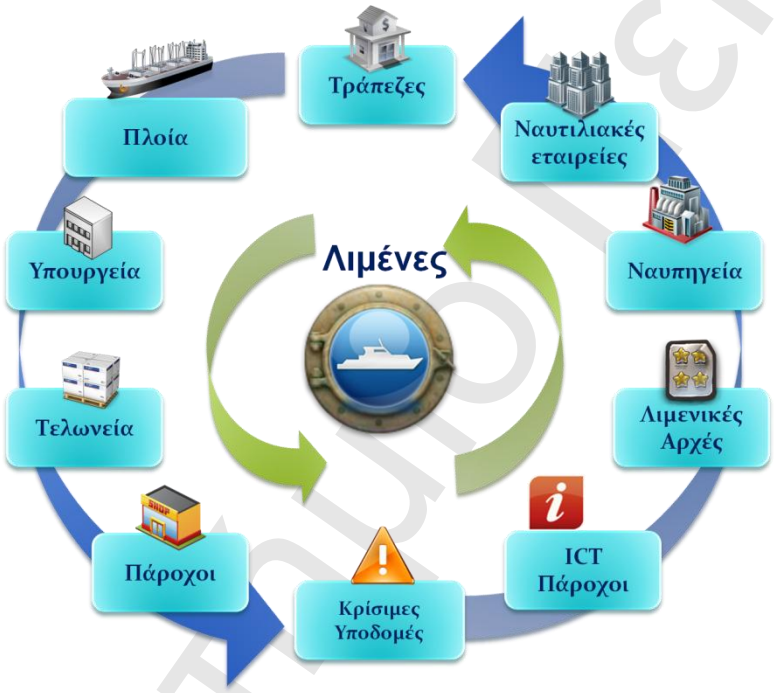
Οι εμπορικοί λιμένες είναι κρίσιμες υποδομές πληροφορικής (Critical Infrastructure, CI), καθώς φιλοξενούν κρίσιμα ΠΣ όπου τυχόν διακοπή ή δυσλειτουργία τους έχουν σημαντικές επιπτώσεις στην οικονομία, το εμπόριο και την εθνική ασφάλεια [1][53].

Η ομαλή λειτουργία των εμπορικών λιμένων εξαρτάται σε μεγάλο βαθμό από την ορθή λειτουργία των ΠΣ τους. Ο μεγάλος αριθμός των κρίσιμων και ευαίσθητων δεδομένων, των πληροφοριών και των υπηρεσιών που διαχειρίζονται σε καθημερινή βάση, ο μεγάλος αριθμός των χρηστών που καλούνται να εξυπηρετήσουν και οι αλληλεξαρτήσεις τους με άλλες υποδομές απαιτούν αποτελεσματική διαχείριση της ασφάλειας. Οι υποδομές αυτές είναι εκτεθειμένες σε ένα μεγάλο αριθμό καθημερινών απειλών, με κίνδυνο την υπολειτουργία ή ακόμη και την διακοπή των ηλεκτρονικών υπηρεσιών που προσφέρουν στους πολίτες αλλά και στους ίδιους τους φορείς.

Οι εμπορικοί λιμένες παρέχουν κρίσιμες ηλεκτρονικές υπηρεσίες και επιχειρηματικές διαδικασίες, και για το λόγο αυτό απαιτούνται κατάλληλες διαδικασίες και πρακτικές διαχείρισης ασφάλειας με στόχο την ομαλή λειτουργία τους και την ανάκαμψη σε περίπτωση κακόβουλου συμβάντος, μειώνοντας κατά το δυνατόν τους χρόνους ανάκαμψης και ελαχιστοποιώντας τυχόν

απώλειες. Πρέπει λοιπόν να δοθεί μεγάλη προσοχή στην ασφάλεια και την προστασία των υπαρχουσών, των αναπτυσσόμενων και της νέας γενιάς κρίσιμων ηλεκτρονικών υπηρεσιών λιμένων.

Το περιβάλλον ναυτιλίας είναι πολύπλοκο, όπως φαίνεται στην Εικόνα 49, εμπλέκοντας και αλληλεπιδρώντας με διάφορες οντότητες όπως λιμένες, πλοία (μαζί με τους επιβάτες, πλήρωμα και εμπόρευμα) λιμενικές αρχές, τηλεπικοινωνιακούς παρόχους, ναυτιλιακές εταιρείες, τελωνεία, τράπεζες, υπουργεία, και άλλες κρίσιμες υποδομές (π.χ. σιδηροδρόμους, αεροδρόμια) με πολύπλοκα ΠΣ.



Εικόνα 49: Περιβάλλον ναυτιλίας

Κεντρικό ρόλο στο περιβάλλον ναυτιλίας παίζουν τα εμπορικά λιμάνια, δεδομένου ότι είναι η μόνη οντότητα που αλληλεπιδρά άμεσα με όλους τους συμμετέχοντες στο περιβάλλον αυτό, προσφέροντας τις υπηρεσίες (λιμενικές υπηρεσίες), με διαφορετικό βαθμό κρισιμότητας [21][53].

Υπάρχουν διάφορες η-υπηρεσίες οι οποίες παρέχονται από τα ΠΣ των εμπορικών λιμένων. Οι υπηρεσίες αυτές μπορεί να κατηγοριοποιηθούν ανάλογα με τις λειτουργίες τους σε πέντε (5) κατηγορίες:

- ✓ **Υπηρεσίες διαχείρισης πλοίων,** οι οποίες παρέχουν:
  - ηλεκτρονικές πληροφορίες στους πράκτορες για τη κατάσταση των πλοίων,
  - ηλεκτρονικές διαδικασίες διαχείρισης (e- administrative procedures),

- η-επικοινωνία με άλλα λιμάνια και λιμενικές αρχές,
- αυθεντικοποίηση και παρακολούθηση πλοίων μέσω RFIDs και γεωγραφικών Συστήματα (GIS systems), και
- υπηρεσίες πλοήγησης.

✓ **Υπηρεσίες διαχείρισης φορτίου** οι οποίες παρέχουν**:**

- η-έγγραφα στους εμπλεκόμενους πράκτορες,
- η-πληροφορίες για την κατάσταση των φορτίων,
- η-διαχείριση φορτίων, και
- αυθεντικοποίηση και παρακολούθηση των φορτίων μέσω RFIDs και γεωγραφικών Συστήματα (GIS systems)**.**

✓ **Εσωτερικές εφοδιαστικές (Logistics) υπηρεσίες** οι οποίες παρέχουν**:**

- η-διαχείριση των εσωτερικών διαδικασιών (π.χ. μεταφορά/αποδοχή/παραλαβή η-παραγγελιών),
- η-προμήθειες,
- η-τιμολόγηση,
- η-πληρωμή,
- η-ανίχνευση (e.g. η-πληροφορίες σχετικά με τις μεταφορές σε ολόκληρη την εφοδιαστική αλυσίδα), και
- η-κράτηση.

✓ **Επικοινωνία λιμένων:** επικοινωνία πολλαπλών καναλιών για την επικοινωνία των λιμένων με άλλες ναυτιλιακές οντότητες (άλλοι λιμένες, πλοία, πλήρωμα κτλ).

✓ **Υπηρεσίες διασύνδεσης** με άλλα συστήματα**:**

- διασύνδεση με τελωνεία για την διαχείριση απαραίτητων η-εγγράφων (τελωνιακές δηλώσεις, εισαγωγές / εξαγωγές) και ελέγχων (π.χ. φόροι, πρόσθημα),
- διασύνδεση με λιμεναρχεία και συστήματα μετανάστευσης για την παρακολούθηση και τον έλεγχο των φορτίων, τροφίμων, επιβατών του λιμένα,
- διασύνδεση με φορείς υγείας για την παροχή υπηρεσιών υγείας, και
- διασύνδεση με άλλες κρίσιμες υποδομές (όπως σιδηροδρομικοί σταθμοί, αεροδρόμια) για την παροχή συνεργατικών η-τουριστικών υπηρεσιών (κρατήσεις εισιτηρίων, έκδοση εισιτηρίων, πρόγραμμα δρομολογίων κτλ).

Τα ΠΣ εμπορικών λιμένων (ΠΣΕΛ) αποτελούνται (όπως όλα τα ΠΣ) από τα ακόλουθα έξι (6) επίπεδα:

1. **Υποδομές** (π.χ. κτήρια, πλατφόρμες, πύλες, προβλήτες, μαρίνες, κέντρα δεδομένων),
2. **Τηλεπικοινωνιακή υποδομή** (π.χ. δίκτυα, εξοπλισμός, δορυφορικά συστήματα, εξυπηρετητές),
3. **Συστήματα και Λογισμικά** (π.χ. δίκτυα επικοινωνιών, συστήματα μετάδοσης (transmission systems), συστήματα πλοήγησης, συστήματα διαχείρισης επιχειρησιακών πόρων (ERP), ticketing, γεωγραφικά συστήματα πληροφοριών (GIS)),
4. **Πληροφορία και ηλεκτρονικά δεδομένα** (π.χ. λιμενικά και ακτοπλοϊκά δεδομένα, εμπορικά δεδομένα),
5. **Υπηρεσίες** (π.χ. τιμολόγηση, πλοήγηση, διαχείριση εμπορευματοκιβωτίων, φορτοεκφόρτωση, διαχείριση επιβατών),
6. **Χρήστες** :
    - εσωτερικούς χρήστες (π.χ. διαχειριστές, προσωπικό),
    - εξωτερικούς χρήστες (π.χ. ναυτιλιακές εταιρείες, τελωνεία, ασφαλιστικές εταιρείες, τηλεπικοινωνιακούς παρόχους), και
    - οντότητες (π.χ. πλοία, οχήματα, αποσκευές, φορτία).

Ένα ΠΣ θεωρείται ότι είναι ασφαλές όταν όλα τα αγαθά των παραπάνω έξι επιπέδων ικανοποιούν τις απαιτήσεις ασφάλειας δηλαδή εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και έλεγχο πρόσβασης. Με τον όρο φυσική ασφάλεια (Safety) εννοούμε την ικανοποίηση των δύο απαιτήσεων ασφάλειας της *διαθεσιμότητας* και του *ελέγχου πρόσβασης* των αγαθών του 1^{ου} και 6^{ου} επιπέδου. Ως συνέπεια, η φυσική ασφάλεια (Safety) είναι υποσύνολο της ασφάλειας ΠΣ (Information Security), όπως φαίνεται και στην Εικόνα 50.

Εικόνα 50: Ασφάλεια (security) και Φυσική ασφάλεια (safety)

Στην βιβλιογραφία της ναυτιλίας, υπάρχει μια σύγχυση των δύο αυτών εννοιών οι οποίες τις περισσότερες φορές συμπίπτουν [53]. Ειδικότερα, διάφορες υφιστάμενες προσπάθειες (όπως θα δούμε στην ενότητα 6.1.2 που ακολουθεί) υποστηρίζοντας ότι αντιμετωπίζουν την ασφάλεια ΠΣ, στην πραγματικότητα αντιμετωπίζουν μόνο την φυσική ασφάλεια.

6.2.2 Υφιστάμενη κατάσταση στη διαχείριση ασφάλειας ΠΣ εμπορικών λιμένων

Ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) [26], έχει εκδώσει μια σειρά οδηγιών που εμπίπτουν σε δύο κατηγορίες: SOLAS and MARPOL. Οι οδηγίες SOLAS είναι για την φυσική ασφάλεια (safety) των πλοίων, επιβατών και φορτίων και οι οδηγίες MARPOL είναι για την περιβαντολλογική προστασία των θαλασσών.

Ο κώδικας International Ships and Port Facilities Security Code (ISPS), ο οποίος αποτελεί οδηγία του IMO (2004), είναι ο πιο κατάλληλος για θέματα ασφάλειας αλλά, όμως, καλύπτει μόνο τις περιοχές: ασφαλή πρόσβαση, έλεγχος, ασφαλή διακίνηση φορτίου, διαθεσιμότητα τηλεπικοινωνιακής υποδομής, αναφορά περιστατικών, δημιουργία ομάδα ασφάλειας, ανάλυση επικινδυνότητας και εκπαίδευση σε θέματα ασφάλειας. Δεν αναφέρεται καθόλου σε μέτρα προστασίας ΠΣ και κυβερνοαπειλές (cyber threats).

Ο Ευρωπαϊκός Οργανισμός Ναυτιλιακής Ασφάλειας (European Maritime Safety Agency (EMSA) [20]) είναι ένας φορέας παροχής υπηρεσιών στους τομείς της ασφάλειας στη θάλασσα, τη φυσική ασφάλεια, την πρόληψη της ρύπανσης και την αντιμετώπιση σχετικών πληροφοριών προς την Ευρωπαϊκή Επιτροπή, τα κράτη μέλη και άλλους σχετικούς φορείς της Ευρωπαϊκής Ένωσης. Το σύστημα SafeSeaNet [59], το οποίο φιλοξενείται από τον EMSA, συλλέγει πληροφορίες σχετικά με την ναυτιλία από τις αρμόδιες εθνικές αρχές, αφήνοντας την διαχείριση της ασφάλειας στο εθνικό επίπεδο.

Άλλοι συναφείς οργανισμοί (όπως οι European Aviation Safety Agency [19], Trans-European Transport Network Executive Agency (TEN-T EA) [63]) δεν περιλαμβάνουν οδηγίες και πρακτικές για την ασφάλεια ΠΣ και τις κυβερνοαπειλές.

Οι στοχευμένες μεθοδολογίες ανάλυσης επικινδυνότητας ΠΣ λιμένων όπως η Maritime Security Risk Analysis Model (MSRAM) [17] καθώς και η επέκτασή της MSRAM-PLUS/FORETELL [2] είναι συμβατές με τις οδηγίες του ISPS και αντιμετωπίζουν μόνο την φυσική ασφάλεια. Αντίστοιχα και η MARISA [7] επικεντρώνεται στην ασφαλή πλοήγηση των πλοίων κατά τη διάρκεια της παραμονής τους στο λιμάνι, ενώ και το σύστημα CMA [37] επικεντρώνεται στην μη φυσιολογική συμπεριφορά των πλοίων και τον εντοπισμό πιθανών απειλών.

Ταυτόχρονα, οι υπάρχουσες εθνικές προσεγγίσεις για την διαχείριση επικινδυνότητας σε περιβάλλοντα λιμένων (όπως της Εσθονίας [23], της Ιορδανίας [36] και της Ρωσίας [43][62]), επικεντρώνονται στην φυσική ασφάλεια των λιμένων.

Την τελευταία δεκαετία έχει ξεκινήσει ενας μεγάλος αριθμός από Ερευνητικά Προγράμματα Ασφάλειας τα οποία σχετίζονται με την αντιμετώπιση ζητημάτων ασφάλειας των λιμένων και των ΠΣΕΛ**.** Τα προγράμματα αυτά χωρίζονται σε τρεις (3) κύριες κατηγορίες [53]:

- ✓ αναβαθμισμένα συστήματα θαλάσσιας επιτήρησης (σε αυτή την κατηγορία βρίσκονται τα προγράμματα όπως: AMASS, UNCOSS, SOBCAH, SEABILLA),
- ✓ διαλειτουργικότητα των ΠΣΕΛ (σε αυτή την κατηγορία βρίσκονται τα προγράμματα : AMASS, UNCOSS, SOBCAH, SEABILLA, OPERAMAR, SECCONDD),
- ✓ προστασία κρίσιμων υποδομών λιμένων (σε αυτή την κατηγορία βρίσκονται τα προγράμματα SECTRONIC, SUPPORT).

Όλες οι παραπάνω οδηγίες, μεθοδολογίες και ερευνητικά προγράμματα ασφάλειας στο περιβάλλον της ναυτιλίας επικεντρώνονται κυρίως στην φυσική ασφάλεια και ελάχιστα στην ασφάλεια των ΠΣ, καλύπτουν δηλαδή μόνο τα δύο επίπεδα του ΠΣΕΛ - τις υποδομές και τους χρήστες - αφήνοντας τα υπόλοιπα επίπεδα απροστάτευτα. Αντιμετωπίζουν μόνο τις φυσικές απειλές και υπολογίζουν τον αντίστοιχο φυσικό κίνδυνο, μην λαμβάνοντας υπόψη απειλές οι οποίες προκύπτουν από τις εξαρτήσεις των λιμένων από τα πληροφοριακά τους συστήματα και τις αλληλεξαρτήσεις αυτών από άλλες οντότητες του περιβάλλοντος ναυτιλίας οι οποίες μπορεί να προκαλέσουν πολλαπλές επιπτώσεις. Δεν αντιμετωπίζουν την ασφάλεια ΠΣ ξεχωριστά παρά μόνο σε σχέση με την φυσική ασφάλεια των πλοίων.

Η υλοποίηση του κώδικα ISPS έχει μείνει στο εθνικό επίπεδο χωρίς να υπάρχουν πρότυπα (όπως υπάρχει το ISO27002 [28] για την ασφάλεια ΠΣ) που να παρέχουν ακριβείς διαδικασίες και μέτρα που πρέπει να υλοποιηθούν ώστε ένα λιμάνι να είναι συμβατό με τον κώδικα.

Ταυτόχρονα, όλες οι υπάρχουσες μεθοδολογίες διαχείρισης ασφάλειας λιμένων δεν είναι ανθρωποκεντρικές, δεν υποστηρίζουν την συνεργατικότητα και εμπλέκουν τον χρήστη ως παθητική οντότητα χωρίς να απαιτείται η ενεργή συμμετοχή του στα βήματά τους.

Η ισχύουσα νομοθεσία στη ναυτιλία και οι προσπάθειες προτυποποίησης δεν καλύπτουν επαρκώς την ασφάλεια των ΠΣΕΛ. Ειδικότερα, τα εμπορικά λιμάνια δεν αντιμετωπίζονται ως ανεξάρτητες κρίσιμες υποδομές οι οποίες φιλοξενούν κρίσιμα ΠΣ τα οποία αλληλεπιδρούν με πολλούς φορείς και δεν γίνεται μια ολιστική διαχείριση της ασφάλειάς τους. Το γεγονός ότι οι λιμένες είναι ζωτικής σημασίας υποδομές εγείρει συγκεκριμένες απειλές (π.χ. απεργίες,

τρομοκρατικές επιθέσεις, καιρικές συνθήκες), και ο μη προσδιορισμός τέτοιων απειλών και των επιπτώσεών τους στην εθνική οικονομία, την εθνική ασφάλεια και τη διατάραξη της δημόσιας τάξης μπορεί να οδηγήσει σε ανακριβείς αξιολογήσεις κινδύνων.

6.2.3 Ανοιχτά θέματα - Συνεισφορά διατριβής

Οι γνωστές μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητες, οι οποίες παρουσιάστηκαν στο 2ο Κεφάλαιο της παρούσας διδακτορικής διατριβής (π.χ. OCTAVE, CRAMM, MAGERIT, MEHARI), δεδομένου ότι είναι αρκετά γενικές, δεν είναι σε θέση να καλύψουν τις ανάγκες των σημερινών πολύπλοκων κατανεμημένων ΠΣ.

Στις μέρες μας, τα ΠΣ των λιμένων, χρησιμοποιούνται από πολλούς χρήστες και αντιμετωπίζουν έναν αυξανόμενο αριθμό, διαφορετικού τύπου χωροχρονικές επιπτώσεις από το μεγάλο πλήθος των απειλών. Οι υφιστάμενες μεθοδολογίες και τα εργαλεία πρέπει να ενισχυθούν προκειμένου να αντιμετωπίσουν αυτές τις προκλήσεις, παρέχοντας συνεργατικότητα, μειωμένο κόστος και χρόνο για την συλλογή της γνώσης από όλους τους συμμετέχοντες στο ΠΣ. Επιπλέον, θα πρέπει να εξετάζουν και να λαμβάνουν υπόψη τους τα ιδιαίτερα χαρακτηριστικά του υπό εξέταση οργανισμού και του επιχειρησιακού κλάδου στον οποίο ανήκει.

Μια προτεινόμενη λύση για την καλύτερη αντιμετώπιση της ασφάλειας ΠΣΕΛ είναι ο συνδυασμός του κώδικα ISPS με τα διαθέσιμα πρότυπα διαχείρισης ασφάλειας και τα πρότυπα προστασίας κρίσιμων υποδομών (Critical Information Infrastructure Protection, CIIP). Παρόλα αυτά, όμως, τα πρότυπα αυτά χρειάζονται περαιτέρω αναβάθμιση ώστε να είναι σε θέση να καλύψουν τις συγκεκριμένες απειλές (οι οποίες προκύπτουν από την αλληλεξάρτηση των ΠΣΕΛ με άλλες οντότητες του περιβάλλοντος ναυτιλίας) και την σχετική νομοθεσία στις οποίες υπόκεινται τα ΠΣΕΛ (π.χ. οδηγίες του κώδικα ISPS).

Μια στοχευμένη μεθοδολογία διαχείρισης ασφάλειας ΠΣΕΛ θα πρέπει να λαμβάνει υπόψη της τις παρακάτω απαιτήσεις:

- ✓ **Συμβατότητα με τα υπάρχοντα πρότυπα**: όπως το πρότυπο ISO27001, τα πρότυπα προστασίας κρίσιμων υποδομών (CIIP) και τον κώδικα ISPS,
- ✓ **Συνεργατικότητα**: να υποστηρίζει την συνεργατικότητα μεταξύ όλων των χρηστών των ΠΣΕΛ,
- ✓ **Ευρεία ανάλυση**: να αναλύει απειλές που προκύπτουν από την αλληλεξάρτηση των ΠΣΕΛ με άλλους φορείς και να αξιολογεί τους έμμεσους και τους άμεσους κινδύνους,
- ✓ **Εξοικονόμηση χρόνου και κόστους**: να μπορεί να αποφευχθεί η πληθώρα των ερωτηματολογίων και των χρονοβόρων συνεντεύξεων με όλους τους συμμετέχοντες οι οποίες απαιτούνται για την καταγραφή της αρχιτεκτονικής του υπό εξέταση ΠΣΕΛ, τις

αλληλεξαρτήσεις των αγαθών και την σημαντικότητα των αγαθών, των απειλών και των αδυναμιών που αντιμετωπίζουν,

- ✓ **Εύκολα υλοποιήσιμη**: να είναι σε θέση να υλοποιηθεί ως εύχρηστη ηλεκτρονική υπηρεσία σε ένα συνεργατικό περιβάλλον για την διαχείριση ασφάλειας.

Επιπλέον, κάθε στοχευμένη μεθοδολογία θα πρέπει να μπορεί να υλοποιηθεί ως εργαλείο ή να ενσωματωθεί σε ένα συνεργατικό περιβάλλον το οποίο θα χρησιμοποιείται από την ομάδα ασφάλειας με στόχο την εύκολη διαχείριση ασφάλειας των ΠΣΕΛ. Ένα τέτοιο συνεργατικό περιβάλλον θα πρέπει να ακολουθεί κάποιες γενικές προδιαγραφές:

- ✓ **Υποστήριξη κατηγοριοποίησης και κωδικοποίησης περιεχομένου**: οι συμμετέχοντες θα πρέπει να είναι σε θέση να βρίσκουν την χρήσιμη πληροφορία σχετικά με την διαχείριση επικινδυνότητας εύκολα και γρήγορα. Για το λόγο αυτό, θα πρέπει να υποστηρίζεται από το εργαλείο μηχανισμός κωδικοποίησης του περιεχομένου ώστε οι χρήστες να βρίσκουν εύκολα χρήσιμα έγγραφα όπως βέλτιστες πρακτικές, υπάρχουσα νομοθεσία κτλ.
- ✓ **Υποστήριξη εξατομίκευσης της πληροφορίας**: επειδή η διαχείριση ασφάλειας είναι μια συνεχώς εξελισσόμενη διαδικασία λήψης αποφάσεων θα πρέπει να υποστηρίζεται η τήρηση ιστορικού με τις απόψεις και τις αποτιμήσεις των εμπλεκόμενων χρηστών καθώς και των διαφορετικών εκδόσεων των αναλύσεων διαχείρισης ασφάλειας. Με την προοπτική αυτή είναι εύκολο να εξατομικεύεται η πληροφορία και να γίνονται συζητήσεις και ανταλλαγές απόψεων για την πολιτική η οποία θα ακολουθηθεί λαμβάνοντας υπόψη όλες τις διαφορετικές απόψεις των χρηστών οι οποίες θα προκύπτουν από την προσωπική τους εμπειρία και τεχνογνωσία.
- ✓ **Συνεργατικότητα**: λόγω του ότι η διαχείριση ασφάλειας είναι ένα πρόβλημα συνεργατικής λήψης αποφάσεων, ένα εργαλείο διαχείρισης ασφάλειας θα πρέπει να επιτρέπει την συνεργασία μεταξύ των εμπλεκόμενων. Με τον τρόπο αυτό θα γίνεται εφικτή η ενεργή συμμετοχή όλων των απαραίτητων χρηστών και θα λαμβάνεται υπόψη η γνώση και η εμπειρία τους πάνω σε θέματα των αρμοδιοτήτων τους.
- ✓ **Διαφορετική απεικόνιση περιεχομένου ανάλογα με το ρόλο των χρηστών**: δεδομένου ότι η διαχείριση ασφάλειας περιλαμβάνει τρεις λειτουργίες (πρακτική, κριτική και αναθεώρηση), στην οποία συμμετέχουν συνήθως συμμετέχοντες με διαφορετικό ρόλο, το εργαλείο θα πρέπει να υποστηρίζει διαφορετικές όψεις δημιουργίας και απεικόνισης της διαθέσιμης πληροφορίας.
- ✓ **Περιγραφική προσέγγιση**: δεδομένου ότι η διαδικασία της διαχείρισης ασφάλειας είναι εξαιρετικά δημιουργική, δεν πρέπει το εργαλείο να είναι περιοριστικό. Μια πιο περιγραφική

προσέγγιση προς την κατεύθυνση της διαχείρισης γνώσης θα διευκολύνει με τον καλύτερο τρόπο τη δημιουργικότητα των συμμετεχόντων.

- ✓ **Βασισμένο σε υπηρεσίες**: όλα τα βήματα της μεθοδολογίας διαχείρισης ασφάλειας θα πρέπει να παρέχονται ως ξεχωριστές συνεργατικές υπηρεσίες.

Οι παραπάνω απαιτήσεις λαμβάνονται υπόψη στο παρόν κεφάλαιο όπου και παρουσιάζονται οι προτεινόμενες λύσεις.

6.2.4 S-PORT: συνεργατικό περιβάλλον ΔΑ των ΠΣ εμπορικών λιμένων

Δεδομένης της πολυπλοκότητας των πληροφοριακών συστημάτων των κρίσιμων υποδομών των λιμένων, της αδιάλειπτης λειτουργίας τους, των κρίσιμων και ευαίσθητων δεδομένων που διαχειρίζονται καθώς και το πλήθος των χρηστών που καλούνται να εξυπηρετούν, καθίσταται απαραίτητη η ύπαρξη αυτοματοποιημένων συνεργατικών μεθοδολογιών και εργαλείων διαχείρισης ασφάλειας των ΠΣΕΛ.

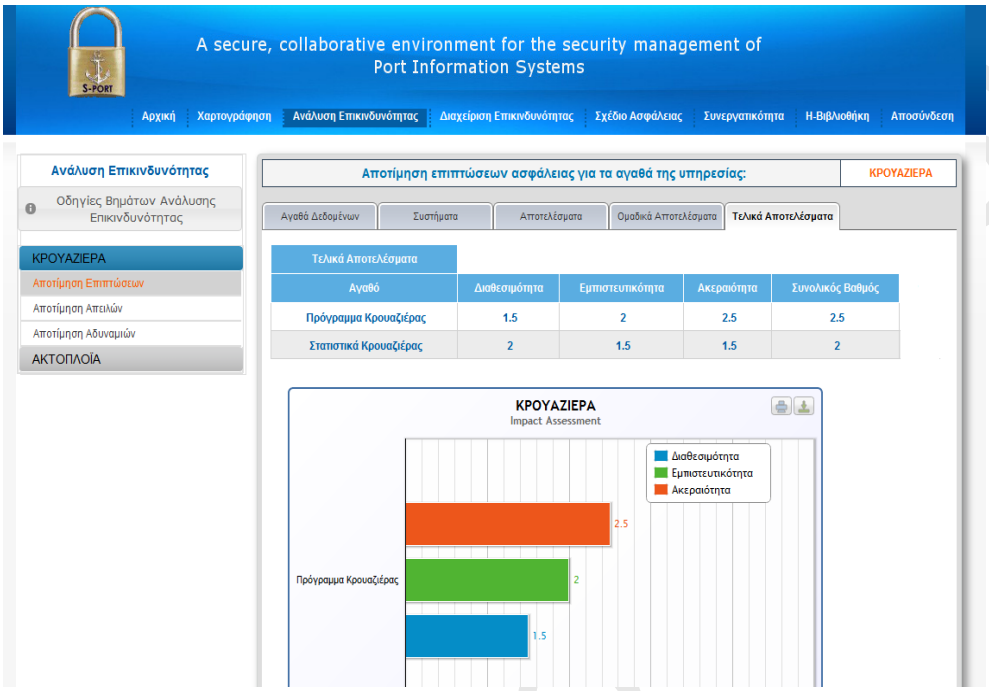
Προς αυτή την κατεύθυνση έρχεται να απαντήσει η ύπαρξη της μεθοδολογίας STORM-RM και του συνεργατικού περιβάλλοντος STORM. Συγκεκριμένα, κάνοντας χρήση των υπηρεσιών του συνεργατικού περιβάλλοντος οι χρήστες των εμπορικών λιμένων θα είναι σε θέση να:

- ✓ προσδιορίζουν, αξιολογούν και κατηγοριοποιούν τις περιοχές επικινδυνότητας του οργανισμού μέσω της υπηρεσίας Χαρτογράφησης,
- ✓ αναγνωρίζουν τις επιπτώσεις που θα έχει ένα σοβαρό περιστατικό στην λειτουργία των οργανισμών μέσω της υπηρεσίας Αποτίμησης Επιπτώσεων,
- ✓ αξιολογούν τις ενδεχόμενες απειλές και τις αντίστοιχες αδυναμίες των αγαθών του ΠΣ, μέσω των υπηρεσιών Αποτίμησης Απειλών και Αδυναμιών αντίστοιχα,
- ✓ επιλέγουν κατάλληλα και αξιόπιστα αντίμετρα ώστε να επιτυγχάνεται η διαθεσιμότητα και ακεραιότητα των δεδομένων μέσω της υπηρεσίας Διαχείρισης Επικινδυνότητας,
- ✓ καθορίζουν μία επίσημη διαδικασία που θα ακολουθηθεί σε περίπτωση καταστροφής μέσω της υπηρεσίας Διαχείρισης Εγγράφων Ασφαλείας,
- ✓ αναπτύσσουν αποτελεσματική στρατηγική τήρησης αντιγράφων ασφαλείας και ανάκτησης δεδομένων ώστε να ελαχιστοποιηθεί η επίπτωση τυχών καταστροφών μέσω της υπηρεσίας Διαχείρισης Εγγράφων Ασφαλείας,
- ✓ έχουν την δυνατότητα συνεχούς ενημέρωσης των σχεδίων Επιχειρησιακής Συνέχειας / Αποκατάστασης Καταστροφών και της Πολιτικής Ασφάλειας του οργανισμού τους μέσω της υπηρεσίας Διαχείρισης Εγγράφων Ασφαλείας, και να

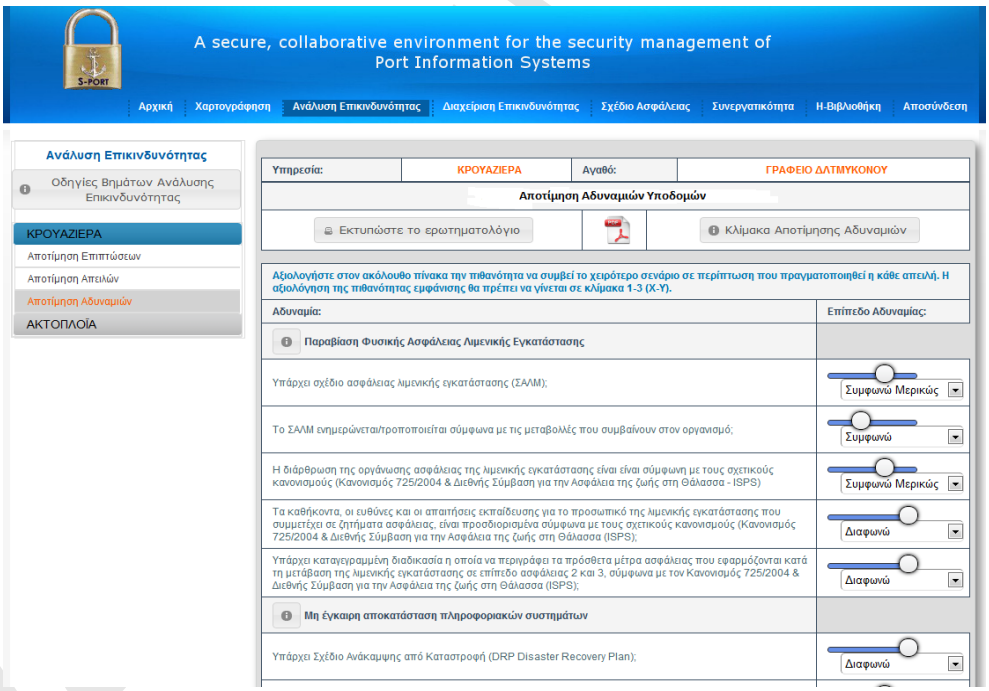
- ✓ ενημερώνονται για τους νέους νόμους και τα πρότυπα που θα πρέπει να ακολουθεί η Πολιτική Ασφάλειας του οργανισμού τους μέσω της υπηρεσίας η-βιβλιοθήκης.

Τέλος αξίζει να σημειωθεί ότι το συνεργατικό περιβάλλον STORM, λόγω του γεγονότος ότι επιτρέπει την επέκταση, παραμετροποιήθηκε προκειμένου να αντιμετωπίσει τις ανάγκες των ΠΣΕΛ [44][47][52]. Στις εικόνες 51-57 φαίνονται κάποιες βασικές οθόνες του προτεινόμενου εργαλείου διαχείρισης ασφάλειας ΠΣΕΛ (S-PORT).

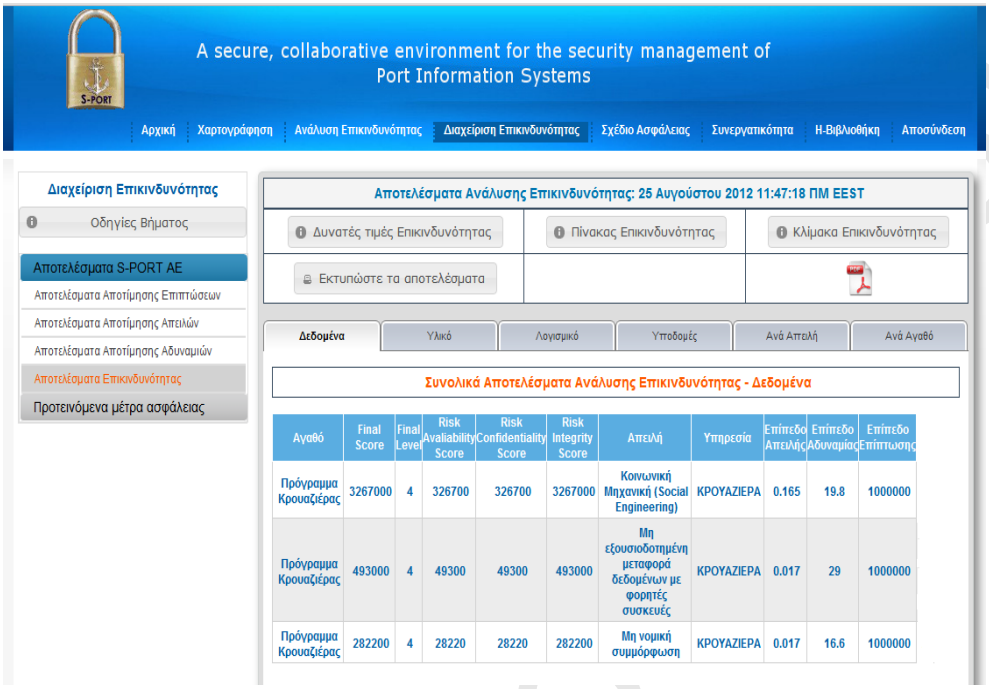
Εικόνα 51: Ηλεκτρονικό ερωτηματολόγιο αποτίμησης επιπτώσεων



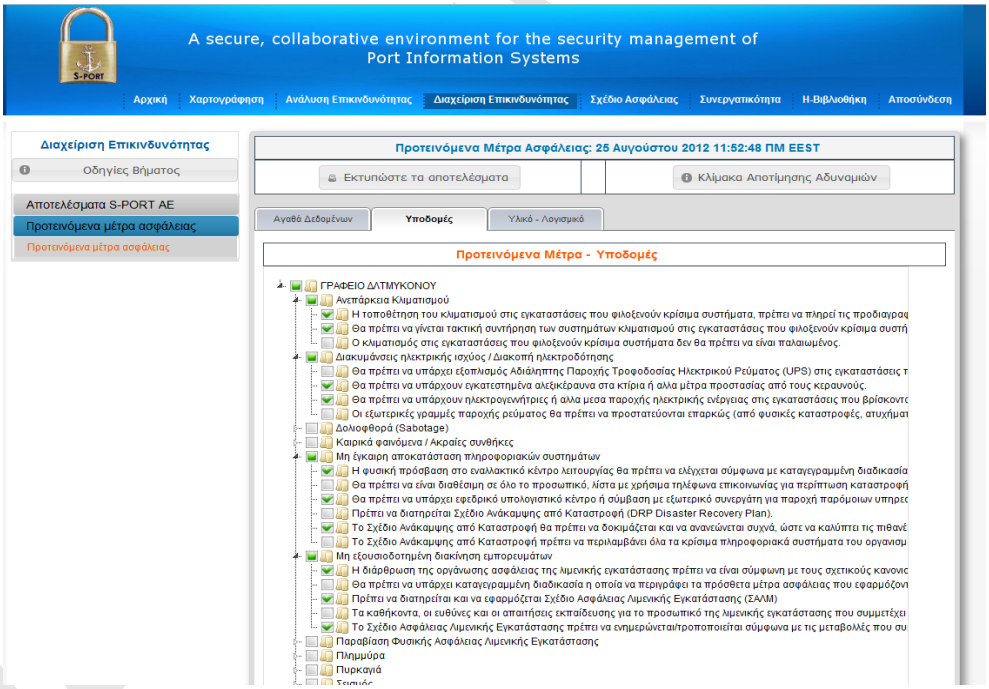
Εικόνα 52: Απεικόνιση αποτελεσμάτων αποτίμησης επιπτώσεων



Εικόνα 53: Ηλεκτρονικό ερωτηματολόγιο αποτίμησης αδυναμιών

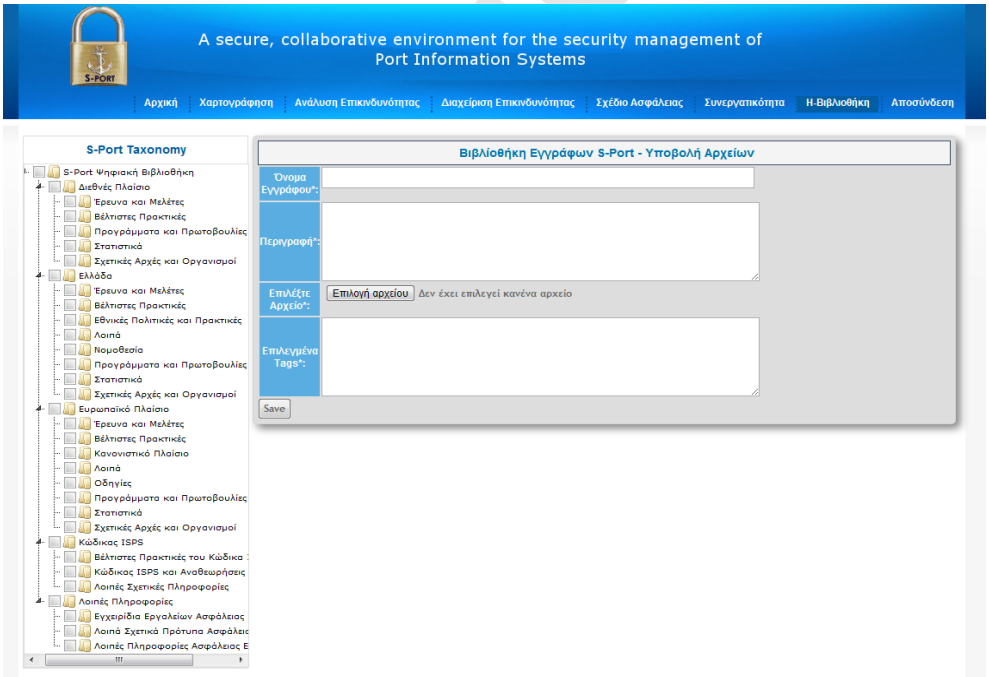


Εικόνα 54: Απεικόνιση αποτελεσμάτων ανάλυσης επικινδυνότητας



Εικόνα 55: Επιλογή μέτρων ασφάλειας προς υλοποίηση

Εικόνα 56: Ηλεκτρονική φόρμα δημιουργίας της πολιτικής ασφάλειας του ΠΣ λιμένα



Εικόνα 57: Ηλεκτρονική βιβλιοθήκη του S-PORT

Συγκεκριμένα, έχει ενημερωθεί με λίστα στοχευμένων απειλών και αδυναμιών που αντιμετωπίζουν τα ΠΣΕΛ (όπως απεργίες, καιρικά φαινόμενα κλπ), εμπλουτίστηκε η ηλεκτρονική βιβλιοθήκη με τα απαραίτητα έγγραφα ναυτιλιακού περιεχομένου (όπως διατάξεις του ISPS, νόμους σχετικά με την

ναυτιλία κλπ) και τέλος η υπηρεσία Διαχείρισης Εγγράφων ασφαλείας έχει παραμετροποιηθεί ώστε να καλύπτει και να συνδυάζει τις απαιτήσεις του ISO27001 και του ISPS.

6.2.5 Συμπεράσματα – Ανοιχτά θέματα

Τα λιμάνια είναι μείζονες φορείς παροχής υπηρεσιών όμως δεν υιοθετούν «Καλές πρακτικές ασφάλειας ΠΣ» [53], δηλαδή δεν αντιμετωπίζουν αποτελεσματικά την ασφάλεια των ΠΣ (π.χ. επιθέσεις, παρακολούθηση της κυκλοφορίας του δικτύου) ή απειλές της ιδιωτικής ζωής (π.χ. κλοπή / τροποποίηση των προσωπικών δεδομένα), δεν εφαρμόζουν τα κατάλληλα μέτρα ασφαλείας για τις τεχνολογίες που χρησιμοποιούν (π.χ. RFID) προκαλώντας τεράστιες ζημιές και θέτοντας σε κίνδυνο (π.χ. απώλεια φήμης, απώλεια της νομικής συμμόρφωσης, διακοπή της λειτουργίας των επιχειρήσεων), όχι μόνο τους ίδιους αλλά και το σύνολο των οντοτήτων του ναυτιλιακού περιβάλλοντος. Η αντιμετώπιση της ασφάλειας των ΠΣΕΛ γίνεται ένα σημαντικό πρόβλημα, καθώς αυτό μπορεί να έχει επιχειρηματικές επιπτώσεις και στις άλλες οντότητες του ναυτιλιακού περιβάλλοντος και μπορούν να χαρακτηριστούν ως αδύνατοι κρίκοι στην ασφάλεια των πληροφοριών.

Η ισχύουσα νομοθεσία στη ναυτιλία και οι προσπάθειες προτυποποίησης δεν καλύπτουν επαρκώς την ασφάλεια των ΠΣ των εμπορικών λιμένων. Ειδικότερα, τα εμπορικά λιμάνια δεν αντιμετωπίζονται ως ανεξάρτητες κρίσιμες υποδομές οι οποίες φιλοξενούν κρίσιμα ΠΣ τα οποία αλληλεπιδρούν με πολλούς φορείς και η ασφάλεια τους δεν αξιολογείται ή δεν διαχειρίζεται με ολιστικό και αποτελεσματικό τρόπο. Το γεγονός ότι οι λιμένες είναι ζωτικής σημασίας υποδομές αναδεικνύει συγκεκριμένες απειλές (π.χ. απεργίες, τρομοκρατικές επιθέσεις, καιρικές συνθήκες) για τις οποίες δεν λαμβάνονται υπόψη οι επιπτώσεις τους (π.χ. στην εθνική οικονομία, την εθνική ασφάλεια, διατάραξη της δημόσιας τάξης) με αποτέλεσμα να οδηγούμαστε σε ανακριβείς αξιολογήσεις κινδύνων. Οι θαλάσσιες προσπάθειες προτυποποίησης επικεντρώνονται μόνο στη φυσική ασφάλεια των λιμένων, αφήνοντας απροστάτευτα τα ΠΣ από απειλές του κυβερνοχώρου και, κατά συνέπεια, οι η-υπηρεσίες και τα δεδομένα των λιμένων είναι σε κίνδυνο.

Επιπλέον, οι υπάρχουσες μεθοδολογίες ΑΔΕ απαιτούν πληθώρα συνεντεύξεων με όλους τους συμμετέχοντες προκειμένου να προσδιοριστεί η αρχιτεκτονική των ΠΣΕΛ, η κρισιμότητα των αγαθών των ΠΣΕΛ, οι αλληλεξαρτήσεις τους και οι αντίστοιχες απειλές τους. Χρειάζονται χρόνο, πόρους και κόστος με αποτέλεσμα οι συγκεκριμένες μεθοδολογίες να μην μπορούν να ανταποκριθούν στις ανάγκες των ΠΣΕΛ.

Λαμβάνοντας υπόψη την υπάρχουσα κατάσταση και τις ανάγκες για ολιστική διαχείριση της ασφάλειας ΠΣΕΛ, η παρούσα διδακτορική διατριβή πρότεινε τη νέα συνεργατική μεθοδολογία

STORM-RM και το συνεργατικό περιβάλλον διαχείρισης ασφάλειας STORM με στόχο να βοηθήσει τους χρήστες των ΠΣΕΛ να αντιμετωπίσουν την ασφάλεια με αποτελεσματικό τρόπο, διασφαλίζοντας την αδιάλειπτη παροχή η-υπηρεσιών λιμένων.

6.3 Μελέτη περίπτωσης στα ΠΣ μικρών, μεσαίων και πολύ μικρών επιχειρήσεων (ΜΜΕ)

6.3.1 ΜΜΕ

Οι μικρές, μεσαίες και πολύ μικρές επιχειρήσεις (ΜΜΕ) παίζουν καθοριστικό ρόλο στην ευρωπαϊκή οικονομία. Παρά την αυξανόμενη ζήτηση για τις υπηρεσίες τους ως προμηθευτές και υπεργολάβοι μεγαλύτερων εταιρειών, έχουν χαρακτηριστεί ως ένας από τους πιο αδύναμους κρίκους της ασφάλειας των πληροφοριών.

Όμως έχει αναγνωριστεί [14], [16], [24], [34], [38], [54], [56], [58] ότι οι ΜΜΕ δεν υιοθετούν καλές πρακτικές ασφάλειας και προστασίας της ιδιωτικότητας, δηλαδή δεν αντιμετωπίζουν αποτελεσματικά την ασφάλεια ΠΣ (π.χ. επιθέσεις, παρακολούθηση δικτύων) ή τις απειλές της ιδιωτικότητας (π.χ. κλοπή, τροποποίηση των προσωπικών δεδομένων), γεγονός το οποίο προκαλεί τεράστια ζημιά και θέτει σε κίνδυνο (π.χ. απώλεια φήμης, απώλεια νομικής συμμόρφωσης, διακοπή της λειτουργίας των επιχειρήσεων) όχι μόνο τους ίδιους, αλλά όλο το σύνολο της αλυσίδας παραγωγής [3],[4]. Ο ENISA έχει χαρακτηρίσει τα ΜΜΕ ως τους πιο αδύναμους κρίκους της ασφάλειας των πληροφοριών [15].

Οι κύριοι λόγοι που καθιστούν τις ΜΜΕ αδύναμους κρίκους στο θέμα της ασφάλειας, προκύπτουν από τα παρακάτω χαρακτηριστικά τους:

- ✓ η ύπαρξη ελάχιστων πόρων από τον προϋπολογισμό ή το χρόνο εμποδίζουν τις ΜΜΕ να αξιολογούν και να διασφαλίζουν την αξιολόγηση και διασφάλιση της ασφάλειας ως μια απαραίτητη και συνεχιζόμενη δραστηριότητα,
- ✓ η έλλειψη εκπαιδευμένου προσωπικού για θέματα ασφάλειας και ιδιωτικότητας,
- ✓ η έλλειψη αποκλειστικής εκπαίδευσης σε θέματα ασφάλειας εξαιτίας του γεγονότος ότι η εκπαίδευση θεωρείται από τις ΜΜΕ περιττό κόστος χωρίς απτό όφελος,
- ✓ η εξάρτησή τους από εξωτερικούς εμπειρογνώμονες ασφαλείας,
- ✓ η έλλειψη επίσημης πολιτικής ασφάλειας και στρατηγικής: ένα σχέδιο που να καθορίζει το επίπεδο ασφάλειας που απαιτείται καθώς και η πολιτική ασφάλειας η οποία να περιγράφει τον τρόπο λειτουργίας και τη διατήρηση της ασφάλειας δεν είναι ένα θέματα ύψιστης προτεραιότητας για τη διοίκηση των ΜΜΕ,

- ✓ η έλλειψη προσοχής εκ μέρους της διοίκησης των ΜΜΕ για την αντιμετώπιση νομοθετικών ή κανονιστικών απαιτήσεων, είτε από άγνοια είτε από το κόστος που απαιτείται (π.χ. ακριβά firewall, συστήματα ανίχνευσης εισβολής, αντίμετρα βάσης δεδομένων), ώστε να γίνουν συμβατοί με αυτές τις απαιτήσεις ακόμα και αν υπάρχει ποινή για το αντίθετο,
- ✓ η έλλειψη διορατικότητας από τα διευθυντικά στελέχη οι οποίοι σκέφτονται τους εαυτούς τους ως «μη ενδιαφέροντος» από μια παγκόσμια προοπτική ("Είμαστε πάρα πολύ μικροί οργανισμοί - Ποιος θα ήθελε να μας επιτεθεί;"), και
- ✓ η έλλειψη γνώσης των πληροφοριακών κινδύνων και, ως αποτέλεσμα, των επιχειρησιακών κινδύνων (π.χ. επιχειρησιακές απώλειες, παραβίαση νόμιμων υποχρεώσεων, απώλεια πελατών, καθώς και απώλεια φήμης) καθώς και των κινδύνων για το ηλεκτρονικό επιχειρείν ως σύνολο.

Ταυτόχρονα, δεν είναι δυνατή η συμμόρφωση των ΜΜΕ με τις αυστηρότερες απαιτήσεις ασφαλείας, όπως ορίζεται από τις συνεργαζόμενες μεγάλες επιχειρήσεις και τους πελάτες τους, με αποτέλεσμα οι ΜΜΕ να χάνουν επιχειρηματικές ευκαιρίες. Όντας η ραχοκοκαλιά της οικονομίας και επικεφαλής της παροχής θέσεων εργασίας σε πολλά κράτη μέλη της ΕΕ, αυτό μπορεί να δημιουργήσει σοβαρές βλάβες στην καινοτομία και την ανταγωνιστικότητα της ευρωπαϊκής οικονομίας. Ως εκ τούτου, καθίσταται επιτακτική ανάγκη, ιδιαίτερα αυτές τις μέρες που η Ευρώπη πρέπει να ενισχύσει την οικονομία της, η ενίσχυση των πρακτικών ασφάλειας των πληροφοριών των ΜΜΕ.

Με στόχο οι ΜΜΕ να ακολουθήσουν βέλτιστες πρακτικές ασφάλειας και ιδιωτικότητας χρειάζονται:

- ✓ καλύτερη κατανόηση και εξοικείωση με τις διάφορες πτυχές και τις απαιτήσεις της ασφάλειας των πληροφοριών και τη διαχείριση της ιδιωτικότητας,
- ✓ συμβουλές και καθοδήγηση σχετικά με διαδικαστικά ζητήματα,
- ✓ απλούστευση των βημάτων και αυτοματοποίηση των πολύπλοκων διαδικασιών, λόγω της περιορισμένης γνώσης και εμπειρία τους σε θέματα ασφάλειας ΠΣ,
- ✓ ενθάρρυνση και ενίσχυση της επικοινωνίας και βελτίωση της συνεργασίας μεταξύ των σε κοινά θέματα και προβλήματα ασφάλειας,
- ✓ βελτιστοποίηση της πρόσβασης στη γνώση και τη μάθηση με στόχο την ενδυνάμωση της ευαισθητοποίησης και κατάρτισης σε θέματα ασφάλειας και προστασίας της ιδιωτικότητας, και
- ✓ πρόσβαση σε αυτό-διαχειριζόμενες και αυτό-εκτιμόμενες προσεγγίσεις οι οποίες να δίνουν έμφαση στη φύση, τα εμπόδια και τις ιδιαιτερότητές τους (από άποψη μεγέθους, των

επιχειρήσεων, διασυνδέσεων με άλλες επιχειρήσεις κ.λπ.), αποφεύγοντας το υψηλό κόστος από την χρήση ακριβών εμπειρογνωμόνων ή συμβούλων ασφάλειας.

Στις ενότητες που ακολουθούν παρουσιάζεται η υφιστάμενη κατάσταση στη διαχείριση ασφάλειας των ΠΣ των ΜΜΕ, αναδεικνύονται οι αδυναμίες τους να ανταπεξέλθουν στις ανάγκες των ΠΣ τέτοιου είδους οργανισμών και στην συνέχεια παρουσιάζονται οι προτάσεις της συγκεκριμένης διδακτορικής διατριβής.

6.3.2 Υφιστάμενη κατάσταση στη διαχείριση ασφάλειας ΠΣ ΜΜΕ

Η διαχείριση της ασφάλειας των πληροφοριών απαιτεί μια συνεχή και συστηματική διαδικασία προσδιορισμού, ανάλυσης, μετριασμού και ελέγχου των τεχνικών, των λειτουργικών και άλλων τύπων κινδύνων. Αυτή η ενότητα περιγράφει και αξιολογεί τις αδυναμίες των υφιστάμενων προσεγγίσεων της ασφάλειας των πληροφοριών να αντιμετωπίσουν τις ανάγκες των ΠΣ των ΜΜΕ.

6.3.2.1 Πρότυπα Διαχείρισης Ασφάλειας ΠΣ ΜΜΕ

Έχουν αναπτυχθεί διάφορα πρότυπα διαχείρισης ασφάλειας προκειμένου να βοηθήσουν τους οργανισμούς να αναπτύξουν ένα Σύστημα Διαχείρισης Ασφαλείας Πληροφοριών (ΣΔΑΠ), όπως το COBIT [12], το ITIL [35], το πρότυπο ISO 17799 [29] και το πρότυπο ISO 27001 [30]. Τα πρότυπα αυτά καθορίζουν τις απαιτήσεις ασφαλείας και καλύπτουν πολλούς τομείς του κύκλου ζωής ασφάλειας, όπως την ασφάλεια, των ΠΣ, επιχειρησιακές, νομικές και οργανωτικές απαιτήσεις ασφαλείας. Ταυτόχρονα, έχουν αναπτυχθεί πρότυπα ασφάλειας για να υποστηρίξουν τους ελέγχους εφαρμογής των μέτρων προστασίας, όπως το πρότυπο ISO 27002 [28].

Συνήθως, η δημιουργία ενός ΣΔΑΠ απαιτεί οικονομικούς και ανθρώπινους πόρους, τη διενέργεια διαφόρων τύπων αναλύσεων και την ανάθεση νέων αρμοδιοτήτων ασφάλειας στο υπάρχον προσωπικό των επιχειρήσεων. Επίσης, η ανάπτυξη και διαχείριση ενός ΣΔΑΠ απαιτεί τεκμηριωμένες πολιτικές, έγγραφες διαδικασίες και την επιβολή της εφαρμογής τους. Οι πόροι αυτοί συνήθως δεν είναι διαθέσιμοι στο περιβάλλον των ΜΜΕ που έχουν την τάση να θεωρούν την ασφάλεια ως επιβάρυνση και όχι πλεονέκτημα. Αν και υπάρχουν αυτοματοποιημένα εργαλεία για την υποστήριξη της διαχείρισης ασφάλειας (όπως το ISO17799 Toolkit [31] ή το NetSPoC [41], VeriNice [64]), αυτά είναι είτε πολύ ακριβά για τις ΜΜΕ ή σε περίπτωση των δωρεάν εργαλείων, δεν υπάρχουν δυνατότητες καθοδήγησης και οδηγίες για τους μη-ειδικούς.

6.3.2.2 Μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας

Ένα ευρύ φάσμα μεθοδολογιών (βλ. Πίνακα 37) έχουν αναπτυχθεί, οι οποίες περιγράφουν συγκεκριμένα βήματα για την ανάλυση επικινδυνότητας. Πολλές από αυτές τις προσεγγίσεις έρχονται με εμπορικά ή σε ορισμένες περιπτώσεις δωρεάν εργαλεία, που όμως δεν είναι εύκολα και φιλικά στην χρήση και απαιτούν τεχνογνωσία ασφάλειας.

Πίνακας 37: Υπάρχουσες μεθοδολογίες και εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας

Μεθοδολογίες / **Κριτήρια**	**Austrian IT Security Handbook [5]**	**COBRA [11]**	**CRAMM [13]**	**Dutch A&K Analysis [18]**	**EBIOS [22]**	**ENISA RM & IT Security [10]**	**IT-Grund-schutz [8]**	**Mehari [39]**	**Octave-S [48]**	**RiskWatch [57]**	**MAGERIT [40]**	**ISO 27005 [27]**
RA/RM	RA / RM	RA/ RM	RA/ RM	RA	RA/ RM	RA/ RM	RA/ RM	RA	RA/ RM	RA/ RM	RA/ RM	RA/ RM
Κόστος	Δωρεάν	Εμπορικό	Εμπορικό	Δωρεάν	Δωρεάν	Δωρεάν	Δωρεάν	Εμπορικό	Δωρεάν	Εμπορικό	Δωρεάν	Εμπορικό
Υποστήριξη ΜΜΕ	Ναι	Ναι	Όχι	Ναι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
Εργαλείο/ Κόστος	Πρωτότυπο / Δωρεάν	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Δωρεάν	Όχι	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Όχι
Συμβατότητα με πρότυπα	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι
Πολύγλωσσο	Μόνο Γερμανικά	Μόνο Αγγλικά	Μόνο Αγγλικά	Μόνο Ολλανδικά	Ναι	Ναι	Μόνο Γερμανικά	Μόνο Γαλλικά	Μόνο Αγγλικά	Μόνο Αγγλικά	Αγγλικά, Ισπανικά	Μόνο Αγγλικά

Σε γενικές γραμμές, οι υπάρχουσες μεθοδολογίες απευθύνονται σε μεγαλύτερους οργανισμούς και απαιτούν την ύπαρξη ειδικών με πολλά χρόνια εμπειρίας. Η ανάλυση και διαχείριση επικινδυνότητας είναι μια πολύπλοκη διαδικασία για τον προσδιορισμό, την αποτίμηση και την διαχείριση των κινδύνων των ΠΣ των ΜΜΕ, οι οποίοι δεν διαθέτουν τους κατάλληλους πόρους, όπως προσωπικό με τεχνογνωσία στην ασφάλεια των πληροφοριών. Ταυτόχρονα, η επιλογή να το αναθέσουν σε ειδικούς είναι μία πολύ ακριβή λύση. Οι προσπάθειες που στοχεύουν ειδικά στις ΜΜΕ, όπως η OCTAVE-S [48] και η ENISA RM & IT Security [10] ακόμα δεν υποστηρίζεται από δωρεάν αυτοματοποιημένα εργαλεία.

Ως αποτέλεσμα, παρά την ύπαρξη πολλών μεθόδων και εργαλείων για την ΑΔΕ, οι μικρότερες επιχειρήσεις αντιμετωπίζουν σοβαρά οργανωτικά προβλήματα κατά την διάρκεια της χρήσης αυτών των εργαλείων και μεθόδων. Οι περιορισμοί των υφιστάμενων μεθοδολογιών μπορούν να συνοψιστούν παρακάτω:

- ✓ Αν και υπάρχουν μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας που επικεντρώνονται στις ΜΜΕ, δεν υποστηρίζονται από δωρεάν αυτοματοποιημένα εργαλεία, ενώ τα υπάρχοντα εμπορικά εργαλεία δεν είναι πιθανόν να χρησιμοποιηθούν από τις ΜΜΕ.
- ✓ Απαιτούνται μερικές απλουστεύσεις των βημάτων των μεθοδολογιών και των αυτοματοποιημένων εργαλείων τους ώστε να είναι πιο στοχευμένες στις ανάγκες των ΜΜΕ.
- ✓ Είναι απίθανο οι χρήστες των ΜΜΕ να χρησιμοποιήσουν τις υπάρχουσες μεθοδολογίες, χωρίς εξωτερική υποστήριξη από ειδικούς ασφάλειας, τουλάχιστον για την πρώτη εφαρμογή.
- ✓ Υπάρχει έλλειψη εμπλοκής οργανώσεων (π.χ. εμπορικά επιμελητήρια) οι οποίοι έχουν ασχοληθεί με ζητήματα που αντιμετωπίζουν οι ΜΜΕ και κατανοούν τις κύριες απαιτήσεις τους, στη σχεδίαση και ανάπτυξη των μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας.
- ✓ Απαιτείται ο σχεδιασμός εξειδικευμένων προσεγγίσεων για κάθε κατηγορία των μικρών, μεσαίων και πολύ μικρών επιχειρήσεων, λαμβάνοντας υπόψη το μέγεθός τους, το τεχνολογικό υπόβαθρο, την εξάρτησή τους από την τηλεπικοινωνιακή τους δομή, τον επιχειρησιακό τους τομέα.
- ✓ Υπάρχει έλλειψη προσεγγίσεων οι οποίες επιτρέπουν την συνεργατικότητα τόσο μεταξύ των ΜΜΕ και άλλων συνεργαζόμενων φορέων, όσο και στο εσωτερικό των ίδιων των ΜΜΕ.

6.3.2.3 Προσεγγίσεις και εργαλεία πρακτικής ανάλυσης Αδυναμιών

Πολλές προσπάθειες έχουν πραγματοποιηθεί από ένα σύνολο μεθόδων και πλαισίων για την Πρακτική Ανάλυση Αδυναμιών (ΠΑΑ). Μερικές από αυτές τις προσπάθειες δίνουν έμφαση στις δοκιμές ασφάλειας των εφαρμογών με την βοήθεια εργαλείων, κατευθυντήριων οδηγιών, λιστών ελέγχου (checklists) με στόχο την αξιολόγηση και τη βελτίωση της ασφάλειας διαδικτυακών εφαρμογών, π.χ. [49], [50]. Άλλες προσπάθειες επικεντρώνονται κυρίως στις δοκιμές ασφάλειας των δικτύων προσδιορίζοντας απαιτήσεις ασφάλειας που πρέπει να καλύπτουν τα δίκτυα, περιγράφοντας τεχνικές εφαρμογής και χρήση συγκεκριμένων εργαλείων [51], [61], [66]. Επίσης, ο έλεγχος ασφάλειας έχει πλαισιωθεί από μια σειρά προτύπων όπως τα OSSTMM [32] και ISSAF [33].

Ένα σύνολο εμπορικών, δωρεάν και ανοικτού κώδικα εργαλείων δοκιμών διείσδυσης (π.χ. [25][55][65]) έχουν αναπτυχθεί και παρέχονται είτε ανεξάρτητα είτε μέσω προ-ρυθμισμένων ανοιχτών περιβαλλόντων (πλατφόρμες) πρακτικής ανάλυσης επικινδυνότητας (π.χ. Backtrack [6], Net Tools 5.0 [42], Samurai Web Testing Framework [60]). Ωστόσο, η σωστή παραμετροποίηση των απαιτούμενων εργαλείων είναι μια πολύ τεχνική και χρονοβόρα διαδικασία που απαιτεί ειδικές γνώσεις και εξειδικευμένο ανθρώπινο δυναμικό. Επιπλέον, οι ανοικτές αυτές πλατφόρμες, συνήθως δεν συνοδεύονται από οδηγίες για το πώς αυτά τα περιβάλλοντα έχουν ρυθμιστεί ή οδηγίες εγκατάστασης των ενσωματωμένων εργαλείων. Ως εκ τούτου, οι δυνητικοί χρήστες (π.χ. άτομα, οργανισμοί) αντιμετωπίζουν αρκετές δυσκολίες για την υιοθέτηση και την ενσωμάτωση αυτών των πλατφορμών στις υποδομές τους. Εν κατακλείδι, η ανεπαρκής χρήση της πρακτικής ανάλυσης αδυναμιών προκαλεί σημαντικά κενά ασφαλείας στη συνολική διαδικασία διαχείρισης κινδύνου.

Συμπερασματικά, οι αδυναμίες που εντοπίστηκαν στις υπάρχουσες προσεγγίσεις πρακτικής ανάλυσης αδυναμιών μπορούν να συνοψιστούν ως εξής:

- ✓ Παρόλο που υπάρχουν δωρεάν εργαλεία ΠΑΑ, είναι μάλλον απίθανο οι ΜΜΕ να είναι σε θέση να χρησιμοποιήσουν αυτά τα εργαλεία, λόγω της έλλειψης τεχνογνωσίας.
- ✓ Υπάρχει έλλειψη κατάλληλων μεθοδολογιών ΠΑΑ για τα ΠΣ των ΜΜΕ, με τις οποίες οι ΜΜΕ θα είναι σε θέση να χρησιμοποιήσουν εύκολα μόνοι τους και εκτελέσουν τεχνική αξιολόγηση των αδυναμιών του ΠΣ τους. Οι χρήστες των ΜΜΕ δεν έχουν την πείρα να εντοπίσουν, να αξιολογήσουν, να εγκαταστήσουν και να παραμετροποιήσουν τα εργαλεία ασφαλείας που απαιτούνται από τις υπάρχουσες μεθοδολογίες.
- ✓ Υπάρχει έλλειψη μεθοδολογιών ΠΑΑ οι οποίες να συνδέονται με προ-ρυθμιζόμενες πλατφόρμες.
- ✓ Υπάρχει έλλειψη μεθοδολογιών και εργαλείων ΠΑΑ των οποίων τα αποτελέσματα να συνδέονται άμεσα με τις διαδικασίες της ανάλυσης και διαχείρισης επικινδυνότητας.

- ✓ Δεν υπάρχει ενεργός συμμετοχή οργανισμών/ενώσεων (π.χ. εμπορικά επιμελητήρια) στην εφαρμογή και υλοποίηση τέτοιων μεθοδολογιών και εργαλείων, γεγονός το οποίο θα βοηθούσε σημαντικά τους χρήστες των ΜΜΕ τόσο οικονομικά όσο και εκπαιδευτικά. Τέτοιου είδους οργανισμοί θα έπαιζαν το ρόλο των συμβούλων ασφάλειας ώστε να εκπαιδευτούν οι χρήστες των ΜΜΕ για την χρήση τέτοιων μεθόδων και εργαλείων, εξοικονομώντας χρόνο και μειώνοντας το κόστος.
- ✓ Τα υπάρχοντα εργαλεία ΠΑΑ που είναι διαθέσιμα και προσβάσιμα κατά απαίτηση μέσω διαδικτύου ή παρέχονται σαν υπηρεσία (software as a Service), είτε απαιτούν κάποιο συμβεβλημένο ποσό είτε παρέχονται δωρεάν από μη αξιόπιστα πρόσωπα.

6.3.3 Ανοιχτά θέματα - Συνεισφορά διατριβής

Οι ΜΜΕ δυσκολεύονται να ερμηνεύσουν και να κατανοήσουν τι σημαίνει ασφάλεια πληροφοριών, τι ακριβώς χρειάζεται να προστατεύσουν, πώς μπορούν να χρησιμοποιήσουν τα πρότυπα ασφαλείας, πώς τα μέτρα ασφαλείας επηρεάζουν τη λειτουργία των επιχειρήσεων τους, πώς οι κανονισμοί ασφάλειας και ιδιωτικότητας μπορεί να επηρεάσουν την επιχείρησή τους και τι οφέλη μπορεί να τους φέρουν [9]. Συνήθως, δεν είναι ενήμεροι βασικών όρων, όπως η ασφάλεια των πληροφοριών, η διαχείριση κινδύνων, η πολιτική ασφάλειας, η συμμόρφωση με την ασφάλεια, η προστασία της ιδιωτικότητας ή διασφάλιση της πληροφορίας, ενώ ταυτόχρονα υποφέρουν από διάφορες παραβιάσεις της ασφάλειας οι οποίες προκαλούν επιχειρηματικές απώλειες. Η ενίσχυση της ασφάλειας των η-υπηρεσιών των ΜΜΕ μπορεί να χρησιμοποιηθεί ως ένα σημαντικό ανταγωνιστικό πλεονέκτημα.

Οι υφιστάμενες μεθοδολογίες, πρότυπα και προσεγγίσεις διαχείρισης ασφάλειας και προστασίας της ιδιωτικότητας, οι οποίες παρουσιάστηκαν στις προηγούμενες ενότητες, είναι πολύ βαριές για τις υποδομές των ΜΜΕ, την τεχνογνωσία και τον προϋπολογισμό τους. Επίσης, δεν είναι σε θέση να αντιμετωπίσουν τα χαρακτηριστικά τους (π.χ. μέγεθος των επιχειρήσεων), τις ανάγκες και απαιτήσεις, δεδομένου ότι είναι πολύ γενικές, σύνθετες, με περιορισμένη καθοδήγηση σχετικά με το πώς πρέπει να χρησιμοποιούνται από άπειρους και μη εξειδικευμένους χρήστες. Επιπλέον, βασίζονται σε μια πληθώρα ερωτηματολογίων που περιλαμβάνουν όρους, τεχνικά χαρακτηριστικά και λειτουργίες τα οποία για τους περισσότερους χρήστες των ΜΜΕ είναι άγνωστα. Αυτό καθιστά την εφαρμογή των διαδικασιών διαχείρισης ασφάλειας με μια ακόμη πιο επώδυνη, απογοητευτική και αποθαρρυντική δραστηριότητα, με αποτέλεσμα να οδηγούνται στο να συμβουλεύονται εμπειρογνώμονες.

Η παρούσα διδακτορική διατριβή στοχεύει να απαντήσει στις παραπάνω προκλήσεις με την παραμετροποίηση του συνεργατικού περιβάλλοντος διαχείρισης ασφάλειας STORM.

Συγκεκριμένα, όραμα του STORM είναι να βοηθήσει τις ΜΜΕ να έχουν επίγνωση της ασφάλειας ΠΣ, να ακολουθούν βέλτιστες πρακτικές και να διαχειρίζονται την ασφάλεια των ΠΣ με έναν οικονομικό (από άποψη προϋπολογισμού, πόρων, προσπάθειας και χρόνου), φιλικό και αποτελεσματικό τρόπο, καλύπτοντας τις ιδιαιτερότητές τους οι οποίες πηγάζουν από τις περιορισμένες γνώσεις, τον προϋπολογισμό και την πολυμορφία των υποδομών τους. Στο πλαίσιο αυτό, το συνεργατικό περιβάλλον STORM στοχεύει να βοηθήσει τις ΜΜΕ να αναπτύξουν μια κουλτούρα ασφάλειας και ταυτόχρονα να αποκτήσουν ένα πολύτιμο εργαλείο για την αποτελεσματική διαχείριση ασφάλειας. Ειδικότερα, το περιβάλλον STORM και οι υπηρεσίες που παρέχει συμβάλλουν:

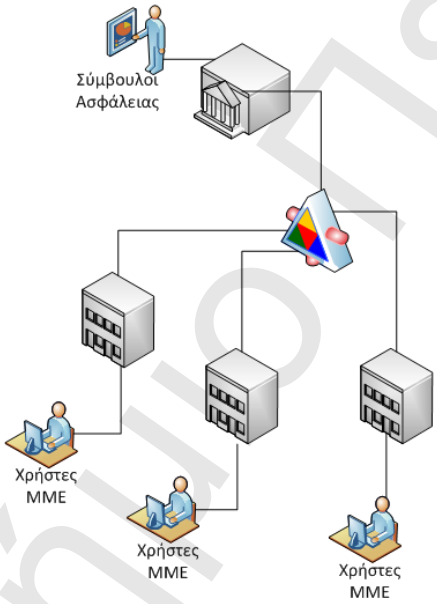
- ✓ στην αύξηση της κουλτούρας ασφάλειας ΠΣ,
- ✓ στην ανάπτυξη του αισθήματος εμπιστοσύνης στους πελάτες τους,
- ✓ στην αύξηση της προβλεψιμότητας και στη μείωση της αβεβαιότητας των επιχειρηματικών δραστηριοτήτων, με τη μείωση των κινδύνων και των προσδιορισμό των αποδεκτών επιπέδων κινδύνου,
- ✓ στην συνεχή ενημέρωση με τις τρέχουσες και τις επερχόμενες απειλές, τις βέλτιστες πρακτικές και τους σχετικούς κανονισμούς που τους αφορούν μειώνοντας τις πιθανότητες διακοπής της επιχειρησιακής λειτουργίας τους,
- ✓ στην παροχή εκπαίδευσης και ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας,
- ✓ στην καθοδήγηση επιλογής κατάλληλων μέτρων προστασίας τα οποία ταιριάζουν στις ανάγκες τους, με εξισορρόπηση του κόστους με τα επιχειρηματικά οφέλη,
- ✓ στον διευκόλυνση της επικοινωνίας και στην προώθηση της συνεργασίας τόσο μεταξύ των ΜΜΕ όσο και μεταξύ εργαζομένων με από κοινού ανησυχίες,
- ✓ στο να βοηθήσει τις ΜΜΕ για το πώς να συμμορφωθούν με τις νομικές και κανονιστικές κυρώσεις και να τηρούν ενήμερο το νομικό τους καθεστώς,
- ✓ στην υιοθέτηση μιας στρατηγικής ασφάλειας η οποία μπορεί να ενσωματωθεί στην υπάρχουσα επιχειρησιακή λειτουργία και λογική των ΜΜΕ.

Στόχος του συνεργατικού περιβάλλοντος STORM είναι να παρέχει στις ΜΜΕ τη δυνατότητα να αποκτήσουν μια συνολική στρατηγική εικόνα της ασφάλειας των ΠΣ τους, βοηθώντας τους να την αντιμετωπίζουν ως ένα παράγοντα που εγγυάται και ενισχύει τη βιωσιμότητά τους σε μία ανταγωνιστική, ταραχώδη και ποικιλόμορφη παγκοσμιοποιημένη ηλεκτρονική αγορά. Στο πλαίσιο αυτό, οι επιχειρήσεις αυτές θα κερδίσουν την εμπιστοσύνη στις παγκόσμιες αγορές ώστε να μπορούν να γίνουν ανταγωνιστικές και βασικές κινητήριες δυνάμεις της ευρωπαϊκής οικονομίας.

6.3.4 Συνεργατικό εργαλείο για την διαχείριση ασφάλειας των ΠΣ ΜΜΕ

Λαμβάνοντας υπόψη τις παραπάνω ανάγκες και με στόχο την ικανοποίηση των ιδιαίτερων χαρακτηριστικών των ΜΜΕ παραμετροποιήθηκε το συνεργατικό περιβάλλον διαχείρισης ασφάλειας STORM [45], [46].

Το περιβάλλον STORM προτείνεται να φιλοξενηθεί από κατάλληλους φορείς παροχής υπηρεσιών (SP), (π.χ. Εμπορικά Επιμελητήρια, ενώσεις ΜΜΕ) οι οποίοι θα υποστηρίζονται από κατάλληλα εξειδικευμένο προσωπικό και θα προσφέρουν τις υπηρεσίες του STORM σε χαμηλό κόστος για τις ΜΜΕ μέλη (Εικόνες 58, 59).

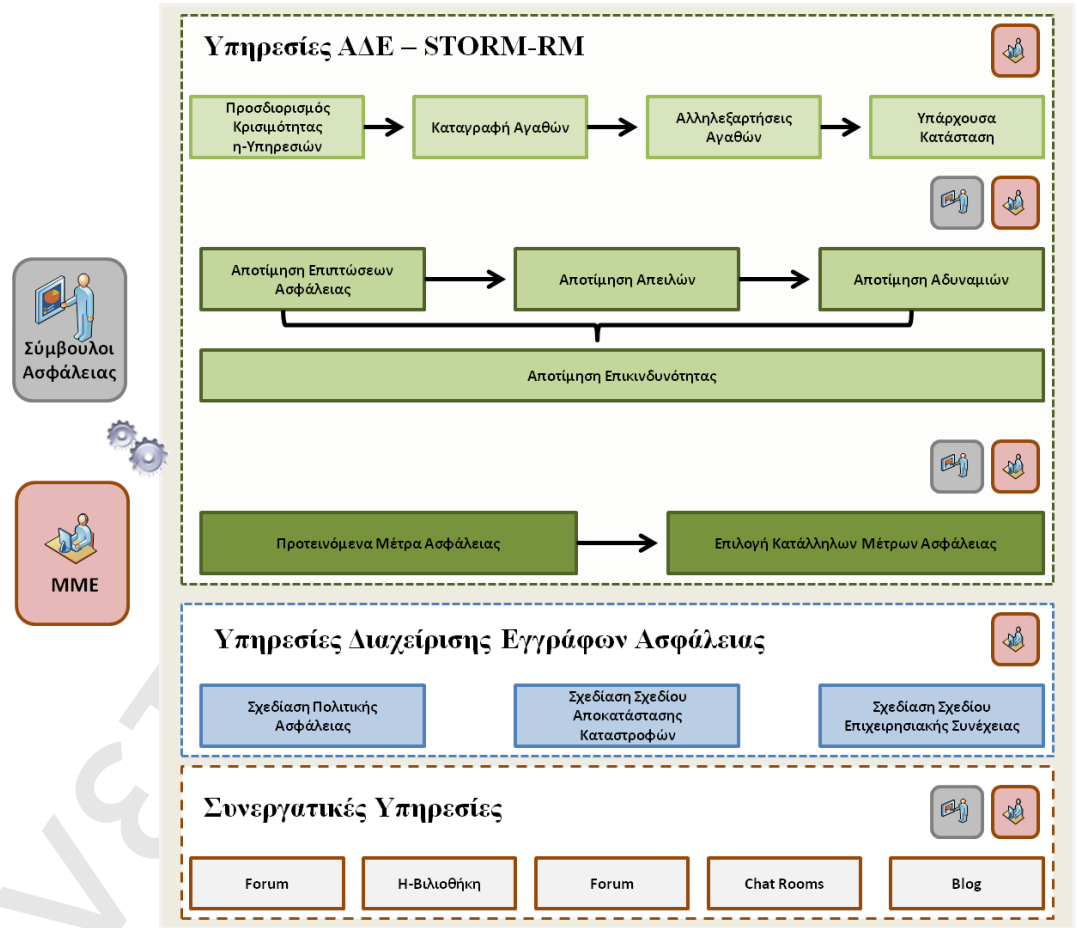


Εικόνα 58: Περιβάλλον STORM

Οι ειδικοί σε θέματα ασφάλειας, θα παίξουν το ρόλο συμβούλων για τις ΜΜΕ προκειμένου να βοηθήσουν τους χρήστες τους να διαχειριστούν την ασφάλεια των ΠΣ τους. Πιο συγκεκριμένα, οι εμπειρογνώμονες σε θέματα ασφάλειας θα αναλάβουν τον ρόλο της *Ομάδας Ασφάλειας* (βλ. Κεφάλαιο 5), καθώς οι ΜΜΕ δεν έχουν την δυνατότητα ύπαρξης τέτοιας ομάδας, οι οποίοι θα είναι σε θέση να:

- ✓ ενημερώνουν συνεχώς το εργαλείο με όλες τις απαραίτητες πληροφορίες (τεχνικές οδηγίες, εγχειρίδια των εργαλείων ασφάλειας, της επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, διεθνή πρότυπα, νομοθεσία κλπ.),
- ✓ να αναλύουν τα αποτελέσματα της εκτίμησης κινδύνου,
- ✓ να αναλύουν τα αποτελέσματα από τις δοκιμές πρακτικής ανάλυσης αδυναμιών, και
- ✓ να προτείνουν κατάλληλα μέτρα προστασίας για τα ΠΣ των ΜΜΕ.

Προκειμένου να χρησιμοποιηθεί το STORM από τις MME, παραμετροποιήθηκε το *Σύστημα Διαχείρισης Ταυτοτήτων* (βλ. Κεφάλαιο 5) έτσι ώστε να ελέγχει την πρόσβαση των χρηστών των MME στις υπηρεσίες STORM. Μέσω του *Συστήματος Διαχείρισης Ταυτοτήτων* του STORM, οι χρήστες των MME θα έχουν πρόσβαση στις *Συνεργατικές Υπηρεσίες* (βλ. 5.6.3Συνεργατικές Υπηρεσίες STORM) έτσι ώστε να συνεργάζονται και να ανταλλάσσουν πληροφορίες και ιδέες, να δουλεύουν μαζί σε ανοιχτές ομάδες εργασίας, και να εξασφαλίζεται η πολυμορφία απόψεων, σκέψεων και της ανταλλαγής πληροφοριών, εμπειρίας και τεχνογνωσίας. Αξιοσημείωτα σημεία των υπηρεσιών αυτών είναι τα Forum, τα Blog και τα chat rooms τα οποία υποστηρίζουν δημόσιες και ιδιωτικές συζητήσεις καθώς και το Wiki το οποίο θα λειτουργεί ως πηγή γνώσης σχετικά με την ασφάλεια πληροφοριών (π.χ. πρότυπα ασφαλείας, προδιαγραφές των εκθέσεων ασφάλειας, μεθοδολογίες και πλαίσια πρακτικής ανάλυσης αδυναμιών, νομικές και ρυθμιστικές οδηγίες και συστάσεις, ανοιχτού κώδικα και δωρεάν εργαλεία και πλατφόρμες).



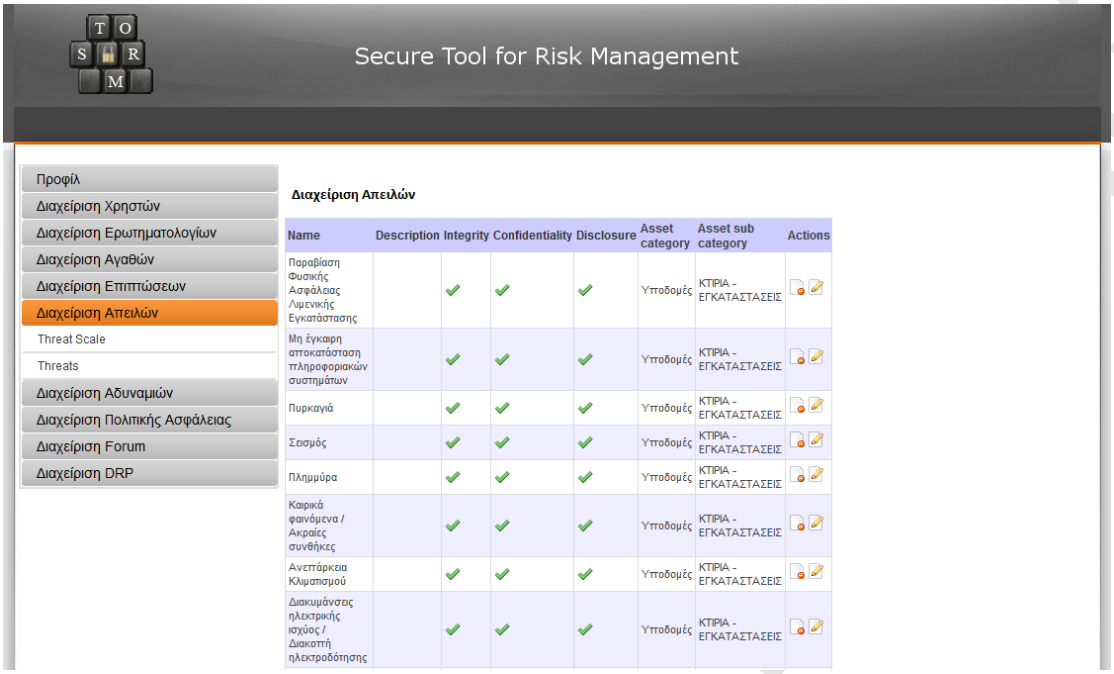
Εικόνα 59: Υπηρεσίες STORM προσανατολισμένες σε χρήστες MME

Ταυτόχρονα μέσω των υπόλοιπων υπηρεσιών του STORM οι χρήστες των MME θα είναι σε θέση να:

- ✓ καταγράφουν, επεξεργάζονται και ανανεώνουν τις απαραίτητες λίστες των πληροφοριακών αγαθών τους (π.χ. δρομολογητές, εξυπηρετητές εφαρμογές, βάσεις δεδομένων),
- ✓ καταγράφουν τις αλληλεξαρτήσεις των πληροφοριακών αγαθών τους, μέσω της Υπηρεσίας Χαρτογράφησης,
- ✓ αξιολογούν την σημαντικότητα των αγαθών σε περίπτωση απώλειας της ασφάλειας τους (απώλεια διαθεσιμότητας, εμπιστευτικότητας, ακεραιότητας) μέσω της Υπηρεσίας Αποτίμησης Επιπτώσεων Ασφάλειας,
- ✓ προσδιορίζουν και αξιολογούν τις απειλές και αδυναμίες των αγαθών τους, μέσω των υπηρεσιών Αποτίμησης Απειλών και Αδυναμιών,
- ✓ αξιολογούν τον βαθμό κρισιμότητας των η-υπηρεσιών τους, μέσω της Υπηρεσίας Αποτίμησης Επικινδυνότητας.
- ✓ επιλέγουν τα κατάλληλα μέτρα προστασίας (με την βοήθεια των ειδικών συμβούλων) μέσω των Υπηρεσιών Διαχείρισης Επικινδυνότητας, και
- ✓ δημιουργούν και να επικαιροποιούν την Πολιτική ασφάλειας, το Σχέδιο Αποκατάστασης Καταστροφών και Επιχειρησιακής Συνέχειας μέσω της Υπηρεσίας Διαχείρισης Εγγράφων Ασφάλειας.

Παρακάτω ακολουθούν κάποιες ενδεικτικές οθόνες του παραμετροποιημένου συνεργατικού περιβάλλοντος STORM για τις ΜΜΕ.

Εικόνα 60: Απεικόνιση αποτελεσμάτων Ανάλυσης Επικινδυνότητας από τους κατάλληλους χρήστες των ΜΜΕ



Εικόνα 61: Διαχείριση Απειλών από τους συμβούλους ασφάλειας

6.3.5 Συμπεράσματα – Ανοιχτά θέματα

Οι ΜΜΕ πρέπει να αποκτήσουν μια συνολική εικόνα της ασφάλειας των πληροφοριών. Θα πρέπει να την αντιμετωπίζουν ως ένα παράγοντα που εγγυάται και ενισχύει τη βιωσιμότητά τους σε ένα ανταγωνιστικό, ταραχώδη και ποικιλόμορφο περιβάλλον ηλεκτρονικού επιχειρείν. Προς την κατεύθυνση αυτή, το περιβάλλον STORM, μέσω της παροχής ενός συνόλου καινοτόμων υπηρεσιών ασφάλειας και προστασίας της ιδιωτικότητας, προσφέρει στις μικρές και μικρομεσαίες επιχειρήσεις πολλά οφέλη, τα οποία μπορούν να συνοψιστούν στα εξής:

- ✓ **Διαφοροποίηση της αγοράς**: η συμμόρφωση των ΜΜΕ με ένα σύνολο νομικών και ρυθμιστικών κανόνων αλλά και προτύπων διαχείρισης ασφάλειας αποτελεί βασική προϋπόθεση της συνεργασίας τους με μεγάλους οργανισμούς οι οποίοι καθορίζουν με τη σειρά τους παρόμοιες απαιτήσεις ασφαλείας στους προμηθευτές τους.
- ✓ **Προσαρμογή στις ανάγκες του νέου επιχειρηματικού περιβάλλοντος**: Το επιχειρηματικό περιβάλλον έχει γίνει όλο και πιο πολύπλοκο, με τις επιχειρήσεις και τα ΠΣ τους να αλληλοεξαρτώνται, με τα προσωπικά δεδομένα των πελατών να μοιράζονται όλο και περισσότερο σε ολόκληρη την αλυσίδα παραγωγής με αποτέλεσμα να απαιτείται προστασία της ιδιωτικότητας και της ασφάλειας, προκειμένου να εκτελέσει το ηλεκτρονικό επιχειρείν με έναν αξιόπιστο και ασφαλή τρόπο. Η υιοθέτηση και η ανάπτυξη αυστηρών πολιτικών ασφαλείας και η υλοποίηση κατάλληλων μέτρων

προστασίας των δεδομένων των πελατών από τις ΜΜΕ, θα τους επιτρέψει να ανταπεξέλθουν στο νέο επιχειρηματικό περιβάλλον,

- ✓ **Προστασία φήμης και βελτίωση της εικόνας:** Μια υπεύθυνη και προοδευτική στάση σε θέματα ασφάλειας και προστασίας των πληροφοριών, συμπεριλαμβανομένης της προστασίας των προσωπικών δεδομένων των πελατών καθώς και των αποκλειστικών πληροφοριών των ίδιων των επιχειρήσεων έχει ως αποτέλεσμα να προστατευθεί η φήμη και το όνομα της επιχείρησης,
- ✓ **Μεγαλύτερα περιθώρια κερδοφορίας**: Το αυξημένο ποσοστό των παραβιάσεων ασφάλειας των προσωπικών δεδομένων των πελατών, το οποίο οφείλεται σε ανεπαρκή προσέγγιση της ασφάλειας εκ μέρους των ΜΜΕ, μπορεί να οδηγήσει σε μείωση της εμπιστοσύνης των πελατών και μείωση των πωλήσεων.
- ✓ **Πρόσθετες παρεχόμενες υπηρεσίες/ προϊόντα**: Μια αρκετά καλή διαχείριση ασφάλειας αποτελεί προϋπόθεση να διατηρηθούν τα υφιστάμενα προϊόντα και υπηρεσίες και να δημιουργηθούν νέα προϊόντα και υπηρεσίες. Ως εκ τούτου, η ασφάλεια των πληροφοριών είναι θεμελιώδους σημασίας για την συνέχεια της επιχειρηματικής δραστηριότητας για τις μικρές, μεσαίες και πολύ μικρές επιχειρήσεις.
- ✓ **Μείωση του κόστους παραβιάσεων της ασφάλειας:** Οι ΜΜΕ οι οποίες αντιμετωπίζουν παραβιάσεις ασφάλειας μπορεί να είναι σε οικονομική δυσχέρεια. Μια παραβίαση μπορεί να προκαλέσει είτε άμεσο κόστος, όπως είναι τα πρόστιμα που επιβάλλονται από τις ρυθμιστικές αρχές ή οι αποζημιώσεις σε πελάτες, ή ακόμα και έμμεσο κόστος, για παράδειγμα μέσω της απώλειας των δικαιωμάτων πνευματικής ιδιοκτησίας ή διαρροή εσόδων. Σε αυτά θα πρέπει επίσης να προστεθεί και το κόστος αντιμετώπισης των περιστατικών που συνδέονται με το χρόνο και τα χρήματα που απαιτούνται για την αποκατάσταση των πραγματικών περιστατικών. Με τον τρόπο αυτό, οι ΜΜΕ είναι σε θέση να εξοικονομήσουν μακροπρόθεσμα ένα σημαντικό χρηματικό ποσό για περαιτέρω επενδύσεις και οικονομική ανάπτυξη.

Το κύριο πλεονέκτημα του περιβάλλοντος STORM είναι η υιοθέτηση μίας νέας καινοτόμας, συνεργατικής και εξειδικευμένης μεθοδολογίας ανάλυσης και διαχείρισης επικινδυνότητας, η οποία με τη χρήση απλουστευμένων εργαλείων, τα οποία ενσωματώνουν αυτοματοποιημένα βήματα, ανταποκρίνεται στις ιδιαίτερες ανάγκες των μικρών, μεσαίων και μικρομεσαίων επιχειρήσεων.

6.4 Βιβλιογραφία 6ου Κεφαλαίου

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

[2] Adler R., Fuller J., "An Integrated Framework for Assessing and Mitigating Risks to Maritime Critical Infrastructure", in Proc. of IEEE Conference on Technologies for Homeland Security, pp. 252-257, May 2007.

[3] Allison & Strangwick. (2008). Privacy Through Security, Policy & Practice in an SME. In R. Subramanian, Computer Security, Privacy & Politics: Current Issues, Challenges & Solutions. IRM Press.

[4] Anderson & Moore. (2006). Information Security Economics - and Beyond. Science , 610-613.

[5] Austrian IT Security Handbook, available at www.cio.gv.at (accessed August 2012).

[6] Backtrack, available at http://www.backtrack-linux.org/ (accessed August 2012).

[7] Balmat J., Lafont F., Maifret R., Pessel N., "MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor", Ocean Engineering, Vol. 36, No. 15-16, pp. 1278-1286, November 2009.

[8] BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, available at https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile (accessed December 2011).

[9] Burns, A., Davies, A. & Beynon Davies, P. (2006) A study of the uptake of Information Security Policies by small and medium sized businesses in Wales, paper presented to Global Conference on Emergent Business Phenomena in the Digital Economy, Tampere, Finland, November 28th - December 2nd, 2006.

[10] D. Catteddu and L. Marinos, "An Information Security Risk Assessment & Management Approach for SMEs", Vol. 4, No. 4, Oct-Dec 2008, available at http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2008-vol.-4-no.-4 (accessed August 2012).

[11] COBRA Methodology - Security Risk Analysis & Assessment, available at http://www.riskworld.net/method.htm (accessed August 2012).

[12] COBIT4.0 - Control Objectives Management Guidelines Maturity Models, available at http://www.sis.pitt.edu/~gray/ITMgnt/references/cobit/COBIT4.pdf (accessed August 2012).

[13] CRAMM version 5.2 information security toolkit, available at http://www.cramm.com (accessed August 2012).

[14] Cyril Onwubiko, Andrew P. Lenaghan. Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. In Proceedings of ISI'2007. pp.244~249.

[15] Werner Degenhardt, Urs E. Gattiker, Philipp Graf, Nineta Polemi, Ken Rabey, David Reynolds, Claudio Telmon, Philippe Vanries, IIari Patrick Lindy, Peter Pfeifhofer. "ENISA report Analysing Micro Enterprises" Needs and Expectations in the Area of Information Security (IS)". ENISA, 19/10/08 available at http://www.enisa.europa.eu/act/sr/reports/micro-enterprises/files/wg-micro-report (accessed August 2012).

[16] Ian Diamond AcSS "The economics of information security" ESRC Seminar Series, Economic and Social Research Council, available at http://www.abdn.ac.uk/~csc335/ESRC-PPS-EIS.pdf (accessed August 2012).

[17] Downs B., "The Maritime Security Risk Analysis Model", in US Coast Guard Proc. Of the Marine Safety and Security Council, Spring 2007. Available at http://www.uscg.mil/proceedings/ (accessed February 2011).

[18] Dutch A&K Analysis, available at http://rm-inv.enisa.europa.eu/methods_tools/m_dutch_ak_analysis.html (accessed August 2012).

[19] European Aviation Safety Agency, available at http://www.easa.europa.eu, (accessed December 2011).

[20] European Maritime Safety Agency, available at http://www.emsa.europa.eu/, (accessed August 2012).

[21] European Network and Information Security Agency (ENISA), "workshop on cyber security aspects in the maritime sector". Available at http://www.enisa.europa.eu/act/res/workshops-1/2011/cyber-security-aspects-in-the-maritime-sector, 2011.

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

[23] Haavel R., Oit M., Usk A., "Maritime surveillance information availability in Estonia", E. Shahbazian, et al. (Eds.), Harbor protection through data fusion technologies, pp. 53-60, Springer, Netherlands, 2009.

[24] Henson, Richard and Hallas, Bruce (2009) "SMEs, Information Risk Management, and ROI". In: Athens Institute for Education and Research (ATINER) SMEs Conference 2009, 10th-13th August 2009, Athens, Greece.

[25] "Information Assurance. Tools Report. Vulnerability Assessment." Sixth Edition. May 2, 2011, IATAC, Distribution Statement A, available at http://iac.dtic.mil/iatac/download/vulnerability_assessment.pdf.

[26] International Maritime Organization, available at http://www.imo.org/Pages/home.aspx (accessed December 2011)

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

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

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

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

[31] ISO17799 Toolkit, available at http://www.iso17799-made-easy.com/ (accessed August 2012).

[32] Introduction and Sample to the Open Source Security Testing Methodology Manual (OSSTMM 3 LITE), available at http://www.idpnow.net/Documents/OSSTMM_3.0_LITE.pdf (accessed August 2012).

[33] Information Systems Security Assessment Framework (ISSAF), available at http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1a/view.html (accessed August 2012).

[34] Information security for small and medium sized enterprises (ISSA-UK 5173). A draft standard by the UK Information Systems Security Association (ISSA). March 2011, available at http://www.issa-uk.org/issa_5173/ISSA-UK_Draft_Standard_on_Information_Security_for_SMEs.pdf (accessed August 2012).

[35] ITIL V3 - Quick Reference Jul 2008, available at http://www.scribd.com/ITIL-V3-Quick-Reference-Jul-2008/d/15337807 (accessed August 2012).

[36] Kakish B., "Harbour protection in the Jordanian port of Aqaba", E. Shahbazian, et al. (Eds.), Harbour protection through data fusion technologies, pp. 37-41, Springer, Netherlands, 2009.

[37] Kang M., Li M., Montrose B., Khashnobish A., Elliott S., Bell M., Pieper S., "Overview of the security architecture of the Comprehensive Maritime Awareness system", in Proc. of Military Communications Conference (MILCOM 2009), pp. 1-7, IEEE Press, October 2009.

[38] M Kimwele, W Mwangi, S Kimani Adoption of information technology security policies: Case study of Kenyan small and medium enterprises (SMES). in Journal of Theoretical and Applied Information Technology (2010)

[39] Mehari, available at www.clusif.asso.fr (accessed August 2012).

[40] Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2), launched by the Public Administration Ministry, available at http://www.csi.map.es/csi/pg5m20.htm#_blank (accessed August 2012).

[41] NetSPoC - Network Security Policy Compiler, available at http://netspoc.berlios.de/ (accessed August 2012).

[42] Net Tools 5.0, available at http://www.mabsoft.com/nettools.htm (accessed August 2012).

[43] Novikov S., "Implementation of the ISPS code in the Russian Federation: Ships and ports", E. Shahbazian, et al. (Eds.), Harbour protection through data fusion technologies, pp. 23-26, Springer, Netherlands, 2009.

[44] Ntouskas, T., Polemi, N., "Collaborative security management services for Port Information Systems", in Proc. of International Conference on e-Business, ICE-B 2012, Rome, Italy, SciTePress, pp. 305-308.

[45] Ntouskas, T., Papanikas, D. and Polemi, N. (2012) "Trusted collaborative services for the IT security management of SMEs/mEs", Int. J. Electronic Security and Digital Forensics, Vol. 4, Nos. 2/3, pp.124–137.

[46] Ntouskas, T., Papanikas, D., Polemi N., "A collaborative system offering security management services for SMEs/mEs", in Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability (ICGS3-2011), R. Bashroush, et al. (Eds.), LNICST 99, Springer, pp. 220–228, 2012.

[47] Ntouskas, T., Polemi, N., "A secure, collaborative environment for the security management of Port Information Systems" Proceedings of the Fifth International Conference on the Internet and Web Applications and Services, ICIW 2010, IEEE Computer Society Digital Library, Barcelona, Spain, 2010, pp 374-379.

[48] OCTAVE methods. (2003). Retrieved 9 February 2006 from http://www.cert.org/octave/methods.html (accessed August 2012).

[49] "OWASP Testing Guide", 2008 V3.0, available at http://www.mare-system.de/whitepaper/OWASP_Testing_Guide_V3.pdf (accessed August 2012).

[50] "OWASP Code review", 2008 V1.1, available at https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf (accessed August 2012).

[51] Penetration Testing Framework v0.21, available at http://www.vulnerabilityassessment.co.uk/Penetration%20Test.htm (accessed August 2012).

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

[53] Polemi, N.: Security management of the ports' information systems. ENISA Personal study. Available at http://www.enisa.europa.eu (accessed August 2012)..

[54] C. Potter, A. Beard, "Information Security Breaches Survey 2010", technical report, PricewaterhouseCoopers. Available at http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf (accessed August 2012).

[55] Renub Research. "Worldwide Vulnerability Assessment Market and 13 Companies Analysis" MarketResearch.com, 2011.

[56] R. Richardson, "CSI Computer Crime & Security Survey", 2008, available at http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

[57] RiskWatch: Information systems & ISO 17799 2005 Product Sheet, available at http://www.riskwatch.com (accessed August 2012).

[58] George Sadowsky, J.X. Dempsey, A. Greenberg, B.J. Mack and A. Schwartz, Information Technology Security Handbook, infoDev (World Bank), 2003, pp. 178-179. http://www.infodev-security.net/ (accessed August 2012).

[59] SafeSeaNet: http://www.emsa.eu.int/ (accessed August 2012).

[60] Samurai Web Testing Framework, available at http://samurai.inguardians.com/ (accessed August 2012).

[61] K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh, "Technical Guide to Information Security Testing and Assessment", Special Publication 800-115, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (accessed August 2012).

[62] Sokolov A., "Steps to Better Waterside Port and Harbor Security: The Development of Regional Maritime Safety Systems in the Russian Federation", E. Shahbazian, et al. (Eds.), Harbour protection through data fusion technologies pp. 27–32, Springer, Netherlands, 2009.

[63] Trans-European Transport Network Executive Agency, available at http://tentea.ec.europa.eu/ (accessed August 2012).

[64] Verinice, available at http://www.verinice.org/en/ (accessed August 2012).

[65] Vladimirov, Andrew, Konstantin Gavrilenko, and Andriej Michajlowski. "Assessing Information Security: Strategies, Tactics, Logic and Framework", IT Governance Publishing, 2010.

[66] J. Wack, M. Tracy, M. Souppaya, "Guideline on Network Security Testing - Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-42. Available at http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf (accessed August 2012).

Κεφάλαιο 7ο

7 Επίλογος - Μελλοντικές ερευνητικές κατευθύνσεις

Η παρούσα διδακτορική διατριβή ερεύνησε τις μεθοδολογίες και τα εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ. Συγκεκριμένα αξιολόγησε, βάση συγκεκριμένων κριτηρίων, τις υπάρχουσες προσεγγίσεις με στόχο να εκτιμήσει την αποτελεσματικότητά τους στα σημερινά πολύπλοκα και κατανεμημένα ΠΣ. Αντιμετώπισε την ανάλυση και διαχείριση επικινδυνότητας ως ένα πολυκριτηριακό πρόβλημα συλλογικής λήψης αποφάσεων, όπου πολλοί συμμετέχοντες (όλοι οι χρήστες του ΠΣ) καλούνται να επιλύσουν τα εξής προβλήματα:

- ✓ Εντοπισμός των κρίσιμων η-υπηρεσιών του οργανισμού.
- ✓ Εντοπισμός των επιπτώσεων ασφάλειας ενός κακόβουλου γεγονότος.
- ✓ Προσδιορισμός των απειλών και των αδυναμιών των αγαθών του ΠΣ του οργανισμού τους.
- ✓ Προσδιορισμός και αξιολόγηση του βαθμού επικινδυνότητας στον οποίο είναι εκτεθειμένα τα αγαθά του ΠΣ του οργανισμού τους.
- ✓ Επιλογή των κατάλληλων μέτρων προστασίας από τους επικείμενους κινδύνους.

Για κάθε ένα από τα παραπάνω προβλήματα, οι χρήστες των ΠΣ, δηλαδή οι τοπικοί χρήστες, οι διαχειριστές, τα μέλη της διοίκησης, τα μέλη της ομάδας ασφάλειας, καλούνται να δώσουν την δική τους λύση βασισμένοι στην εμπειρία τους και τις προσωπικές τους αντιλήψεις και τεχνολογικές ή επιχειρηματικές γνώσεις.

Για τους λόγους αυτούς, αναπτύχθηκε μια συνεργατική και πολυκριτηριακή μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας, η STORM-RM, η οποία είναι βασισμένη στα πρότυπα ασφάλειας και συνδυάζει την πολυκριτηριακή ανάλυση προκειμένου να αντιμετωπίσει και να επιλύσει τα πολυσύνθετα παραπάνω προβλήματα.

Ταυτόχρονα, έπειτα από βιβλιογραφική έρευνα πάνω στον αντίστοιχο χώρο και εντοπισμό των ελλείψεων των υπαρχόντων εργαλείων ανάλυσης και διαχείρισης ασφάλειας ΠΣ, προτάθηκε ένα συνεργατικό περιβάλλον το οποίο πρόκειται να αλλάξει τον τρόπο με τον οποίο γίνεται η διαχείριση της ασφάλειας ΠΣ. Συγκεκριμένα, προτείνεται το συνεργατικό περιβάλλον STORM, το οποίο ενσωματώνει και παρέχει ως υπηρεσία την προτεινόμενη πολυκριτηριακή μεθοδολογία STORM-RM, καθώς επίσης και μια σειρά από συνεργατικές υπηρεσίες με στόχο την ολιστική διαχείριση ασφάλειας ΠΣ. Στόχος του STORM, είναι:

- ✓ η συλλογή της γνώσης η οποία βρίσκεται κατανεμημένη σε όλους τους χρήστες μέσα στους οργανισμούς,
- ✓ η ενεργή συμμετοχή όλων των χρηστών στην διαδικασία εντοπισμού, αξιολόγησης και αντιμετώπισης των κινδύνων που απειλούν την ομαλή λειτουργία του ΠΣ του οργανισμού τους, και
- ✓ η διαρκής παρακολούθηση βέλτιστων πρακτικών και η εκπαίδευση των χρηστών πάνω σε θέματα ασφάλειας και προστασίας της ιδιωτικότητας με στόχο την δημιουργία μια κουλτούρας ασφάλειας μέσα στον οργανισμό.

Μεγάλο πλεονέκτημα του STORM είναι το ότι βασίζεται σε ανοιχτού κώδικα τεχνολογίες με αποτέλεσμα να επιτρέπει την εύκολη επέκταση και προσαρμογή του στις ανάγκες οποιουδήποτε οργανισμού, ενώ ακόμη επιτρέπει την ενσωμάτωση νέων αδυναμιών ή απειλών που τυχόν προκύπτουν.

Επίσης, αξίζει να σημειωθεί ότι παρουσιάστηκαν δύο ξεχωριστές μελέτες περίπτωσης εφαρμογής του συνεργατικού περιβάλλοντος STORM και των υπηρεσιών του, αποδεικνύοντας ότι η ύπαρξη τέτοιου είδους εργαλείων στην διαχείριση ασφάλειας αποτελούν επιτακτική ανάγκη. Μελετήθηκε η χρήση του STORM στην διαχείριση ασφάλειας ΠΣ των λιμένων και των ΜΜΕ, όπου αποδείχθηκε για διαφορετικούς λόγους ότι η χρήση του STORM μπορεί να βοηθήσει κατά πολύ στην αποτελεσματικότερη διαχείριση της ασφάλειας τόσο σε μεγάλης κλίμακας οργανισμούς όσο και σε μικρότερης.

Ως μελλοντικές επεκτάσεις της παρούσας διδακτορικής διατριβής, θα μπορούσαν να αποτελέσουν τα εξής:

- ✓ Η χρήση μιας άλλης πολυκριτηριακής μεθοδολογίας στον αλγόριθμο υπολογισμού της STORM-RM, όπως η MACBETH ή η UTA με στόχο να συγκριθούν και να αξιολογηθούν τα αποτελέσματα.
- ✓ Η αναβάθμιση των βημάτων της πρακτικής ανάλυσης αδυναμιών και ο συνδυασμός των αποτελεσμάτων με την υπάρχουσα κλίμακα αποτίμησης αδυναμιών της STORM-RM.
- ✓ Η αναβάθμιση του εργαλείου STORM και η σύνδεσή του με βάσεις εύρεσης και ενημέρωσης γνωστών ευπαθειών ώστε να αναβαθμίζεται συνεχώς η βάση αδυναμιών του συνεργατικού περιβάλλοντος.
- ✓ Η αναβάθμιση του εργαλείου STORM ώστε να μπορεί να υιοθετήσει τεχνολογίες Υπολογιστικού Νέφους (Cloud Computing) με στόχο την παροχή διασυνοριακών, αδιάλειπτων και οικονομικών υπηρεσιών διαχείρισης ασφάλειας, θα αποτελούσε σημαντική καινοτομία στον χώρο, έχοντας εφαρμογή σε διαφορετικής φύσεως οργανισμούς.

Συμπερασματικά, οι λύσεις της παρούσας διατριβής στοχεύουν στην αποτελεσματικότερη διαχείριση ασφάλειας μέσω της εμπλοκής όλων των χρηστών των οργανισμών, λαμβάνοντας υπόψη την πολυπλοκότητα των σημερινών ΠΣ, τις μειωμένες οικονομικές τους δυνατότητες, τον περιορισμό στη διάθεση ανθρώπινων πόρων, συνδυάζοντας τις υπάρχουσες πολυκριτηριακές μεθοδολογίες ομαδικής λήψης αποφάσεων και τις συνεργατικές τεχνολογίες Web 2.0 και προτείνοντας ένα ολοκληρωμένο εφόδιο ολιστικής διαχείρισης της ασφάλειας ΠΣ.

8 Παραρτήματα

Στο κεφάλαιο αυτό της διατριβής παρατίθενται χρήσιμα παραρτήματα τα οποία περιλαμβάνουν τα ερωτηματολόγια της μεθοδολογίας STORM-RM, τη λίστα με την αντιστοίχιση αγαθών-απειλών-αδυναμιών, τα οποία έχουν ενσωματωθεί στην βάση δεδομένων του STORM, την ταξονομία STORM πάνω στην οποία βασίζεται η η-βιβλιοθήκη, ένα προτεινόμενο πρότυπο χειρόγραφης αποτύπωσης επιχειρησιακών διαδικασιών και τέλος τις προτεινόμενες αναφορές ανάλυσης και διαχείρισης επικινδυνότητας της STORM-RM.

8.1 Παράρτημα Ι: Ερωτηματολόγια μεθοδολογίας

8.1.1 Ερωτηματολόγια αποτίμησης επιπτώσεων

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ
Αξιολογήστε στον ακόλουθο πίνακα την σοβαρότητα των επιπτώσεων σε περίπτωση που αποκαλυφθούν δεδομένα, που διαχειρίζεται το πληροφοριακό σύστημα, σε μη εξουσιοδοτημένα άτομα (παραβίαση της εμπιστευτικότητας).

Κατά την αξιολόγηση θα πρέπει να ληφθούν υπ όψιν οι ακόλουθες περιπτώσεις αποκάλυψης δεδομένων:

- **Εσωτερική αποκάλυψη,** σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού
- **Εξωτερική αποκάλυψη,** σε άτομα εκτός του οργανισμού (π.χ. συνεργάτες, εξωτερικοί χρήστες)

Η αξιολόγηση των επιπτώσεων θα πρέπει να γίνεται λαμβάνοντας υπόψη τη χειρότερη δυνατή περίπτωση σε κλίμακα 1-5.

Μετρική	Αξιολόγηση Επιπτώσεων	Σχόλια / Επεξηγήσεις
Οικονομικές επιπτώσεις Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει σε άμεσες ή έμμεσες οικονομικές ζημίες;		
Νομικές επιπτώσεις Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει σε παραβίαση του νομικού πλαισίου ή ιδιωτικών συμφωνητικών; Π.χ. αποκάλυψη ευαίσθητων		

προσωπικών δεδομένων, βιομηχανικών μυστικών, παρεμπόδιση ανταγωνισμού, παρεμπόδιση της δικαιοσύνης, παραβίαση συμφωνητικών μη αποκάλυψης		
Δημόσια εικόνα / Κοινή γνώμη Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να έχει αρνητική επίπτωση στην δημόσια εικόνα του οργανισμού και να οδηγήσει στην απώλεια της εμπιστοσύνης του κοινού στον οργανισμό; (στο κοινό, πελάτες, προμηθευτές, μετόχους)		
Ασφάλεια προσωπικού και κοινού Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να θέσει σε κίνδυνο την σωματική ακεραιότητα του προσωπικού, των πελατών ή τρίτων με άμεσο ή έμμεσο τρόπο;		
Παρεμπόδιση επιχειρηματικών διαδικασιών του οργανισμού Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών του οργανισμού; Επηρεάζονται άλλες κρίσιμες υποδομές;		
Παρεμπόδιση επιχειρηματικών δραστηριοτήτων άλλων οργανισμών Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών άλλων οργανισμών;		
Επιπτώσεις σε Εθνικό Επίπεδο Η αποκάλυψη πληροφοριών / δεδομένων θα μπορούσε να επηρεάσει		

την άμυνα και την εθνική ασφάλεια της χώρας; Θα μπορούσε να διαταράξει τις Διεθνείς σχέσεις της χώρας; Θα μπορούσε να οδηγήσει στην διαταραχή της δημόσιας τάξης;		

ΑΚΕΡΑΙΟΤΗΤΑ

Αξιολογήστε στον ακόλουθο πίνακα την σοβαρότητα των επιπτώσεων σε περίπτωση απώλειας της ακεραιότητας δεδομένων, που διαχειρίζεται το πληροφοριακό σύστημα.
Κατά την αξιολόγηση θα πρέπει να ληφθούν υπ όψιν οι ακόλουθες περιπτώσεις παραποίησης δεδομένων:

- **Κακόβουλη αλλοίωση δεδομένων**, από άτομα εκτός ή / και εντός του οργανισμού
- **Ακούσια αλλοίωση δεδομένων** από άτομα εκτός ή / και εντός του οργανισμού
- **Ολική απώλεια ακεραιότητας**
- **Μερική απώλεια ακεραιότητας**

Η αξιολόγηση των επιπτώσεων θα πρέπει να γίνεται λαμβάνοντας υπ όψιν τη χειρότερη δυνατή περίπτωση σε κλίμακα 1-5.

Μετρική	Αξιολόγηση Επιπτώσεων	Σχόλια / Επεξηγήσεις
Οικονομικές επιπτώσεις Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει σε άμεσες ή έμμεσες οικονομικές ζημίες;		
Νομικές επιπτώσεις Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει σε παραβίαση του νομικού πλαισίου ή ιδιωτικών συμφωνητικών; Π.χ. παραποίηση ευαίσθητων προσωπικών δεδομένων, βιομηχανικών μυστικών, παρεμπόδιση ανταγωνισμού, παρεμπόδιση της δικαιοσύνης		
Δημόσια εικόνα / Κοινή γνώμη Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να έχει αρνητική επίπτωση στην δημόσια εικόνα του οργανισμού; (στο κοινό, πελάτες, προμηθευτές, μετόχους)		
Ασφάλεια προσωπικού και κοινού Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να θέσει σε κίνδυνο την σωματική ακεραιότητα του προσωπικού, των πελατών ή		

τρίτων;		
Παρεμπόδιση επιχειρηματικών διαδικασιών του οργανισμού Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών του οργανισμού; Επηρεάζονται άλλες κρίσιμες υποδομές;		
Παρεμπόδιση επιχειρηματικών δραστηριοτήτων άλλων οργανισμών Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών άλλων οργανισμών; Υπάρχει αλληλεξάρτηση λειτουργιών και δραστηριοτήτων άλλων οργανισμών;		
Επιπτώσεις σε Εθνικό Επίπεδο Η παραποίηση πληροφοριών / δεδομένων θα μπορούσε να επηρεάσει την άμυνα και την εθνική ασφάλεια της χώρας; Θα μπορούσε να διαταράξει τις Διεθνείς σχέσεις της χώρας; Θα μπορούσε να οδηγήσει στην διαταραχή της δημόσιας τάξης;		

ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Αξιολογήστε στον ακόλουθο πίνακα την σοβαρότητα των επιπτώσεων σε περίπτωση απώλειας της διαθεσιμότητας των αγαθών του πληροφοριακού συστήματος. Η αξιολόγηση των επιπτώσεων θα πρέπει να γίνεται λαμβάνοντας υπ όψιν τη χειρότερη δυνατή περίπτωση σε κλίμακα 1-5.

Μετρική	**Απώλεια διαθεσιμότητας ≤ 3 ώρες**	**Απώλεια διαθεσιμότητας ≤ 24 ώρες**	**Απώλεια διαθεσιμότητας ≤ 1 εβδομάδα**	**Ολική Απώλεια**	**Σχόλια / Επεξηγήσεις**
	Αξιολόγηση επιπτώσεων	**Αξιολόγηση επιπτώσεων**	**Αξιολόγηση επιπτώσεων**	**Αξιολόγηση επιπτώσεων**	
Οικονομικές επιπτώσεις Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να οδηγήσει σε άμεσες ή έμμεσες οικονομικές ζημίες;					
Νομικές επιπτώσεις Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να οδηγήσει σε παραβίαση του νομικού πλαισίου ή ιδιωτικών συμφωνητικών; Π.χ. παρεμπόδιση ανταγωνισμού, παρεμπόδιση της δικαιοσύνης, παραβίαση ιδιωτικών συμφωνητικών,					

Μετρική	Απώλεια διαθεσιμότητας ≤ 3 ώρες	Απώλεια διαθεσιμότητας ≤ 24 ώρες	Απώλεια διαθεσιμότητας ≤ 1 εβδομάδα	Ολική Απώλεια	Σχόλια / Επεξηγήσεις
παραβίαση συμφωνητικών παροχής υπηρεσιών (Service Level Agreements)					
Δημόσια εικόνα / Κοινή γνώμη Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να έχει αρνητική επίπτωση στην δημόσια εικόνα του οργανισμού; (στο κοινό, πελάτες, προμηθευτές, μετόχους)					
Ασφάλεια προσωπικού και κοινού Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να θέσει σε κίνδυνο την σωματική ακεραιότητα του προσωπικού, των πελατών ή τρίτων;					
Παρεμπόδιση επιχειρηματικών διαδικασιών του οργανισμού Η μη διαθεσιμότητα					

Μετρική	Απώλεια διαθεσιμότητας ≤ 3 ώρες	Απώλεια διαθεσιμότητας ≤ 24 ώρες	Απώλεια διαθεσιμότητας ≤ 1 εβδομάδα	Ολική Απώλεια	Σχόλια / Επεξηγήσεις
δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών του οργανισμού;					
Παρεμπόδιση επιχειρηματικών δραστηριοτήτων άλλων οργανισμών Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να οδηγήσει στην παρεμπόδιση των επιχειρηματικών λειτουργιών και διαδικασιών άλλων οργανισμών; Επηρεάζονται άλλες κρίσιμες υποδομές;					
Επιπτώσεις σε Εθνικό Επίπεδο Η μη διαθεσιμότητα δεδομένων ή του πληροφοριακού συστήματος θα μπορούσε να επηρεάσει					

Μετρική	Απώλεια διαθεσιμότητας ≤ 3 ώρες	Απώλεια διαθεσιμότητας ≤ 24 ώρες	Απώλεια διαθεσιμότητας ≤ 1 εβδομάδα	Ολική Απώλεια	Σχόλια / Επεξηγήσεις
την άμυνα και την εθνική ασφάλεια της χώρας; Θα μπορούσε να διαταράξει τις Διεθνείς σχέσεις της χώρας; Θα μπορούσε να οδηγήσει στην διαταραχή της δημόσιας τάξης;					

8.1.2 Ερωτηματολόγια αποτίμησης απειλών

Αξιολογήστε στον ακόλουθο πίνακα (Παράρτημα ΙΙ) την πιθανότητα να συμβεί κάθε μία απειλή που αντιστοιχούν στο συγκεκριμένο αγαθό. Η αξιολόγηση της πιθανότητας εμφάνισης θα πρέπει να γίνεται σε κλίμακα 1-5 (ΠΧ-ΠΥ).

8.1.3 Ερωτηματολόγια αποτίμησης αδυναμιών

Αξιολογήστε στον ακόλουθο πίνακα (Παράρτημα ΙΙ) την πιθανότητα να συμβεί το χειρότερο σενάριο σε περίπτωση που πραγματοποιηθεί η κάθε απειλή. Η αξιολόγηση της πιθανότητας εμφάνισης θα πρέπει να γίνεται σε κλίμακα 1-3 (Χ-Υ).

8.2 Παράρτημα ΙΙ: Πίνακες αντιστοίχισης αγαθών / απειλών / αδυναμιών

Στο συγκεκριμένο παράρτημα παρατίθενται οι πίνακες με αντιστοίχισης απειλών,αδυναμιών,μέτρων ασφάλειας, υπο-πολιτική ασφάλειας ανά κατηγορία αγαθού (σύμφωνα με τις κατηγορίες αγαθών της μεθοδολογίας STORM-RM).

ΔΕΔΟΜΕΝΑ (DATA)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Μη εξουσιοδοτημένη μεταφορά δεδομένων με φορητές συσκευές	Οι χρήστες έχουν δικαιώματα χρήσης εξωτερικών μέσων αποθήκευσης π.χ. cd - usb κτλ.	20	C	I	A	Έχει ληφθεί μέριμνα ώστε οι απλοί χρήστες να μην μπορούν να χρησιμοποιούν εξωτερικά μέσα αποθήκευσης στον υπολογιστή τους, π.χ. usb;	Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση εξωτερικού μέσου αποθήκευσης (π.χ. κάρτα μνήμης - usb κτλ).	8.7.1
	Ελλειπής κρυπτογράφηση φορητών συσκευών	25	C	I	A	Τα ευαίσθητα δεδομένα που βρίσκονται σε φορητές συσκευές είναι κρυπτογραφημένα;	Τα κρισιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	10.3.1
	Ελλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	25	C	I	A	Υπάρχουν μηχανισμοί πρόληψης διαρροής	Θα πρέπει να υπάρχουν μηχανισμοί	10.3.1

ΔΕΔΟΜΕΝΑ (DATA)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						δεδομένων (Data Leak Prevention - DLPs);	πρόληψης διαρροής δεδομένων	
	Έλλειψη διαβάθμισης (classification) των πόρων	40	C	I	A	Υπάρχει μεθοδολογία διαβάθμισης των πόρων του οργανισμού;	Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού	5.2.1
	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	40	C	I	A	Γίνεται κρυπτογράφηση των ευαίσθητων δεδομένων με αναγνωρισμένες μεθόδους κρυπτογράφησης; (π.χ. AES)	Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	10.3.1
Κοινωνική Μηχανική (Social Engineering)	Έλλειψη ενημέρωσης και εκπαίδευσης για την απειλή της κοινωνικής μηχανικής (social engineering)	40	C			Παρέχεται ενημέρωση και εκπαίδευση για την απειλή της κοινωνικής μηχανικής (social engineering)	Θα πρέπει να παρέχεται ενημέρωση και εκπαίδευση για την απειλή της κοινωνικής μηχανικής	6.2.2
	Έλλειψη ειδίκευσης των χρηστών και των διαχειριστών	40	C	I	A	Υπάρχει σχέδιο εκπαίδευσης για τους χρήστες / διαχειριστές;	Θα πρέπει να παρέχεται ενημέρωση και εκπαίδευση για την απειλή της κοινωνικής μηχανικής	6.2.2

ΔΕΔΟΜΕΝΑ (DATA)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη πολιτικής που να καθορίζει τις πληροφορίες που επιτρέπεται να δωθούν δια τηλεφώνου	40	C			Υπάρχει πολιτική που να καθορίζει τις πληροφορίες που επιτρέπεται να δωθούν δια τηλεφώνου	Απουσία πολιτικής και σχετικών οδηγιών οπου καθορίζονται οι πληροφορίες που επιτρέπεται να δωθούν δια τηλεφώνου	8.1.1
Μη νομική συμμόρφωση	Έλλειψη παρακολούθησης πνευματικών δικαιωμάτων και αδειών	20	C	I	A	Παρακολούθουνται τα πνευματικά δικαιωμάτα και οι σχετικές άδειες;	Παρακολούθηση των πνευματικών δικαιωμάτων και αδειών	13.1.2
	Έλλειψη παρακολούθησης ιδιωτικών συμφωνητικών (Service level Agreements SLA's)	20	C	I	A	Παρακολούθείται η συμμόρφωση με τα ιδιωτικά συμφωνητικά; (Service level Agreements SLA's)	Παρακολούθηση συμμόρφωσης με τα ιδιωτικά συμφωνητικά;	13.1.1
	Ανεπαρκής παρακολούθηση και συμμόρφωση με σχετική νομοθεσία (π.χ. ISPS)	20	C	I	A	Παρακολούθούνται οι εξελίξεις στο νομικό πλαίσιο και η συμμόρφωση με τις απαιτήσεις αυτών;	Παρακολούθηση και συμμόρφωση με σχετική νομοθεσία	13.1.1
	Ανεπαρκής προστασία του απορρήτου των επικοινωνιών	20	C	I	A	Λαμβάνονται τα κατάλληλα μέτρα για την προστασία του απορρήτου των επικοινωνιών;	προστασία του απορρήτου των επικοινωνιών	13.1.1
	Διατήρηση αρχείων	20	C	I	A	Τα αρχεία δεδομένων	Διατήρηση αρχείων για όσο	13.1.3

ΔΕΔΟΜΕΝΑ (DATA)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						διατήρούνται για όσο χρονικό διάστημα ορίζει η σχετική νομοδεσία;	χρονικό διάστημα ορίζει η σχετική νομοδεσία	
	Ανεπαρκής Προστασία Προσωπικών Δεδομένων	20	C	I	A	Λαμβάνονται τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων;	Προστασία Προσωπικών Δεδομένων	13.1.4
	Ανεπαρκείς εσωτερικοί έλεγχοι ασφαλείας (internal audits)	20	C	I	A	Πραγματοποιούνται περιοδικοί εσωτερικοί έλεγχοι ασφαλείας (internal audits);	Πραγματοποίηση περιοδικών εσωτερικών έλεγχων ασφαλείας (internal audits)	13.3.1
	Ανεπαρκείς εξωτερικοί έλεγχοι ασφαλείας (external audits)	20	C	I	A	Πραγματοποιούνται περιοδικοί εξωτερικοί έλεγχοι ασφαλείας (external audits)	Πραγματοποίηση περιοδικών εξωτερικών έλεγχων ασφαλείας (external audits)	13.3.1

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Παραβίαση Φυσικής Ασφάλειας Οργανισμού	Έλλειψη σχεδίου ασφάλειας φυσικής εγκατάστασης (ΣΑΦΕ) του οργανισμού	70			A	Υπάρχει σχέδιο ασφάλειας φυσικής εγκατάστασης;	Πρέπει να διατηρείται και να εφαρμόζεται Σχέδιο Ασφάλειας Φυσικής Εγκατάστασης	7.1
	Το ΣΑΦΕ δεν ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό	20			A	Το ΣΑΦΕ ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό;	Το ΣΑΦΕ πρέπει να ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό.	3.2
	Ανεπαρκής διάρθρωση της οργάνωσης ασφάλειας της φυσικής εγκατάστασης	20			A	Η διάρθρωση της οργάνωσης ασφάλειας της φυσικής εγκατάστασης είναι σύμφωνη με τους σχετικούς κανονισμούς;	Η διάρθρωση της οργάνωσης ασφάλειας της φυσικής εγκατάστασης πρέπει να είναι σύμφωνη με τους σχετικούς κανονισμούς	4.1
	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας δεν είναι προσδιορισμένα σύμφωνα με τους σχετικούς κανονισμούς	10			A	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας, είναι προσδιορισμένα σύμφωνα με τους σχετικούς κανονισμούς;	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας, θα πρέπει να είναι καλύπτουν τις απαιτήσεις των σχετικών κανονισμών	4.1.3
Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	50			A	Υπάρχει Σχέδιο Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan);	Πρέπει να διατηρείται Σχέδιο Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan).	12.1.3

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών	20			A	Υπάρχει εφεδρικό υπολογιστικό κέντρο ή σύμβαση με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών;	Θα πρέπει να υπάρχει εφεδρικό υπολογιστικό κέντρο ή σύμβαση με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών.	12.1.3
	Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	10			A	Το Σχέδιο Ανάκαμψης από Καταστροφή περιλαμβάνει όλα τα κρίσιμα πληροφοριακά συστήματα του οργανισμού, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας;	Το Σχέδιο Ανάκαμψης από Καταστροφή πρέπει να περιλαμβάνει όλα τα κρίσιμα πληροφοριακά συστήματα του οργανισμού, όπως αυτά προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας.	12.1.2
	Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	10			A	Το Σχέδιο Ανάκαμψης από Καταστροφή δοκιμάζεται και ανανεώνεται συχνά ώστε να καλύπτει τις πιθανές μεταβολές στις υποδομές του οργανισμού;	Το Σχέδιο Ανάκαμψης από Καταστροφή θα πρέπει να δοκιμάζεται και να ανανεώνεται συχνά, ώστε να καλύπτει τις πιθανές μεταβολές στις υποδομές του οργανισμού.	12.1.5
	Δεν είναι διαθέσιμη σε όλο το προσωπικό λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής	10			A	Είναι διαθέσιμη σε όλο το προσωπικό λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής;	Θα πρέπει να είναι διαθέσιμη σε όλο το προσωπικό λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής.	12.1.3
	Έλλειψη ελέγχου φυσικής πρόσβασης στο εναλλακτικό κέντρο λειτουργίας	10			A	Υπάρχει διαδικασία ελέγχου φυσικής πρόσβασης για το εναλλακτικό κέντρο λειτουργίας;	Η φυσική πρόσβαση στο εναλλακτικό κέντρο λειτουργίας θα πρέπει να ελέγχεται σύμφωνα με καταγεγραμμένη διαδικασία.	7.1.2

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Πυρκαγιά	Ακαταλληλότητα υλικών κατασκευής (π.χ. μη πυράντοχες πόρτες, πάτωμα, ξύλινη επικάλυψη στον τοίχο κλπ.)	20			A	Οι χώροι που φυλοξενούν κρίσιμο εξοπλισμό είναι κατασκευασμένοι με πυράντοχα υλικά;	Οι χώροι που φυλοξενούν κρίσιμο εξοπλισμό θα πρέπει να είναι κατασκευασμένοι με πυράντοχα υλικά.	7.1.4
	Έλλειψη κατάλληλων μέσων πυρόσβεσης	30			A	Υπάρχουν κατάλληλα μέσα πυρόσβεσης;	Θα πρέπει να υπάρχουν εγκατεστημένα κατάλληλα μέσα πυρόσβεσης στις εγκαταστάσεις που φιλοξενούν κρίσιμο εξοπλισμό.	7.1.3
	Έλλειψη κατάλληλων μηχανισμών ανίχνευσης φωτιάς	30			A	Υπάρχουν κατάλληλοι μηχανισμοί ανίχνευσης φωτιάς;	Θα πρέπει να είναι εγκατεστημένος μηχανισμός ανίχνευσης φωτιάς/καπνού, στις εγκαταστάσεις που φιλοξενούν κρίσιμο εξοπλισμό	7.1.3
	Ύπαρξη εύφλεκτων υλικών και ελλιπής καθαριότητα	10			A	Υπάρχει μέριμνα ώστε να μην υπάρχουν εύφλεκτα υλικά σε χώρους όπου φυλάσσεται κρίσιμος εξοπλισμός; Πραγματοποιείται καθαρισμός των χώρων σε τακτά χρονικά διαστήματα;	Δεν επιτρέπεται η αποθήκευση εύφλεκτων υλικών σε χώρους όπου φυλάσσεται κρίσιμος εξοπλισμός. Ο καθαρισμός αυτώντων χώρων θα πρέπει να γίνεται σε τακτά χρονικά διαστήματα.	7.1.3
	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	10			A	Πραγματοποιείται περιοδίκη συντήρηση των πυροσβεστικών μέσων;	Θα πρέπει να πραγματοποιείται περιοδίκη συντήρηση των πυροσβεστικών μέσων.	7.1.3
	Απουσία πλάνου εκκένωσης	50			A	Υπάρχει πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση πυρκαγίας; Υπάρχει κατάλληλη σήμανση;	Θα πρέπει να διατηρείται πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση έκτακτης ανάγκης. Στους χώρους εργασίας θα πρέπει να υπάρχει κατάλληλη σήμανση ενδείξεων	7.1.5

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							εκκένωσης.	
	Ελλειπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	10			A	Το προσωπικό είναι εκπαιδευμένο σε ζητημάτα πυρόσβεσης και πυροπροστασίας;	Θα πρέπει να πραγματοποιείται τακτική εκπαίδευση / ενημέρωση του προσωπικού σε ζητημάτα πυρόσβεσης και πυροπροστασίας.	6.2.2
	Η εγκατάσταση βρίσκεται κοντά σε χώρους με αυξημένο κίνδυνο πυρκαγίας (π.χ. πρατήριο καυσίμων, δασική εκταση κλπ.)	20			A	Έχει εξασφαλιστεί ότι δεν υπάρχουν χώροι πλησίον της εγκατάστασης με αυξημένο κίνδυνο πυρκαγιάς (π.χ. πρατήριο καυσιμών, δασική έκταση κλπ);	Λαμβάνεται υπόψη η ύπαρξη χώρων πλησίον της εγκατάστασης με αυξημένο κίνδυνο πυρκαγιάς (π.χ. πρατήριο καυσιών, δασική έκταση κλπ).	7.1.4
Σεισμός	Ακατάλληλες κτιριακές υποδομές	70			A	Τα κτίρια πληρούν αντισεισμηκές προδιαγραφές;	Οι εγκαταστάσεις θα πρέπει να πληρούν τις αντισεισμηκές προδιαγραφές.	7.1.4
	Απουσία πλάνου εκκένωσης	50			A	Υπάρχει πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση σεισμού; Υπάρχει κατάλληλη σήμανση;	Θα πρέπει να διατηρείται πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση έκτακτης ανάγκης. Στους χώρους εργασίας θα πρέπει να υπάρχει κατάλληλη σήμανση ενδείξεων εκκένωσης.	7.1.5
Πλημμύρα	Απουσία εξοπλισμού ανίχνευσης διεισδυσης νερού / υγρασίας	20			A	Υπάρχει εξοπλισμός ανίχνευσης διεισδυσης νερού / υγρασίας στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα;	Θα πρέπει να είναι εγκατεστημένος εξοπλισμός ανίχνευσης διεισδυσης νερού / υγρασίας, στις εγκαταστάσεις	7.1.3

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							που φιλοξενούν κρίσιμα συστήματα.	
	Κρίσιμος εξοπλισμός τοποθετημένος σε τοποθεσία με πηγές ύδατος (σωληνώσεις κτλ)	50			A	Γίνεται έλεγχος πριν την τοποθέτηση κρίσιμου εξοπλισμού, ώστε να αποφεύγονται σημεία που διατρέχουν σωληνώσεις ύδρευσης / αποχέτευσης	Θα πρέπει να γίνεται έλεγχος πριν την τοποθέτηση κρίσιμου εξοπλισμού, ώστε να αποφεύγονται σημεία που διατρέχουν σωληνώσεις ύδρευσης / αποχέτευσης.	7.1.3
	Κρίσιμος εξοπλισμός δεν είναι καλυμένος με αδιάβροχα καλύματα	10			A	Υπάρχει κρίσιμος εξοπλισμός που δεν είναι καλυμένος με αδιάβροχα καλύματα;	Ο κρίσιμος εξοπλισμός πρέπει να είναι καλυμένος με αδιάβροχα καλύματα.	7.2.1
	Απουσία αντλιών νερού με ανεξάρτητη παροχή ενέργειας	10			A	Υπάρχουν διαθέσιμες αντλίες νερού με ανεξάρτητη παροχή ενέργειας για την αντιμετώπιση πλημμύρας;	Θα πρέπει να υπάρχουν διαθέσιμες αντλίες νερού με ανεξάρτητη παροχή ενέργειας, για περίπτωση πλημμύρας.	7.1.4
Καιρικά φαινόμενα / Ακραίες συνθήκες	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε παλιρροϊκό κύμα	30			A	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε παλιρροϊκό κύμα;	Θα πρέπει να ληφθούν μέτρα προστασίας για την έκθεση της εγκατάστασης σε παλιρροϊκό κύμα.	7.1.4
	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε ακραίες συνθήκες θερμοκρασίας και υγρασίας	30			A	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε συνθήκες θερμοκρασιών και υγρασίας πέραν του συνηθισμένου;	Οι εγκαταστάσεις που φιλοξενούν κρίσιμο εξοπλισμό θα πρέπει να έχουν κατάλληλα μέσα ελέγχου των συνθηκών θερμοκρασίας και υγρασίας.	7.1.4
	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλοντολογικών κινδύνων	20			A	Υπάρχουν πολιτικές και διαδικασίες που αφορούν τον έλεγχο των περιβαλοντολογικών κινδύνων και την αντιμετώπιση	Θα πρέπει να υπάρχουν καταγεγραμμένες διαδικασίες που αφορούν τον έλεγχο των περιβαλοντολογικών κινδύνων	7.1.4

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);					τους;	και την αντιμετώπιση τους.	
	Ανεπαρκής παρακολούθηση των περιβαλλοντολογικών συνθηκών	20			A	Παρακολουθούνται οι περιβαλλοντολογικές συνθήκες (θερμοκρασία, υγρασία κτλ)	Παρακολουθούνται οι περιβαλλοντολογικές συνθήκες (θερμοκρασία, υγρασία κτλ).	7.1.4
	Ελλιπής συντήρηση των εγκαταστάσεων που φιλοξενούν κρίσιμα συστήματα	20			A	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα συντηρούνται σε τακτά διαστήματα;	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα, θα πρέπει να συντηρούνται σε τακτά διαστήματα.	7.1.3
Ανεπάρκεια Κλιματισμού	Ακαταλληλότητα κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα	70			A	Έχει τοποθετηθεί κλιματισμός με βάση τις προδιαγραφές λειτουργίας, στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα;	Η τοποθέτηση του κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα, πρέπει να πληρεί τις προδιαγραφές ασφαλούς λειτουργίας.	7.2.2
	Παλαιότητα κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα	20			A	Ο κλιματισμός στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα, λειτουργεί σύμφωνα με τις προδιαγραφές του κατασκευαστή; (π.χ. ο εξοπλισμός δεν έχει υπερβεί τον χρόνο ζωής λειτουργίας όπως αυτός καθορίζεται από τον κατασκευαστή)	Ο κλιματισμός στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα δεν θα πρέπει να είναι παλαιωμένος.	7.2.2
	Ελλιπής συντήρηση κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα	40			A	Συντηρείται τακτικά ο κλιματισμός;	Θα πρέπει να γίνεται τακτική συντήρηση των συστημάτων κλιματισμού στις εγκαταστάσεις που φιλοξενούν	7.2.2

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							κρίσιμα συστήματα.	
Διακυμάνσεις ηλεκτρικής ισχύος / Διακοπή ηλεκτροδότησης	Απουσία εξοπλισμού Αδιάληπτης Παροχής Τροφοδοσίας Ηλεκτρικού Ρεύματος (UPS)	40			A	Υπάρχει εξοπλισμός Αδιάληπτης Παροχής Τροφοδοσίας Ηλεκτρικού Ρεύματος (UPS) στις εγκαταστάσεις που βρίσκονται κρίσιμα συστήματα;	Θα πρέπει να υπάρχει εξοπλισμός Αδιάληπτης Παροχής Τροφοδοσίας Ηλεκτρικού Ρεύματος (UPS) στις εγκαταστάσεις που βρίσκονται κρίσιμα συστήματα.	7.2.2
	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	20			A	Υπάρχουν ηλεκτρογεννήτριες ή αλλα μεσα παροχής ηλεκτρικής ενέργειας στις εγκαταστάσεις που βρίσκονται κρίσιμα συστήματα;	Θα πρέπει να υπάρχουν ηλεκτρογεννήτριες ή αλλα μεσα παροχής ηλεκτρικής ενέργειας στις εγκαταστάσεις που βρίσκονται κρίσιμα συστήματα.	7.2.2
	Έλλειψη προστασίας των κτιρίων από αστραπές	20			A	Υπάρχουν αλεξικέραυνα στα κτίρια ή αλλα μέτρα προστασίας από τους κεραυνούς;	Θα πρέπει να υπάρχουν εγκατεστημένα αλεξικέραυνα στα κτίρια ή αλλα μέτρα προστασίας από τους κεραυνούς.	7.2.2
	Οι εξωτερικές γραμμές παροχής είναι εκτεθειμένες σε φυσικές καταστροφές ή σε τρίτους	20			A	Οι εξωτερικές γραμμές παροχής προστατεύονται επαρκώς (από φυσικές καταστροφές, ατυχήματα ή δολιοφθορά);	Οι εξωτερικές γραμμές παροχής ρεύματος θα πρέπει να προστατεύονται επαρκώς (από φυσικές καταστροφές, ατυχήματα ή δολιοφθορά).	7.2.2

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Δολιοφθορά (Sabotage)	Έλλειψη πολιτικών και διαδικασιών (φυσικής) διαχείρισης πρόσβασης	10	C		A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμα συστήματα;	Θα πρέπει να υπάρχουν καταγεγραμμένες πολιτικές και διαδικασίες για την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμες υποδομές πληροφοριακών συστημάτων.	7.1.2
	Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	10	C		A	Οι κτιριακές υποδομές παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack);	Οι κτιριακές υποδομές θα πρέπει να παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack).	7.1.1
	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση	10	C		A	Στους χώρους που φιλοξενούνται κρίσιμα συστήματα, είναι οι πόρτες ανθεκτικές σε επίθεση / έχουν θωράκιση;	Θα πρέπει στους χώρους που φιλοξενούνται κρίσιμα συστήματα, οι πόρτες είναι ανθεκτικές σε επίθεση.	7.1.1
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	20	C		A	Υπάρχουν διαδικασίες ή/και μηχανισμοί παρακολούθησης της πρόσβασης, στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμα συστήματα;	Θα πρέπει να υπάρχουν διαδικασίες ή/και μηχανισμοί παρακολούθησης της πρόσβασης, στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμα συστήματα.	7.1.1
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές	10	C		A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές;	Θα πρέπει να έχει καθοριστεί περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμα συστήματα.	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10	C		A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας θα πρέπει να φωτίζεται επαρκώς.	7.1.1

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Στους χώρους όπου υπάρχει κρίσιμος εξοπλισμος επιτρέπεται η πρόσβαση στο κοινό	20	C		A	Υπάρχουν χώροι με κρίσιμο εξοπλισμό στους οποίους επιτρέπεται η πρόσβαση στο κοινό;	Θα πρέπει να απαγορεύεται η πρόσβαση στο κοινό, σε χώρους με κρίσιμο εξοπλισμό.	7.1.6
	Τοποθεσίες στάθμευσης αυτοκινήτων βρίσκονται εντός της περιμέτρου ασφαλείας	10	C		A	Υπάρχουν τοποθεσίες στάθμευσης αυτοκινήτων εντός της περιμέτρου ασφαλείας;	Πρέπει να ελέγχεται η στάθμευση των αυτοκινήτων εντός της περιμέτρου ασφαλείας.	7.1.6
	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με κρίσιμες υποδομές πληροφοριακών συστημάτων	10	C		A	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με κρίσιμες υποδομές πληροφοριακών συστημάτων;	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με κρίσιμες υποδομές πληροφοριακών συστημάτων;	7.1.6
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	10	C		A	Υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στις τεχνικές και κτιριακές υποδομές;	Θα πρέπει να υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στις τεχνικές και κτιριακές υποδομές.	7.1.3
	Είσερχόμενα υλικά/εξοπλισμός δεν εξετάζονται για πιθανούς κινδύνους πρωτού μεταφερθούν στον τελικό τους προορισμό	20			A	Πραγματοποιείται εξέταση των υλικών/εξοπλισμού με τεχνικά μέσα για πιθανούς κινδύνους, πριν μεταφερθούν στον τελικό τους προορισμό;	Θα πρέπει να πραγματοποιείται εξέταση των υλικών/εξοπλισμού με τεχνικά μέσα για πιθανούς κινδύνους, πριν μεταφερθούν στον τελικό τους προορισμό	7.1.6
	Η παραλαβή αγαθών θα πρέπει να πραγματοποιείται σε περιοχή εκτός της περιμέτρου ασφαλείας	10			A	Η παραλαβή αγαθών πραγματοποιείται σε περιοχή εκτός της περιμέτρου ασφαλείας;	Η παραλαβή αγαθών θα πρέπει να αποφεύγεται σε περιοχή εντός της περιμέτρου ασφαλείας	7.1.6

ΦΥΣΙΚΑ ΑΓΑΘΑ (PHYSICAL ASSETS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Μη εξουσιοδοτημένη διακίνηση εμπορευμάτων	Έλλειψη σχεδίου ασφάλειας φυσικής εγκατάστασης του οργανισμού (ΣΑΦΕ)	70			A	Υπάρχει σχέδιο ασφάλειας φυσικής εγκατάστασης του οργανισμού (ΣΑΦΕ);	Πρέπει να διατηρείται και να εφαρμόζεται Σχέδιο Ασφάλειας φυσικής εγκατάστασης του οργανισμού (ΣΑΦΕ)	7.1
	Το ΣΑΦΕ δεν ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό	20			A	Το ΣΑΦΕ ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό;	Το Σχέδιο Ασφάλειας Φυσικής Εγκατάστασης πρέπει να ενημερώνεται/τροποποιείται σύμφωνα με τις μεταβολλές που συμβαίνουν στον οργανισμό.	3.2
	Ανεπαρκής διάρθρωση της οργάνωσης ασφάλειας της φυσικής εγκατάστασης του οργανισμού	20			A	Η διάρθρωση της οργάνωσης ασφάλειας του οργανισμού είναι είναι σύμφωνη με τους σχετικούς κανονισμούς ;	Η διάρθρωση της οργάνωσης ασφάλειας της φυσικής εγκατάστασης του οργανισμού πρέπει να είναι σύμφωνη με τους σχετικούς κανονισμούς	4.1
	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας δεν είναι προσδιορισμένα σύμφωνα με τους σχετικούς κανονισμούς	10			A	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας, είναι προσδιορισμένα σύμφωνα με τους σχετικούς κανονισμούς;	Τα καθήκοντα, οι ευθύνες και οι απαιτήσεις εκπαίδευσης για το προσωπικό του οργανισμού που συμμετέχει σε ζητήματα ασφάλειας, θα πρέπει να είναι καλύπτουν τις απαιτήσεις των σχετικών κανονισμών	4.1.3

HW – ΕΞΥΠΗΡΕΤΗΤΕΣ (SERVERS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	20		I	A	Ο εξοπλισμός (εξυπηρετητές) έχει λιγότερο απο 5 έτη λειτουργίας;	Η ηλικία των εξυπηρετητών θα πρέπει να είναι μικρότερη από 5 έτη.	7.2.4
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	20		I	A	Τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση των εξυπηρετητών;	Πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση των εξυπηρετητών.	7.2.4
	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	10		I	A	Έχει ληφθεί μέριμνα ώστε ο εξυπηρετητής να μην χρησιμοποιείται κατά το μέγιστο των δυνατοτήτων του (από απόψη χωρητικότητας, φόρτου εργασίας κλπ.);	Θα πρέπει να αποφεύγεται η χρήση του εξυπηρετητή στο μέγιστο των δυνατοτήτων του, από απόψη χωρητικότητας, φόρτου κλπ.	8.3.1
	Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	10	C	I	A	Υπάρχουν διαδικασίες εποπτείας της λειτουργίας των εξυπηρετητών;	Θα πρέπει να υπάρχουν διαδικασίες εποπτείας της λειτουργίας των εξυπηρετητών.	7.2.4
	Δεν εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές	10		I	A	Εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές;	Πρέπει να εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές.	7.1.5
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης των εξυπηρετητών	30			A	Υπάρχει συμβόλαιο συντήρησης για το συγκεκριμένο εξοπλισμό; Είναι εντός εγγυήσης;	Πρέπει να υπάρχει συμβόλαιο συντήρησης για τον συγκεκριμένο εξοπλισμό και να ελέγχεται εάν είναι εντός εγγύησης.	7.2.4
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	20			A	Υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών;	Πρέπει να υπάρχουν διαθέσιμοι πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών στους εξυπηρετητές.	7.2.4

HW – ΕΞΥΠΗΡΕΤΗΤΕΣ (SERVERS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Ελλιπής συντήρηση των εξυπηρετητών	20		I	A	Οι εξυπηρετητές συντηρούνται σε τακτά διαστήματα;	Οι εξυπηρετητές θα πρέπει να συντηρούνται ανά τακτά χρονικά διαστήματα.	7.2.4
Σφάλμα χειρισμού και διαχείρησης	Ανεπαρκής επαγγελματική εμπειρία - εξειδίκευση των διαχειριστών	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη εκπαίδευσης των διαχειριστών	20	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Έλλειψη αξιολόγησης διαχειριστών	10	C	I	A	Υπάρχει διαδικασία τακτικής αξιολόγησης των διαχειριστών;	Πρέπει να υπάρχει πρόγραμμα αξιολόγησης των διαχειριστών.	6.2.3
	Απουσία ετικετών στους εξυπηρετητές	10	C	I	A	Γίνεται χρήση ετικετών στους εξυπηρετητές;	Πρέπει να χρησιμοποιούνται ετικέτες ταυτοποίησης στους εξυπηρετητές.	7.2.3
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών	20	C	I	A	Υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών ;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών.	8.1.1
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στους εξυπηρετητές	10	C		A	Διατηρούνται αρχεία με τις μετατροπές και επισκευές στους εξυπηρετητές;	Πρέπει να διατηρούνται αρχεία με τις μετατροπές και επισκευές στους εξυπηρετητές.	10.5.1
	Εργασία υπό πίεση	10	C	I	A	Έχει ληφθεί μέριμνα ώστε να αποφεύγεται η εργασία των διαχειριστών υπό συνθήκες πίεσης;	Θα πρέπει να αποφεύγεται να εργάζονται οι διαχειριστές υπό συνθήκες πίεσης, οι οποίες αυξάνουν την πιθανότητα λαθών.	6.1.1
	Απουσία μηχανισμών ελέγχου	20	C	I	A	Υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπιστούν τυχόν λάθη χειρισμού;	Πρέπει να υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπίζονται τυχόν λάθη χειρισμού.	7.2.8

HW – ΕΞΥΠΗΡΕΤΗΤΕΣ (SERVERS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	50			A	Για τους εξυπηρετητές που χρησιμοποιούνται για κρίσιμες υπηρεσίες, υπάρχει πλεονάζον ή εφεδρικός εξυπηρετητής;	Για τους εξυπηρετητές που χρησιμοποιούνται για κρίσιμες υπηρεσίες, θα πρέπει να υπάρχει πλεονάζον ή εφεδρικός εξυπηρετητής.	12.1.4
	Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	50			A	Αποφεύγεται η χρήση του εξυπηρετητή για πολλές υπηρεσίες (ώστε να αποφεύγεται η υπερφόρτωση);	Θα πρέπει να αποφεύγεται να χρησιμοποιείται ο εξυπηρετητής για την λειτουργία πολλών υπηρεσιών.	10.1.1
	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	20			A	Χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποίηση και χρήση των εξυπηρετητών;	Πρέπει να χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποίηση και χρήση των εξυπηρετητών.	13.2.1
Κλοπή	Ο εξυπηρετητής δεν βρίσκεται εντός υπολογιστικού κέντρου (data center) με ελεγχόμενη πρόσβαση	35			A	Ο εξυπηρετητής βρίσκεται εντός υπολογιστικού κέντρου με ελεγχόμενη πρόσβαση;	Η πρόσβαση στους χώρους που βρίσκονται οι εξυπηρετητές, θα πρέπει να ελέγχεται.	7.1.7
	Στους χώρους όπου φιλοξενούνται εξυπηρετητές επιτρέπεται η πρόσβαση στο κοινό	35			A	Στους χώρους όπου φιλοξενούνται εξυπηρετητές εφαρμόζεται απαγόρευση πρόσβασης στο κοινό;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού στους χώρους που βρίσκονται εξυπηρετητές και κρίσιμος εξοπλισμός.	7.1.6
	Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης στο χώρο που φιλοξενείται ο εξυπηρετητής	20			A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις που φιλοξενούνται εξυπηρετητές;	Πρέπει να υπαρχουν πολιτικές και διαδικασίες για την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις που βρίσκονται οι εξυπηρετητές.	7.1.2

HW – ΕΞΥΠΗΡΕΤΗΤΕΣ (SERVERS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	10			A	Οι κτιριακές υποδομές παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack);	Οι κτιριακές υποδομές θα πρέπει να παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack).	7.1.1
	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση	10			A	Στους χώρους που φιλοξενούνται οι εξυπηρετητές, είναι οι πόρτες ανθεκτικές σε επίθεση / έχουν θωράκιση;	Θα πρέπει στους χώρους που φιλοξενούνται κρίσιμα συστήματα, οι πόρτες να είναι ανθεκτικές σε επίθεση.	7.1.1
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	20			A	Υπάρχουν μέσα για την επαρκή παρακολούθηση (monitoring) των εγκαταστάσεων που φιλοξενούνται εξυπηρετητές;	Πρέπει να χρησιμοποιούνται κατάλληλα μέσα παρακολούθησης (monitoring) της πρόσβασης στις εγκαταστάσεις που φιλοξενούνται εξυπηρετητές.	7.1.1
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	10			A	Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενούνται εξυπηρετητές;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενούνται εξυπηρετητές.	7.1.4
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές	20			A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές χώροι όπου φιλοξενούνται εξυπηρετητές;	Πρέπει να υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές χώροι όπου φιλοξενούνται εξυπηρετητές.	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10			A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας να φωτίζεται επαρκώς.	7.1.1
	Τοποθεσίες στάθμευσης αυτοκινήτων βρίσκονται εντός της περιμέτρου ασφαλείας	10			A	Έχει ληφθεί μέριμνα ώστε να μην υπάρχουν τοποθεσίες στάθμευσης αυτοκινήτων εντός της περιμέτρου ασφαλείας;	Πρέπει να ελέγχεται η στάθμευση των αυτοκινήτων εντός της περιμέτρου ασφαλείας.	7.1.6

HW – ΕΞΥΠΗΡΕΤΗΤΕΣ (SERVERS)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενούνται εξυπηρετητές	10			A	Έχει ληφθεί μέριμνα ώστε οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών να μην βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενούνται εξυπηρετητές;	Πρέπει να ελέγχεται η διαδικασία φόρτωσης/εκφόρτωσης αγαθών σε χώρους όπου φιλοξενούνται εξυπηρετητές.	7.1.6
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	20			A	Υπάρχει σχέδιο βάσει του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας.	6.2.2

HW - ΣΤΑΘΜΟΣ ΕΡΓΑΣΙΑΣ (CLIENT COMPUTER)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού	20		I	A	Η ηλικία του εξοπλισμού είναι εντός των προδιαγραφών χρήσης (π.χ. μέχρι 5 έτη λειτουργίας);	Η ηλικία των σταθμών εργασίας, συνίσταται να είναι μικρότερη από 5 έτη.	7.2.4
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	20		I	A	Τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση του εξοπλισμού;	Πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση των σταθμών εργασίας.	7.2.4
	Λειτουργία εξοπλισμού σε ακραίες συνθήκες φόρτου	20		I	A	Έχει ληφθεί μέριμνα ώστε ο εξοπλισμός να μην χρησιμοποιείται κατά το μέγιστο των δυνατοτήτων του (από απόψη χωρητικότητας, φόρτου κλπ.);	Θα πρέπει να αποφεύγεται η χρήση των σταθμών εργασίας στο μέγιστο των δυνατοτήτων τους από απόψη χωρητικότητας, φόρτου κλπ.	8.3.1
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης;	20			A	Υπάρχει συμβόλαιο συντήρησης για το συγκεκριμένο εξοπλισμό; Είναι εντός εγγυήσης;	Πρέπει να υπάρχει συμβόλαιο συντήρησης για τους σταθμούς εργασίας και να ελέγχεται εαν είναι εντός εγγύησης.	7.2.4
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	10			A	Υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών;	Πρέπει να υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών.	7.2.4
	Ελλιπής συντήρηση του εξοπλισμού	20		I	A	Ο εξοπλισμός συντηρείται σε τακτά διαστήματα;	Οι εξυπηρετητές θα πρέπει να συντηρούνται ανά τακτά χρονικά διαστήματα.	7.2.4
Σφάλμα χειρισμού	Ανεπαρκής επαγγελματική εμπειρία - εξειδίκευση των χρηστών	20	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των χρηστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των χρηστών.	6.1.2
	Έλλειψη εκπαίδευσης των χρηστων	20	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους χρήστες;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους χρήστες	6.2.2

HW - ΣΤΑΘΜΟΣ ΕΡΓΑΣΙΑΣ (CLIENT COMPUTER)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη αξιολόγησης χρηστών	10	C	I	A	Υπάρχει πρόγραμμα αξιολόγησης των χρηστών;	Πρέπει να υπάρχει πρόγραμμα αξιολόγησης των χρηστών	6.2.3
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης του εξοπλισμού	10	C	I	A	Υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης του εξοπλισμού;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης του εξοπλισμού	8.1.1
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στους σταθμούς εργασίας	20	C		A	Διατηρούνται αρχεία με τις μετατροπές και επισκευές στους σταθμούς εργασίας;	Πρέπει να διατηρούνται αρχεία με τις μετατροπές και επισκευές στους σταθμούς εργασίας	10.5.1
	Εργασία υπό πίεση	10	C	I	A	Έχει ληφθεί μέριμνα ώστε το προσωπικό να μην χρειάζεται να εργάζεται υπό συνθήκες πίεσης οι οποίες αυξάνουν την πιθανότητα λαθών;	Θα πρέπει να αποφεύγεται να εργάζεται το προσωπικό υπό συνθήκες πίεσης οι οποίες αυξάνουν την πιθανότητα λαθών	6.1.1
	Απουσία μηχανισμών ελέγχου	10	C	I	A	Υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπιστούν τυχόν λάθη χειρισμού;	Πρέπει να υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπίζονται τυχόν λάθη χειρισμού	7.2.8
Κλοπή	Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης στο χώρο που φιλοξενείται ο εξυπηρετητής	20			A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται σταθμοί εργασίας;	Πρέπει να γίνεται έλεγχος της πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται σταθμοί εργασίας	7.1.2
	Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	10			A	Οι κτιριακές υποδομές παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack);	Οι κτιριακές υποδομές θα πρέπει να παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	7.1.1

HW - ΣΤΑΘΜΟΣ ΕΡΓΑΣΙΑΣ (CLIENT COMPUTER)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση	10			A	Στους χώρους που φιλοξενούνται κρίσιμα συστήματα, είναι οι πόρτες ανθεκτικές σε επίθεση / έχουν θωράκιση;	Θα πρέπει στους χώρους που φιλοξενούνται κρίσιμα συστήματα, οι πόρτες να είναι ανθεκτικές σε επίθεση.	7.1.1
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	10			A	Υπάρχουν μέσα για την επαρκή παρακολούθηση (monitoring) των εγκαταστάσεων που φιλοξενούνται σταθμοί εργασίας;	Πρέπει να χρησιμοποιούνται κατάλληλα μέσα παρακολούθησης (monitoring) της πρόσβασης στις εγκαταστάσεις που φιλοξενούνται σταθμοί εργασίας.	7.1.1
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	20			A	Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού όπου φιλοξενούνται σταθμοί εργασίας;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού όπου φιλοξενούνται σταθμοί εργασίας.	7.1.2
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές	10			A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές όπου φιλοξενούνται σταθμοί εργασίας;	Πρέπει να υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές χώροι όπου φιλοξενούνται σταθμοί εργασίας.	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10			A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας πρέπει να φωτίζεται επαρκώς.	7.1.1
	Στους χώρους όπου φιλοξενούνται σταθμοί εργασίας επιτρέπεται η πρόσβαση στο κοινό	10			A	Έχει ληφθεί μέριμνα ώστε το κοινό να μην έχει πρόσβαση σε χώρους πλησίον των εγκαταστάσεων οι οποίες φιλοξενούν σταθμούς εργασίας ;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού στους χώρους όπου φιλοξενούνται σταθμοί εργασίας	7.1.6
	Τοποθεσίες στάθμευσης αυτοκινήτων βρίσκονται εντός της περιμέτρου ασφαλείας	10			A	Έχει ληφθεί μέριμνα ώστε να μην υπάρχουν τοποθεσίες στάθμευσης αυτοκινήτων εντός της περιμέτρου ασφαλείας;	Πρέπει να ελέγχεται η στάθμευση των αυτοκινήτων εντός της περιμέτρου ασφαλείας.	7.1.6

HW - ΣΤΑΘΜΟΣ ΕΡΓΑΣΙΑΣ (CLIENT COMPUTER)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενούνται σταθμοί εργασίας	10			A	Έχει ληφθεί μέριμνα ώστε οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών να μην βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενούνται σταθμοί εργασίας;	Πρέπει να ελέγχεται η διαδικασία φόρτωσης/εκφόρτωσης αγαθών σε χώρους όπου φιλοξενούνται σταθμοί εργασίας	7.1.6
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	20			A	Υπάρχει σχέδιο βάσει του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας	6.2.2

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού	10		I	A	Η ηλικία του εξοπλισμού είναι εντός των προδιαγραφών χρήσης (π.χ. μέχρι 5 έτη λειτουργίας);	Η ηλικία του δικτυακού εξοπλισμού συνίσταται να είναι μικρότερη από 5 έτη.	7.2.4
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	10		I	A	Τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση του εξοπλισμού;	Πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση του δικτυακού εξοπλισμού.	7.2.4
	Λειτουργία δικτυακού εξοπλισμού σε ακραίες συνθήκες φόρτου	10		I	A	Έχει ληφθεί μέριμνα ώστε ο εξοπλισμός να μην χρησιμοποιείται κατά το μέγιστο των δυνατοτήτων του (από απόψη χωρητικότητας, φόρτου κλπ.);	Θα πρέπει να αποφεύγεται η χρήση του δικτυακού εξοπλισμού στο μέγιστο των δυνατοτήτων του από απόψη χωρητικότητας, φόρτου κλπ.	8.3.1
	Υπερφόρτωση δικτύου	10			A	Ο σχεδιασμός του δικτύου λαμβάνει υπ όψην του τις ανάγκες για χωρητικότητα και κάλυψης για τις ανάγκες του οργανισμού;	Κατά το σχεδιασμό του δικτύου πρέπει να λαμβάνονται υπόψη οι ανάγκες εύρους ζώνης (bandwidth) του οργανισμού.	10.1.1
	Ανεπαρκής εποπτεία της λειτουργίας του εξοπλισμού και του δικτύου	10	C	I	A	Υπάρχουν διαδικασίες εποπτείας και διαχείρισης του εξοπλισμού και του δικτύου;	Πρέπει να υπάρχουν διαδικασίες εποπτείας και διαχείρισης του εξοπλισμού δικτύου.	7.2.4
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης	30			A	Υπάρχει συμβόλαιο συντήρησης για τον δικτυακό εξοπλισμό; Είναι εντός εγγυήσης;	Πρέπει να υπάρχει συμβόλαιο συντήρησης για τον δικτυακό εξοπλισμό και να ελέγχεται εαν είναι εντός εγγύησης.	7.2.4

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	30			A	Υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών;	Πρέπει να υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών του δικτυακού εξπολισμού.	7.2.4
	Ελλιπής συντήρηση του δικτυακού εξοπλισμού	30		I	A	Ο δικτυακός εξοπλισμός συντηρείται σε τακτά διαστήματα;	Ο δικτυακός εξοπλισμός πρέπει να συντηρείται ανά τακτά χρονικά διαστήματα.	7.2.4
Σφάλμα χειρισμού και συντήρησης	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών	20	C	I	A	Έχουν οι διαχειριστές δικτύου επαρκή εμπειρία και τεχνογνωσία;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών δικτύου.	6.1.2
	Έλλειψη εκπαίδευσης των διαχειριστών	20	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	10	C	I	A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα ασφαλείας.	6.2.2
	Έλλειψη αξιολόγησης χρηστών / διαχειριστών	10	C	I	A	Υπάρχει πρόγραμμα αξιολόγησης των χρηστών / διαχειριστών;	Πρέπει να υπάρχει πρόγραμμα αξιολόγησης των διαχειριστών.	6.2.3
	Απουσία ετικετών στον δικτυακό εξοπλισμό	10	C	I	A	Γίνεται χρήση ετικετών στον δικτυακό εξοπλισμό;	Πρέπει να γίνεται χρήση ετικετών στον δικτυακό εξοπλισμό.	7.2.3
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης του εξοπλισμού	20	C	I	A	Υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης του δικτυακου εξοπλισμού	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης του δικτυακού εξοπλισμού.	8.1.1

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στον δικτυακό εξοπλισμό	20	C		A	Διατηρούνται αρχεία με τις μετατροπές και επισκευές στον εξοπλισμό;	Πρέπει να διατηρούνται αρχεία με τις μετατροπές και επισκευές στον δικτυακό εξοπλισμό.	10.5.1
	Εργασία υπό πίεση	10	C	I	A	Εργάζεται το προσωπικό υπό συνθήκες πίεσης οι οποίες αυξάνουν την πιθανότητα λαθών;	Θα πρέπει να αποφεύγεται να εργάζεται το προσωπικό υπό συνθήκες πίεσης οι οποίες αυξάνουν την πιθανότητα λαθών	6.1.1
	Απουσία μηχανισμών ελέγχου	20	C	I	A	Υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπιστούν τυχόν λάθη χειρισμού;	Πρέπει να υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπίζονται τυχόν λάθη χειρισμού	7.2.8
Άρνηση Υπηρεσίας (Denial of Service)	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	50			A	Υπάρχει πλεονάζον ή εφεδρικός εξοπλισμός (redundant equipment);	Για τον κρίσιμο δικτυακό εξοπλισμό, θα πρέπει να υπάρχει πλεονάζον ή εφεδρικός εξοπλισμός (redundant equipment).	12.1.4
	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	50			A	Χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποιήση και χρήση του δικτυακού εξοπλισμού;	Πρέπει να χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποιήση και χρήση του δικτυακού εξοπλισμού.	13.2.1
Ηλεκτρονικές Παρεμβολές	Η περιοχή είναι ευάλωτη σε ηλεκτρονικές παρεμβολές	50			A	Έχει ληφθεί μέριμνα ώστε η περιοχή οπου φιλοξενούνται δικτυακές υποδομές να μην είναι ευάλωτη σε ηλεκτρονικές παρεμβολές;	Η περιοχή οπου φιλοξενούνται δικτυακές υποδομές δεν πρέπει να είναι ευάλωτη σε ηλεκτρονικές παρεμβολές	7.2.3
	Έλλειψη προστασίας/θωράκισης των δικτυακών υποδομών από Η/Μ παρεμβολές	30		I	A	Ο εξοπλισμός προστατεύεται ενάντια στις Η/Μ παρεμβολές;	Ο εξοπλισμός πρέπει να προστατεύεται ενάντια στις Η/Μ παρεμβολές	7.1.4

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Παρακολούθηση επικοινωνιών	Στους χώρους όπου βρίσκεται ο δικτυακός εξοπλισμός επιτρέπεται η πρόσβαση στο κοινό	30	C			Έχει ληφθεί μέριμνα ώστε να μην υπάρχουν χώροι με δικτυακό εξοπλισμό στους οποίους επιτρέπεται η πρόσβαση στο κοινό;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού στους χώρους με κρίσιμο δικτυακό εξοπλισμό.	7.1.6
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές δικτύου.	30	C			Υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στο δικτυακό εξοπλισμό;	Πρέπει να υπάρχουν διαδικασίες για την πραγματοποίηση αλλαγών και μετατροπών στο δικτυακό εξοπλισμό.	7.2.4
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	20	C			Υπάρχουν μέσα για την επαρκή παρακολούθηση (monitoring) των εγκαταστάσεων που φιλοξενούνται εξυπηρετητές;	Πρέπει να χρησιμοποιούνται κατάλληλα μέσα παρακολούθησης (monitoring) της πρόσβασης στις εγκαταστάσεις που βρίσκεται δικτυακός εξοπλισμός.	7.1.1
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	20	C			Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας.	6.2.2
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	10			A	Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενείται δικτυακός εξοπλισμός;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενείται δικτυακός εξοπλισμός.	7.1.2
Κλοπή	Έλλειψη πολιτικών και διαδικασιών διαχείρισης φυσικής πρόσβασης	20			A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις όπου	Πρέπει να γίνεται έλεγχος της πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενείται ο δικτυακός εξοπλισμός.	7.1.2

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						φιλοξενείται ο δικτυακός εξοπλισμός;		
	Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	10			A	Οι κτιριακές υποδομές παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack);	Οι κτιριακές υποδομές θα πρέπει να παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack).	7.1.1
	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση	10			A	Στους χώρους που φιλοξενούνται κρίσιμα συστήματα, είναι οι πόρτες ανθεκτικές σε επίθεση / έχουν θωράκιση;	Θα πρέπει στους χώρους που φιλοξενούνται κρίσιμα συστήματα, οι πόρτες είναι ανθεκτικές σε επίθεση.	7.1.1
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	10			A	Οι εγκαταστάσεις όπου φιλοξενείται δικτυακός εξοπλισμός παρακολουθείται;	Πρέπει να ελέγχεται η φυσική πρόσβαση στις εγκαταστάσεις οπου φιλοξενείται δικτυακός εξοπλισμός.	7.1.1
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	10			A	Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενείται δικτυακός εξοπλισμός;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενείται δικτυακός εξοπλισμός.	7.1.2
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές	20			A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές χώροι όπου φιλοξενείται δικτυακός εξοπλισμός ;	Πρέπει να υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές χώροι όπου φιλοξενείται δικτυακός εξοπλισμός	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10			A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας πρέπει να φωτίζεται επαρκώς	7.1.1

HW- ΔΙΚΤΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ (NETWORK EQUIPMENT)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Στους χώρους όπου φιλοξενείται ο δικτυακός εξοπλισμός επιτρέπεται η πρόσβαση στο κοινό	20			A	Έχει ληφθεί μέριμνα ώστε να μην έχει πρόσβαση το κοινό σε χώρους πλησίον των εγκαταστάσεων όπου φιλοξενείται ο δικτυακός εξοπλισμός;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού στους χώρους όπου φιλοξενείται ο δικτυακός εξοπλισμός.	7.1.6
	Οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενείται δικτυακός εξοπλισμός	10			A	Έχει ληφθεί μέριμνα ώστε οι τοποθεσίες φόρτωσης/εκφόρτωσης αγαθών να μην βρίσκονται στην ίδια τοποθεσία με χώρους όπου φιλοξενείται ο δικτυακός εξοπλισμός;	Πρέπει να ελέγχεται η διαδικασία φόρτωσης/εκφόρτωσης αγαθών σε χώρους όπου φιλοξενείται ο δικτυακός εξοπλισμός	7.1.6
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	20			A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας	6.2.2

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων υποδομών καλωδίωσης	20		I	A	Οι υποδομές καλωδίωσης είναι εντός των προδιαγραφών λειτουργίας (π.χ. δεν έχουν ξεπεράσει τα 10 έτη λειτουργίας)	Η ηλικία των υποδομών καλωδίωσης θα πρέπει να είναι μικρότερη από 10 έτη.	7.2.4
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	20		I	A	Τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρησης της καλωδίωσης;	Πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή, κατά την εγκατάσταση, λειτουργία και συντήρηση της καλωδίωσης.	7.2.4
	Ανεπαρκής εποπτεία της λειτουργίας των υποδομών καλωδίωσης	20		I	A	Υπάρχουν διαδικασίες εποπτείας και διαχείρισης των υποδομών καλωδίωσης;	Πρέπει να υπάρχουν διαδικασίες εποπτείας και διαχείρισης των υποδομών καλωδίωσης	7.2.4
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης	30			A	Υπάρχει συμβόλαιο συντήρησης; Είναι οι υποδομές καλωδίωσης εντός εγγυήσης;	Πρέπει να υπάρχει συμβόλαιο συντήρησης και να ελέγχεται εαν οι υποδομές καλωδίωσης είναι εντός εγγυήσης.	7.2.4
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	15			A	Υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών;	Πρέπει να υπάρχουν πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών.	7.2.4
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	15	C	I	A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα ασφαλείας;	Το προσωπικό πρέπει να εκπαίδευεται σε ζητήματα φυσικής ασφαλείας.	6.2.2
	Απουσία ετικετών στην καλωδίωση	20	C	I	A	Γίνεται χρήση ετικετών στην καλωδίωση;	Πρέπει να γίνεται χρήση ετικετών στην καλωδίωση.	7.2.3

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές	20	C		A	Διατηρούνται αρχεία με τις μετατροπές και τις επισκευές στην καλωδίωση;	Πρέπει να διατηρούνται αρχεία με τις μετατροπές και τις επισκευές της καλωδίωσης.	10.5.1
Άρνηση Υπηρεσίας (Denial of Service)	Ελλειψη πλεονάζοντος ή εφεδρικής διασύνδεσης καλωδίωσης	30			A	Υπάρχει διαθέσιμη εναλλακτική, πλεονάζουσα ή εφεδρική δικτυακή διασύνδεση των κρίσιμων συστημάτων (π.χ. εναλλακτική καλωδίωση);	Θα πρέπει να υπάρχει διαθέσιμη εναλλακτική, πλεονάζουσα ή εφεδρική δικτυακή διασύνδεση των κρίσιμων συστημάτων (π.χ. εναλλακτική καλωδίωση).	**12.1.4**
	Υπερφόρτωση δικτύου	20			A	Ο σχεδιασμός του δικτύου λαμβάνει υπ όψην του τις ανάγκες για χωρητικότητα και κάλυψης για τις ανάγκες του οργανισμού;	Κατά το σχεδιασμό του δικτύου πρέπει να λαμβάνονται υπόψη οι ανάγκες εύρους ζώνης (bandwidth) του οργανισμού.	10.1.1
	Ανεπαρκής σχεδιασμός και εγκατάσταση της δομημένης καλωδίωσης	30		I	A	Η δομημένη καλωδίωση έχει σχεδιαστεί και εγκατασταθεί βάση μελέτης;	Η δομημένη καλωδίωση θα πρέπει να έχει σχεδιαστεί και εγκατασταθεί βάση μελέτης.	7.2.3
	Ανεπαρκής διαχείριση του δικτύου (ανθεκτικότητα της δρομολόγησης)	20			A	Ο σχεδιασμός του δικτύου έχει γίνει λαμβάνοντας υπόψη την ανθεκτικότητα της δρομολόγησης	Ο σχεδιασμός του δικτύου να έχει γίνει λαμβάνοντας υπόψη την ανθεκτικότητα της δρομολόγησης.	8.3.1
	Έλλειψη ανθεκτικότητας των υποδομών καλωδίωσης	30		I	A	Οι υποδομές καλωδίωσης έχουν σχεδιαστεί κατάλληλα ώστε να είναι ανθεκτικές σε περιβαλλοντολογικές συνθήκες;	Οι υποδομές καλωδίωσης να έχουν σχεδιαστεί κατάλληλα ώστε να είναι ανθεκτικές σε περιβαλλοντολογικές συνθήκες.	7.1.4
	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	20			A	Χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποιήση και χρήση των υποδομών καλωδίωσης;	Πρέπει να χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποιήση και χρήση των υποδομών καλωδίωσης.	13.2.1

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Ηλεκτρονικές Παρεμβολές	Η περιοχή είναι ευάλωτη σε ηλεκτρονικές παρεμβολές	50			A	Οι περιοχές οπου φιλοξενούνται υποδομές καλωδίωσης είναι προστατευμένες από ηλεκτρονικές παρεμβολές;	Οι περιοχές οπου φιλοξενούνται υποδομές καλωδίωσης δεν πρέπει να είναι ευάλωτες σε ηλεκτρονικές παρεμβολές.	7.2.3
	Μη ανθεκτικότητα των ενσύρματων υποδομών	50			A	Οι υποδομές καλωδίωσης έχουν σχεδιαστεί κατάλληλα ώστε να είναι ανθεκτικές σε περιβαλλοντολογικές συνθήκες και ηλεκτρονικές παρεμβολές;	Οι υποδομές καλωδίωσης πρέπει να έχουν σχεδιαστεί κατάλληλα ώστε να είναι ανθεκτικές σε περιβαλλοντολογικές συνθήκες.	7.1.4
Κλοπή	Έλλειψη πολιτικών και διαδικασιών διαχείρισης φυσικής πρόσβασης	30			A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης;	Πρέπει να υπάρχουν πολιτικές και διαδικασίες για την διαχείριση της πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης.	7.1.2
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	30			A	Οι εγκαταστάσεις οπου φιλοξενούνται κρίσιμες υποδομές πληροφοριακών συστημάτων ελέγχονται για μη εξουσιοδοτημένη πρόσβαση;	Πρέπει να ελέγχεται η φυσική πρόσβαση στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης.	7.1.1
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές	20			A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές;	Πρέπει να υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν κρίσιμες υποδομές.	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10			A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας πρέπει να φωτίζεται επαρκώς.	7.1.1

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Στους χώρους επιτρέπεται η πρόσβαση στο κοινό	10			A	Έχει ληφθεί μέριμνα ώστε το κοινό να μην έχει πρόσβαση σε χώρους πλησίον των εγκαταστάσεων οι οποίες περιέχουν καλωδίωση;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού σε χώρους με υποδομές καλωδίωσης.	7.1.6
	Τοποθεσίες στάθμευσης αυτοκινήτων βρίσκονται εντός της περιμέτρου ασφαλείας	10			A	Υπάρχουν τοποθεσίες στάθμευσης αυτοκινήτων εντός της περιμέτρου ασφαλείας;	Πρέπει να ελέγχεται η στάθμευση των αυτοκινήτων εντός της περιμέτρου ασφαλείας.	7.1.6
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	20			A	Υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στις τεχνικές και κτιριακές υποδομές;	Πρέπει να υπάρχουν διαδικασίες για την πραγματοποίηση αλλαγών και μετατροπών στις τεχνικές και κτιριακές υποδομές.	7.1.3
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	10			A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας.	6.2.2
Υποκλοπή Δεδομένων / Παρακολούθηση επικοινωνιών	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	20	C			Οι εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης ελέγχονται για μη εξουσιοδοτημένη πρόσβαση;	Πρέπει να ελέγχεται η φυσική πρόσβαση στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης.	7.1.1
	Στους χώρους όπου βρίσκονται υποδομές καλωδίωσης επιτρέπεται η πρόσβαση στο κοινό	20	C			Υπάρχουν χώροι με υποδομές καλωδίωσης στους οποίους επιτρέπεται η πρόσβαση στο κοινό;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού σε χώρους με υποδομές καλωδίωσης.	7.1.6
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές καλωδίωσης	20	C			Υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στις υποδομές καλωδίωσης;	Πρέπει να υπάρχουν διαδικασίες για την πραγματοποίηση αλλαγών και μετατροπών στις τεχνικές και κτιριακές υποδομές.	7.1.3

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	20	C			Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας	6.2.2
	Έλλειψη πολιτικών και διαδικασιών διαχείρισης φυσικής πρόσβασης	20	C			Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης;	Πρέπει να υπάρχουν πολιτικές και διαδικασίες για την διαχείριση της πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης.	7.1.2
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού	20	C			Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού.	**7.1.3**
	Ανεπαρκής σχεδιασμός και εγκατάσταση της δομημένης καλωδίωσης	30	C			Η δομημένη καλωδίωση έχει σχεδιαστεί και εγκατασταθεί βάση μελέτης;	Η δομημένη καλωδίωση να έχει σχεδιαστεί και εγκατασταθεί βάσει μελέτης.	7.2.3
	Ανεπαρκής φυσική ασφάλεια σε χώρους όπου υπάρχουν υποδομές καλωδίωσης	20	C			Λαμβάνονται μέτρα φυσικής ασφάλειας σε χώρους όπου υπάρχουν υποδομές καλωδίωσης;	Πρέπει να λαμβάνονται μέτρα φυσικής ασφάλειας σε χώρους με υποδομές καλωδίωσης.	7.2.3
Δολιοφθορά	Έλλειψη πολιτικών και διαδικασιών διαχείρισης φυσικής πρόσβασης	20			A	Υπαρχουν πολιτικές και διαδικασίες που αφορούν την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές	Πρέπει να υπάρχουν πολιτικές και διαδικασίες για την διαχείριση της πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται υποδομές	7.1.2

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						καλωδίωσης;	καλωδίωσης.	
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	20			A	Οι εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης παρακολουθούνται;	Πρέπει να ελέγχεται η φυσική πρόσβαση στις εγκαταστάσεις οπου φιλοξενούνται υποδομές καλωδίωσης.	7.1.1
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού	10			A	Υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού;	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού.	**7.1.3**
	Δεν υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν υποδομές καλωδίωσης;	20			A	Υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν υποδομές καλωδίωσης;	Πρέπει να υπάρχει καθορισμένη περίμετρος ασφαλείας για τα κτίρια/περιοχές που φιλοξενούν υποδομές καλωδίωσης	7.1.1
	Η περίμετρος ασφαλείας δεν φωτίζεται επαρκώς	10			A	Η περίμετρος ασφαλείας φωτίζεται επαρκώς;	Η περίμετρος ασφαλείας να φωτίζεται επαρκώς.	7.1.1
	Στους χώρους επιτρέπεται η πρόσβαση στο κοινό	20			A	Υπάρχουν χώροι με κρίσιμο εξοπλισμό στους οποίους επιτρέπεται η πρόσβαση στο κοινό; Έχει το κοινό πρόσβαση σε χώρους πλησίον των εγκαταστάσεων οι οποίες περιέχουν κρίσιμο εξοπλισμό;	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού σε χώρους με κρίσμο εξοπλισμό.	7.1.6

HW - ΚΑΛΩΔΙΩΣΗ								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Τοποθεσίες στάθμευσης αυτοκινήτων βρίσκονται εντός της περιμέτρου ασφαλείας	10			A	Υπάρχουν τοποθεσίες στάθμευσης αυτοκινήτων εντός της περιμέτρου ασφαλείας;	Πρέπει να ελέγχεται η στάθμευση των αυτοκινήτων εντός της περιμέτρου ασφαλείας.	7.1.6
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές καλωδίωσης	30			A	Υπάρχουν διαδικασίες βάση των οποίων πραγματοποιούνται αλλαγές και μετατροπές στις υποδομές καλωδίωσης;	Πρέπει να υπάρχουν διαδικασίες για την πραγματοποίηση αλλαγών και μετατροπών στις υποδομές καλωδίωσης	7.1.3
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	10			A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα φυσικής ασφαλείας;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας	6.2.2
	Η παραλαβή αγαθών θα πρέπει να πραγματοποιείται σε περιοχή εκτός της περιμέτρου ασφαλείας	10			A	Η παραλαβή αγαθών πραγματοποιείται σε περιοχή εκτός της περιμέτρου ασφαλείας;	Πρέπει να γίνεται έλεγχος κατά την παραλαβή αγαθών σε περιοχή εκτός της περιμέτρου ασφαλείας	7.1.6

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Κακόβουλο Λογισμικό (Malicious Code)	Απουσία λογισμικού ανίχνευσης κακόβουλου λογισμικού (antivirus) ή ελλειπής διαχείριση του antivirus (π.χ. δεν ανανεώνεται αυτόματα)	70	C	I	A	Υπάρχει λογισμικό ανίχνευσης κακόβουλου λογισμικού το οποίο ενημερώνεται τακτικά (π.χ. αυτόματα);	Θα πρέπει να είναι εγκατεστημένο λογισμικό ανίχνευσης κακόβουλου λογισμικού (antivirus), το οποίο λαμβάνει και εγκαθιστά αυτόματα ενημερώσεις.	8.4.1
	Απουσία ή ανεπαρκής παραμετροποίηση του λογισμικού αναχώματος ασφαλείας (personal firewall)	20	C	I	A	Το ανάχωμα ασφαλείας εχει παραμετροποιηθεί βάση των αναγκών ασφαλείας του οργανισμού;	Το ανάχωμα ασφαλείας (firewall) θα πρέπει να είναι διαμορφωμένο σύμφωνα με τις ανάγκες ασφάλειας του οργανισμού.	8.4.2
	Οι απλοί χρήστες έχουν διαχειριστικά δικαιώματα (π.χ. δικαίωμα εγκατάστασης λογισμικού)	50	C	I	A	Έχει ληφθεί μέριμνα ώστε οι απλοί χρήστες να μην έχουν διαχειριστικά δικαιώματα στο σταθμό εργασίας τους (π.χ. δημιουργία νέου λογαριασμού χρήστη, εγκατάσταση εφαρμογής κτλ);	Θα πρέπει να εφαρμόζεται η αρχή των ελάχιστων απαραίτητων δικαιωμάτων πρόσβασης. Οι χρήστες θα πρέπει να συνδέονται στους σταθμούς εργασίας με απλό λογαριασμό χρήστη (user account), χωρίς διαχειριστικά δικαιώματα, π.χ. δικαιώματα προσθήκης ή αφαίρεσης λογισμικού).	9.2.2
	Οι χρήστες έχουν δικαιώματα χρήσης εξωτερικών μέσων αποθήκευσης (cd, usb κτλ)	20	C	I	A	Έχει ληφθεί μέριμνα ώστε οι απλοί χρήστες να μην μπορούν να χρησιμοποιούν εξωτερικά μέσα αποθήκευσης στον υπολογιστή τους (π.χ. usb);	Θα πρέπει να απαγορεύεται στους απλούς χρήστες η εγκατάσταση και χρήση ξξωτερικού μέσου αποθήκευσης (π.χ. κάρτα μνήμης, usb κτλ).	8.7.1
	Έλλειψη πολιτικής αυτόματου ελέγχου επισυναπτόμενων αρχείων του ηλεκτρονικού ταχυδρομείου	20	C	I	A	Πραγματοποιείται αυτόματος έλεγχος για κακόβουλο λογισμικό στο ηλεκτρονικό ταχυδρομείο;	Πρέπει να πραγματοποιείται αυτόματος έλεγχος για κακόβουλο λογισμικό στο περιεχόμενο και στα συνημμένα αρχεία που ανταλλάσσονται	8.8.4

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							μέσω ηλεκτρονικού ταχυδρομείου.	
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	15	C	I	A	Υπάρχει σχέδιο βάση του οποίου το προσωπικό ενημερώνεται και εκπαιδεύεται σε ζητήματα ιών και κακόβουλου λογισμικού;	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα ιών και κακόβουλου λογισμικού.	6.2.2
	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	40	C	I	A	το σύστημα είναι ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ασφάλειας (update / patch management);	Θα πρέπει να πραγματοποιείται ενημέρωση του λειτουργικού συστήματος με τις τελευταίες ενημερώσεις (updating / patching).	8.1.2
	Έλλειψη διαδικασίας ελέγχου αξιοπιστίας του λογισμικού πριν την εγκατάστασή του	30	C	I	A	Υπάρχει διαδικασία ελέγχου της αξιοπιστίας του λογισμικού πριν την εγκατάστασή του (π.χ. απαγόρευση χρήσης μη νόμιμου λογισμικού);	Θα πρέπει να υπάρχει διαδικασία ελέγχου της αξιοπιστίας του λογισμικού πριν την εγκατάστασή του (π.χ. απαγόρευση χρήσης μη νόμιμου λογισμικού).	8.4.1
	Έλλειψη διαδικασίας αναφοράς ή/και αντιμετώπισης περιστατικών ασφαλειάς	10	C	I	A	Υπάρχει διαδικασία αναφοράς και αντιμετώπισης περιστατικών ασφαλειάς;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία αναφοράς και αντιμετώπισης περιστατικών ασφάλειας.	11.1.1
	Ανεπαρκείς μηχανισμοί καταγραφής πρόσβασης και ενεργειών στο σύστημα (audit logs)	15	C	I	A	Το λειτουργικό σύστημα διατηρεί αρχεία καταγραφής για την πρόσβαση και τις ενέργειες που πραγατοποιούνται στο σύστημα (audit logs);	Το λειτουργικό σύστημα θα πρέπει να διατηρεί αρχεία καταγραφής της πρόσβασης και των ενεργειών (audit logs), για επαρκές χρονικό διάστημα.	8.10.4

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Ανεπαρκής έλεγχος και επισκόπιση των αρχείων καταγραφής.	15	C	I	A	Υπάρχει διαδικασία τακτικού ελέγχου και επισκόπισης των αρχείων καταγραφής (audit logs);	Θα πρέπει να υπάρχει διαδικασία τακτικού ελέγχου και επισκόπισης των αρχείων καταγραφής (audit logs);	8.10.2
	Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	15	C	I	A	Πραγματοποιούνται σε συστηματική βάση έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests) ;	Θα πρέπει να πραγματοποιούνται σε συστηματική βάση έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests) για τα κρίσιμα συστήματα.	10.6.1
Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Υπάρχει πολιτική για την υποχρεωτική χρήση αυθεντικού λογισμικού;	30	C	I	A	Υπάρχει πολιτική για την υποχρεωτική χρήση αυθεντικού λογισμικού;	Απαγορεύεται η εγκατάσταση και χρήση "πειρατικού" λογισμικού.	10.4.1
	Έλλειψη επισκόπησης (audit) λογισμικού	20	C	I	A	Πραγματοποιείται επισκόπηση για την επιβολή της πολιτικής μη χρήσης "πειρατικού" λογισμικού;	Θα πρέπει να παγματοποιείται τακτικός έλεγχος για τον έλεγχο μη χρήσης "πειρατικού" λογισμικού.	10.4.1
	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	50	C	I	A	Έχει ληφθεί μέριμνα ώστε οι χρήστες να έχουν δυνατότητα να εγκαθιστούν λογισμικό;	Οι χρήστες θα πρέπει να συνδέονται στο στους σταθμούς εργασίας με απλό λογαριασμό χρήστη (user account), χωρίς διαχειριστικά δικαιώματα, π.χ. προσθήκης ή αφαίρεσης λογισμικού.	9.2.2
Μη εξουσιοδοτημένη πρόσβαση χρηστών (unauthorized access / weak authentication)	Η πρόσβαση στο σύστημα είναι δυνατή χωρίς κανένα έλεγχο (π.χ. δεν απαιτείται η χρήση κάποιου κωδικού πρόσβασης ή βιομετρικού χαρακτηριστικού ή/και	70	C	I	A	Η πρόσβαση των χρηστών απαιτεί κάποιο είδος αυθεντικοποίησης όπως ένα κωδικό ασφαλείας, τη χρήση μιας έξυπνης κάρτας ή τη χρήση κάποιου βιομετρικού	Για τη λογική πρόσβαση χρήστη σε σύστημα, απαιτείται κάποιο είδος αυθεντικοποίησης όπως κωδικός ασφαλείας, ή/και χρήση έξυπνης κάρτας ή/και χρήση κάποιου βιομετρικού	9.2.3

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	έξυπνης κάρτας)					χαρακτηριστικού;	χαρακτηριστικού.	
	Η ισχύς (πολυπλοκότητα) των κωδικών δεν ελέγχονται αυτόματα πριν την έκδοσή τους (π.χ. δεν υπάρχει εγκατεστημένη πολιτική κωδικών)	40	C	I	A	Υπάρχει εγκατεστημένη πολιτική κωδικών ασφαλείας (password policy) η οποία να είναι υποχρεωτική για όλους τους χρήστες;	Θα πρέπει να εφαρμόζεται πολιτική κωδικών ασφαλείας (password policy) η οποία να είναι υποχρεωτική για όλους τους χρήστες.	9.1.1
	Επιτρέπονται κωδικοί ασφαλείας μικρού μήκους (<8 χαρακτήρες)	30	C	I	A	Απαγορεύεται η χρήση "μικρών" κωδικών ασφαλείας (π.χ. με λιγότερους από 8 χαρακτήρες);	Δεν θα πρέπει να γίνονται δεκτοί από το σύστημα, κωδικοί ασφαλείας με μήκος μικρότερο από 8 χαρακτήρες.	9.2.2
	Οι κωδικοί πρόσβασης, αποθηκεύονται σε απλή και όχι σε κρυπτογραφημένη μορφή στο σύστημα (π.χ. hashed passwords)	30	C	I	A	Οι κωδικοί πρόσβασης, αποθηκεύονται σε κρυπτογραφημένη μορφή στο σύστημα (π.χ. hashed passwords);	Θα πρέπει οι κωδικοί πρόσβασης να αποθηκεύονται σε κρυπτογραφημένη μορφή στο σύστημα (π.χ. hashed passwords).	9.2.3
	Χρησιμοποιούνται κοινόχρηστοι / διαμοιραζόμενοι κωδικοί πρόσβασης στο σύστημα (group passwords)	30	C	I	A	Έχει ληφθεί μέριμνα ώστε να μην γίνεται χρήση κοινόχρηστων κωδικών πρόσβασης στο σύστημα; (group passwords)	Απαγορεύται η χρήση κοινόχρηστων κωδικών πρόσβασης σε συστήματα (group passwords).	9.2.3
	Οι χρήστες δεν ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους.	20	C	I	A	Οι χρήστες ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους;	Οι χρήστες θα πρέπει να ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους.	9.3.1
	Είναι ενεργοποιημένη η απομακρυσμένη πρόσβαση των χρηστών στο σύστημα (remote login)	20	C	I	A	Απαγορεύεται η απομακρυσμένη πρόσβαση των χρηστών στα συστήματα (remote login);	Απαγορεύεται η απομακρυσμένη πρόσβαση των χρηστών στα συστήματα (remote login).	9.4.2

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Το σύστημα περιέχει τους αρχικούς λογαριασμούς ή/και κωδικούς πρόσβασης (default accounts, default passwords)	25	C	I	A	Έχουν διαγραφεί οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος (default accounts, default passwords);	Θα πρέπει να διαγράφονται οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος; (default accounts, guest accounts, default passwords).	9.2.4
	Το σύστημα επιτρέπει τη χρήση του ίδιου συνθηματικού για περισσότερο από 1 χρόνο	15	C	I	A	Υπάρχει μέγιστο χρονικό όριο χρήσης των συνθηματικών;	Οι κωδικοί πρόσβασης θα πρέπει να ανανεώνονται κάθε 6 μήνες.	9.2.2
	Ανεπαρκείς μηχανισμοί καταγραφής πρόσβασης και ενεργειών στο σύστημα (audit logs)	15	C	I	A	Το λειτουργικό σύστημα διατηρεί αρχεία καταγραφής για την πρόσβαση και τις ενέργειες που πραγματοποιούνται στο σύστημα (audit logs);	Το λειτουργικό σύστημα θα πρέπει να διατηρεί αρχεία καταγραφής της πρόσβασης και των ενεργειών (audit logs), για επαρκές χρονικό διάστημα.	8.10.4
	Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	15	C	I	A	Πραγματοποιούνται σε συστηματική βάση έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests) ;	Θα πρέπει να πραγματοποιούνται σε συστηματική βάση έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests) για τα κρίσιμα συστήματα.	10.6.1
Δικτυακή εισβολή (network intrusion)	Επιτρέπεται η απομακρυσμένη διαχείριση του συστήματος χωρίς ασφαλή σύνδεση	50		I	A	Έχει ληφθεί μέριμνα ώστε να μην επιτρέπεται η απομακρυσμένη διαχείριση των συστημάτων χωρίς ασφαλή σύνδεση (π.χ. χωρίς SSL ή VPN σύνδεση);	Η απομακρυσμένη πρόσβαση για τη διαχείριση των συστημάτων θα πρέπει να επιτρέπεται μόνο μετά από έγκριση και να πραγματοποιείται μόνο μέσα από ασφαλή σύνδεση (π.χ. SSL ή VPN σύνδεση).	9.4.4

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Το σύστημα είναι εγκατεστημένο σε δίκτυο μη προστατευμένο δίκτυο (π.χ. απουσία αναχώματος ασφαλείας - firwewall)	40	C	I	A	Το σύστημα βρίσκεται εγκατεστημένο σε δίκτυο που ελέγχεται από σύστημα firewall;	Η δικτυακή πρόσβαση στα κρίσιμα συστήματα θα πρέπει να ελέγχεται από κατάλληλα διαμορφωμένο σύστημα firewall.	9.4.6
	Η δικτυακή πρόσβαση στο σύστημα δεν ελέγχεται από σύστημα ανίχνευσης παρείσφρησης (Intrusion Detection/ Prevention System)	30	C	I	A	Το σύστημα βρίσκεται εγκατεστημένο σε δίκτυο που ελέγχεται από σύστημα ανίχνευσης δικτυακών εισβολών (IDS);	Η δικτυακή πρόσβαση στα κρίσιμα συστήματα θα πρέπει να ελέγχεται από κατάλληλα διαμορφωμένο σύστημα ανίχνευσης δικτυακών εισβολών (IDS /IPS).	9.4.6
	Έλλειψη διαδικασίας τακτικού ελέγχου των συστημάτων περιμετρικής προστασίας του δικτύου (π.χ. Firewall, IDS κτλ)	30	C	I	A	Εφαρμόζεται διαδικασία τακτικού ελέγχου των συστημάτων προστασίας του δικτύου (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ)	Τα συστήματα και οι μηχανισμοί ασφάλειας δικτύου, θα πρέπει να ελέγχονται τακτικά, με βάση καταγεγραμμένη διαδικασία (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ).	8.10.2
	Το σύστημα δεν διαχωρίζεται από άλλα δίκτυα με τη χρήση αρχιτεκτονικών δικτύων (π.χ. VLAN, LAN, switches κτλ)	30	C	I	A	Το σύστημα διαχωρίζεται δικτυακά από άλλα συστήματα με τη χρήση αρχιτεκτονικών δικτύων (π.χ. VLAN, LAN, switches κτλ);	Τα κρίσιμα συστήματα θα πρέπει να διαχωρίζονται δικτυακά από άλλα συστήματα με τη χρήση αρχιτεκτονικών ασφάλειας δικτύων (π.χ. VLAN, LAN, VPN κτλ).	9.4.5
	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	30	C	I	A	Υπάρχει διαδικασία διόρθωσης αδυναμιών (patch management);	Θα πρέπει να θπάρχει διαδικασία διόρθωσης αδυναμιών (patch management).	10.5.1

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Εσφαλμένος χειρισμός/χρήση συστήματος (System missuse)	Ανεπαρκής επαγγελματική εμπειρία των χρηστών	35	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των χρηστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των χρηστών.	6.1.2
	Έλλειψη εκπαίδευσης χρηστών	35	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους χρήστες;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους χρήστες των συστημάτων	6.2.2
	Οι απλοί χρήστες έχουν διαχειριστικά δικαιώματα (π.χ. δικαίωμα εγκατάστασης λογισμικού)	50	C	I	A	Έχει ληφθεί μέριμνα ώστε οι απλοί χρήστες να μην έχουν διαχειριστικά δικαιώματα στο σταθμό εργασίας τους (π.χ. δημιουργία νέου λογαριασμού χρήστη, εγκατάσταση εφαρμογής κτλ);	Θα πρέπει να εφαρμόζεται η αρχή των ελάχιστων απαραίτητων δικαιωμάτων πρόσβασης. Οι χρήστες θα πρέπει να συνδέονται στους σταθμούς εργασίας με απλό λογαριασμό χρήστη (user account), χωρίς διαχειριστικά δικαιώματα, π.χ. δικαιώματα προσθήκης ή αφαίρεσης λογισμικού).	9.2.2
	Δύσχρηστο περιβάλλον χρήσης	20	C	I	A	Το περιβάλλον / διεπαφή είναι φιλική προς τον χρήστη / διαχειριστή;	Το περιβάλλον του συστήματος εργασίας θα πρέπει να είναι κατά το δυνατό εύχρηστο και φιλικό προς το χρήστη.	
Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Ανεπαρκής επαγγελματική εμπειρία /εξειδίκευση των διαχειριστών	30	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστώνσε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους χρήστες;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους χρήστες	6.2.2

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	25	C	I	A	Υπάρχει διαθέσιμη έγγραφη τεκμηρίωση διαχείρισης του λειτουργικού συστήματος;	Πρέπει να υπάρχει διαθέσιμη έγγραφη τεκμηρίωση διαχείρισης του λειτουργικού συστήματος.	8.1.1
	Έλλειψη τυποποιημένης διαδικασίας εγκατάστασης και διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process); Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων.	10.5.1
	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	40	C	I	A	Το σύστημα είναι ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ασφάλειας (update / patch management);	Θα πρέπει να πραγματοποιείται ενημέρωση του λειτουργικού συστήματος με τις τελευταίες ενημερώσεις (updating / patching).	10.5.2
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3
	Έλλειψη αντιγράφων επαναφοράς του συστήματος	30			A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων (recovery backup);	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων (recovery backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5
Μη εξουσιοδοτημένη πρόσβαση σε	Ελλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak	25	C	I	A	Υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων (Data Leak	Θα πρέπει να υπάρχουν μηχανισμοί πρόληψης διαρροής δεδομένων	8.8.1

SW - ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ (OPERATING SYSTEM)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
δεδομένα	Prevention - DLPs)					Prevention - DLPs);		
	Ελλειπής κρυπτογράφηση φορητών συσκευών	25	C	I	A	Τα ευαίσθητα δεδομένα που βρίσκονται σε φορητές συσκευές είναι κρυπτογραφημένα;	Τα κρισιμα δεδομένα που βρίσκονται σε φορητές συσκευές θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	10.3.1
	Έλλειψη διαβάθμισης (classification) των πόρων	40	C	I	A	Υπάρχει μεθοδολογία διαβάθμισης των πόρων του οργανισμού;	Θα πρέπει να υπάρχει πολιτική και διαδικασία διαβάθμισης των πόρων του οργανισμού	5.2.1
	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	40	C	I	A	Γίνεται κρυπτογράφηση των ευαίσθητων δεδομένων με αναγνωρισμένες μεθόδους κρυπτογράφησης; (π.χ. AES)	Τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται με αναγνωρισμένες μεθόδους κρυπτογράφησης (π.χ. AES)	10.3.1

SW - ΕΦΑΡΜΟΓΗ ΠΕΛΑΤΗ (CLIENT APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Μη εξουσιοδοτημένη πρόσβαση χρηστών	Η πρόσβαση στην εφαρμογή είναι δυνατή χωρίς κανένα έλεγχο (π.χ. δεν απαιτείται η χρήση κάποιου κωδικού πρόσβασης ή βιομετρικού χαρακτηριστικού ή/και έξυπνης κάρτας)	70	C	I	A	Η πρόσβαση των χρηστών απαιτεί κάποιο είδος αυθεντικοποίησης όπως ένα κωδικό ασφαλείας, τη χρήση μιας έξυπνης κάρτας ή τη χρήση κάποιου βιομετρικού χαρακτηριστικού;	Για τη λογική πρόσβαση χρήστη σε σύστημα, απαιτείται κάποιο είδος αυθεντικοποίησης όπως κωδικός ασφαλείας, ή/και χρήση έξυπνης κάρτας ή/και χρήση κάποιου βιομετρικού χαρακτηριστικού.	9.2.3
	Επιτρέπονται κωδικοί ασφαλείας μικρού μήκους (<8 χαρακτήρες)	30	C	I	A	Απαγορεύεται η χρήση "μικρών" κωδικών ασφαλείας (π.χ. με λιγότερους από 8 χαρακτήρες);	Δεν θα πρέπει να γίνονται δεκτοί από το σύστημα, κωδικοί ασφαλείας με μήκος μικρότερο από 8 χαρακτήρες.	9.2.2
	Επιτρέπονται κωδικοί ασφαλείας χαμηλής πολυπλοκοτητας (π.χ. χρήση μόνο γραμμάτων ή μόνο αριθμών)	30	C	I	A	Γίνεται έλεγχος της πολυπλοκότητας των κωδικών πρόσβασης;	Θα πρέπει να ελέγχεται η πολυπλοκότητα των κωδικών πρόσβασης.	9.2.2
	Χρησιμοποιούνται κοινόχρηστοι / διαμοιραζόμενοι κωδικοί πρόσβασης στην εφαρμογή (group passwords)	30	C	I	A	Έχει ληφθεί μέριμνα ώστε να μην γίνεται χρήση κοινόχρηστων κωδικών πρόσβασης στο σύστημα; (group passwords)	Απαγορεύται η χρήση κοινόχρηστων κωδικών πρόσβασης σε εφαρμογές (group passwords).	9.2.3
	Οι χρήστες δεν ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους (π.χ. μη αποκάλυψη κωδικών σε άλλους χρήστες).	20	C	I	A	Οι χρήστες ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους;	Οι χρήστες θα πρέπει να ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους.	9.3.1
	Το σύστημα περιέχει τους αρχικούς λογαριασμούς ή/και κωδικούς πρόσβασης (default accounts, default passwords)	25	C	I	A	Έχουν διαγραφεί οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος (default accounts, default passwords);	Θα πρέπει να διαγράφονται οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος; (default accounts, guest accounts, default	9.2.4

SW - ΕΦΑΡΜΟΓΗ ΠΕΛΑΤΗ (CLIENT APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							passwords).	
	Το σύστημα επιτρέπει τη χρήση του ίδιου συνθηματικού για περισσότερο από 1 χρόνο	15	C	I	A	Υπάρχει μέγιστο χρονικό όριο χρήσης των συνθηματικών;	Οι κωδικοί πρόσβασης θα πρέπει να ανανεώνονται κάθε 6 μήνες.	9.2.2
	Δεν διατηρούνται τα ίχνη πρόσβασης της εφαρμογής (access logs)	15	C	I	A	Η εφαρμογή διατηρεί αρχεία καταγραφής για την πρόσβαση και τις ενέργειες που πραγματοποιούνται στο σύστημα (audit logs);	Οι κρίσιμες εφαρμογές θα πρέπει να διατηρούν διατηρεί αρχεία καταγραφής της πρόσβασης και των ενεργειών (audit logs), για επαρκές χρονικό διάστημα.	8.10.4
Εσφαλμένη χρήση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των χρηστών	35		I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των χρηστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των χρηστών.	6.1.2
	Έλλειψη εκπαίδευσης χρηστών	35		I	A	Υπαρχεί πλάνο εκπαίδευσης για τους χρήστες;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους χρήστες	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης του λογισμικού	35		I	A	Υπάρχει έγγραφη τεκμηρίωση χρήσης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης του λογισμικού εφαρμογών.	8.1.1
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2

SW - ΕΦΑΡΜΟΓΗ ΠΕΛΑΤΗ (CLIENT APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	35	C	I	A	Υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών.	10.5.1
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει διαδικασία διαχείρισης αλλαγών; Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των εφαρμογών.	10.5.1
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	35		I	A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων;	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας των κρίσιμων εφαρμογών (backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3

SW - ΑΝΕΞΑΡΤΗΤΗ ΕΦΑΡΜΟΓΗ (STAND - ALONE APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Μη εξουσιοδοτημένη πρόσβαση χρηστών	Η πρόσβαση στην εφαρμογή είναι δυνατή χωρίς κανένα έλεγχο (π.χ. δεν απαιτείται η χρήση κάποιου κωδικού πρόσβασης ή βιομετρικού χαρακτηριστικού ή/και έξυπνης κάρτας)	70	C	I	A	Η πρόσβαση των χρηστών απαιτεί κάποιο είδος αυθεντικοποίησης όπως ένα κωδικό ασφαλείας, τη χρήση μιας έξυπνης κάρτας ή τη χρήση κάποιου βιομετρικού χαρακτηριστικού;	Για τη λογική πρόσβαση χρήστη σε σύστημα, απαιτείται κάποιο είδος αυθεντικοποίησης όπως κωδικός ασφαλείας, ή/και χρήση έξυπνης κάρτας ή/και χρήση κάποιου βιομετρικού χαρακτηριστικού.	9.2.3
	Επιτρέπονται κωδικοί ασφαλείας μικρού μήκους (<8 χαρακτήρες)	30	C	I	A	Απαγορεύεται η χρήση "μικρών" κωδικών ασφαλείας (π.χ. με λιγότερους από 8 χαρακτήρες);	Δεν θα πρέπει να γίνονται δεκτοί από το σύστημα, κωδικοί ασφαλείας με μήκος μικρότερο από 8 χαρακτήρες.	9.2.2
	Επιτρέπονται κωδικοί ασφαλείας χαμηλής πολυπλοκοτητας (π.χ. χρήση μόνο γραμμάτων ή μόνο αριθμών)	30	C	I	A	Γίνεται έλεγχος της πολυπλοκότητας των κωδικών πρόσβασης;	Θα πρέπει να ελέγχεται η πολυπλοκότητα των κωδικών πρόσβασης	9.2.2
	Χρησιμοποιούνται κοινόχρηστοι / διαμοιραζόμενοι κωδικοί πρόσβασης στην εφαρμογή (group passwords)	30	C	I	A	Έχει ληφθεί μέριμνα ώστε να μην γίνεται χρήση κοινόχρηστων κωδικών πρόσβασης στο σύστημα; (group passwords)	Απαγορεύται η χρήση κοινόχρηστων κωδικών πρόσβασης σε εφαρμογές (group passwords).	9.2.3
	Οι χρήστες δεν ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους (π.χ. μη αποκάλυψη κωδικών σε άλλους χρήστες).	20	C	I	A	Οι χρήστες ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους;	Οι χρήστες θα πρέπει να ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους.	9.3.1
	Το σύστημα περιέχει τους αρχικούς λογαριασμούς ή/και κωδικούς πρόσβασης (default	25	C	I	A	Έχουν διαγραφεί οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος	Θα πρέπει να διαγράφονται οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του	9.2.4

SW - ΑΝΕΞΑΡΤΗΤΗ ΕΦΑΡΜΟΓΗ (STAND - ALONE APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	accounts, default passwords)					(default accounts, default passwords);	συστήματος; (default accounts, guest accounts, default passwords).	
	Το σύστημα επιτρέπει τη χρήση του ίδιου συνθηματικού για περισσότερο από 1 χρόνο	15	C	I	A	Υπάρχει μέγιστο χρονικό όριο χρήσης των συνθηματικών;	Οι κωδικοί πρόσβασης θα πρέπει να ανανεώνονται κάθε 6 μήνες.	9.2.2
	Δεν διατηρούνται τα ίχνη πρόσβασης της εφαρμογής (access logs)	15	C	I	A	Η εφαρμογή διατηρεί αρχεία καταγραφής για την πρόσβαση και τις ενέργειες που πραγματοποιούνται στο σύστημα (audit logs);	Οι κρίσιμες εφαρμογές θα πρέπει να διατηρούν διατηρεί αρχεία καταγραφής της πρόσβασης και των ενεργειών (audit logs), για επαρκές χρονικό διάστημα.	8.10.4
Εσφαλμένη χρήση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των χρηστών	35		I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των χρηστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των χρηστών.	6.1.2
	Έλλειψη εκπαίδευσης χρηστών	35		I	A	Υπαρχεί πλάνο εκπαίδευσης για τους χρήστες;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους χρήστες	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης του λογισμικού	35		I	A	Υπάρχει έγγραφη τεκμηρίωση χρήσης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης του λογισμικού εφαρμογών.	8.1.1
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2

SW - ΑΝΕΞΑΡΤΗΤΗ ΕΦΑΡΜΟΓΗ (STAND - ALONE APPLICATION)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	35	C	I	A	Υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών.	10.5.1
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει διαδικασία διαχείρισης αλλαγών; Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των εφαρμογών.	10.5.1
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	35		I	A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων;	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας των κρίσιμων εφαρμογών (backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3

ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATABASE SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Επίθεση κλοπής/ αλλοίωσης δεδομένων	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	35	C	I	A	Γίνεται κρυπτογράφηση των ευαίσθητων δεδομένων της βάσης με αναγνωρισμένες μεθόδους κρυπτογράφησης; (π.χ. AES)	Θα πρέπει να εφαρμόζεται κρυπτογράφηση των ευαίσθητων δεδομένων της βάσης με αναγνωρισμένες μεθόδους κρυπτογράφησης; (π.χ. AES)	10.3.1
	Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων	35	C	I	A	Γίνεται χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων της βάσης με αναγνωρισμένες μεθόδους; (π.χ. SHA, MD5)	Θα πρέπει να γίνεται χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων της βάσης με αναγνωρισμένες μεθόδους (π.χ. SHA, MD5).	10.2.3
	Έλλειψη διαδικασίας ελέγχου πρόσβασης και καταγραφής ενεργειών σε επίπεδο βάσης δεδομένων	35	C	I	A	Υπάρχει διαδικασία ελέγχου πρόσβασης (access control) και καταγραφής ενεργειών (audit) στη βάση δεδομένων;	Θα πρέπει να εφαρμόζεται διαδικασία ελέγχου πρόσβασης (access control) και καταγραφής ενεργειών (audit) στη βάση δεδομένων.	8.10.2
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	25	C	I	A	Υπάρχει διαδικασία τακτικού ελέγχου του database server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του database server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία….)	50	C	I	A	Πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation); Π.χ. να γίνεται έλεγχος ώστε να κόβονται ειδικοί.	Θα πρέπει να πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation) στα sql ερωτήματα προς τη βάση δεδομένων.	10.2.1

ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATABASE SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	35	C	I	A	Πραγματοποιείται έλεγχος ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	Θα πρέπει να πραγματοποιείται έλεγχος ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση δεδομένων.	10.2.4
	Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	25	C	I	A	Υπάρχει διαδικασία ελέγχου ώστε ο database server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner;	Θα πρέπει να εφαρμόζεται διαδικασία ελέγχου ώστε ο database server να μην παρέχει πληροφορίες διαμόρφωσης (configuration).	10.2.4
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	25	C	I	A	Υπάρχει διαδικασία τακτικού ελέγχου του database server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του database server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	35	C	I	A	Υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών.	10.5.1

ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATABASE SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει διαδικασία διαχείρισης αλλαγών; Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των εφαρμογών.	10.5.1
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	35		I	A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων;	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας των κρίσιμων εφαρμογών (backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5
	Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	35	C	I	A	Το σύστημα είναι ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ασφάλειας (update / patch management);	Θα πρέπει να πραγματοποιείται ενημέρωση του λειτουργικού συστήματος με τις τελευταίες ενημερώσεις (updating / patching).	10.5.1
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3
Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	40			A	Τα αντίγραφα ασφαλείας αποθηκεύονται και σε εναλλακτική τοποθεσία, σε ικανοποιητική απόσταση, η οποία να είναι απρόσβλητη από ζημιές που θα προκληθούν στις κεντρικές υποδομές;	Τα αντίγραφα ασφαλείας θα πρέπει να αποθηκεύονται και σε εναλλακτική τοποθεσία, σε ικανοποιητική απόσταση, η οποία να είναι απρόσβλητη από ζημιές που θα προκληθούν στις κεντρικές υποδομές	8.5.1

ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATABASE SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	40			A	Υπάρχει διαδικασία λήψης αντιγράφων ασφαλείας;	Θα πρέπει να υπάρχει και να ακολουθείται διαδικασία λήψης αντιγράφων ασφαλείας;	8.5.1
	Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	20			A	Υπάρχει σχήμα διαβάθμισης των δεδομένων; Τα συστήματα και δεδομένα αξιολογούνται βάση της κρισιμότητας τους;	Τα συστήματα και δεδομένα θα πρέπει να αξιολογούνται και να κατηγοριοποιούνται βάση της κρισιμότητας τους	5.2.1
	Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	30			A	Υπάρχει διαδικασία ανάκαμψης αντιγράφων ασφαλείας; Δοκιμάζεται σε τακτά χρονικά διαστήματα για τα κρίσιμα συστήματα και δεδομένα;	Θα πρέπει να υπάρχει, να ακολουθείται και να δοκιμάζεται διαδικασία ανάκαμψης αντιγράφων ασφαλείας	8.5.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΕΦΑΡΜΟΓΩΝ (APPLICATION SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Επίθεση XSS	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)	50	C	I	A	Πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation);	Θα πρέπει να πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation) τα οποία αποστέλλονται από την εφαρμογή προς τη βάση δεδομένων.	10.2.1
	Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήτων σε απλή html	30	C	I	A	Γίνεται χρήση συναρτήσεων μετατροπής ειδικών χαρακτήτων σε απλή html;	Θα πρέπει οι διαδικτυακές εφαρμογές να ελέγχονται ώστε να εφαρμόζονται ειδικές συναρτήσεις μετατροπής ειδικών χαρακτήρων σε απλή html.	10.2.1
	Μη χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html	25	C	I	A	Γίνεται χρήση τεχνικών αφαίρεσης μη έγκυρων html ετικετών;	Θα πρέπει στις διαδικτυακές εφαρμογές να γίνεται χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html.	10.2.1
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	25	C	I	A	Υπάρχει διαδικασία τακτικού ελέγχου του application server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του application server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία)	50	C	I	A	Πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation); Π.χ. να γίνεται έλεγχος ώστε να κόβονται ειδικοί χαρακτήρες όπως ', ", κτλ.	Θα πρέπει να πραγματοποιείται έλεγχος της εγκυρότητας των δεδομένων εισόδου (input validation) στα sql ερωτήματα προς τη βάση δεδομένων.	10.2.1
	Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	35	C	I	A	Πραγματοποιείται έλεγχος ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	Θα πρέπει να πραγματοποιείται έλεγχος ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη	10.2.4

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΕΦΑΡΜΟΓΩΝ (APPLICATION SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							βάση δεδομένων.	
	Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	25	C	I	A	Υπάρχει διαδικασία ελέγχου ώστε ο application server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner;	Θα πρέπει να εφαρμόζεται διαδικασία ελέγχου ώστε ο application server να μην παρέχει πληροφορίες διαμόρφωσης (configuration).	10.2.4
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	25	C	I	A	Υπάρχει διαδικασία τακτικού ελέγχου του application server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του application server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	35	C	I	A	Υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών.	10.5.1
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει διαδικασία διαχείρισης αλλαγών; Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των	10.5.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΕΦΑΡΜΟΓΩΝ (APPLICATION SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							εφαρμογών.	
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	35		I	A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων;	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας των κρίσιμων εφαρμογών (backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5
	Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	35	C	I	A	Το σύστημα είναι ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ασφάλειας (update / patch management);	Θα πρέπει να πραγματοποιείται ενημέρωση του λειτουργικού συστήματος με τις τελευταίες ενημερώσεις (updating / patching).	10.5.1
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3

ΛΟΓΙΣΜΙΚΟ ΠΑΡΟΧΗΣ ΙΣΤΟΣΕΛΙΔΩΝ (WEB SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Επίθεση αλλοίωσης σελίδας (web defacement attack)	Επιτρέπεται η απομακρυσμένη διαχείριση του εξυπηρετητή χωρίς ασφαλή σύνδεση	50		I	A	Έχει ληφθεί μέριμνα ώστε να μην επιτρέπεται η απομακρυσμένη διαχείριση χωρίς ασφαλή σύνδεση (π.χ. χωρίς SSL ή VPN σύνδεση);	Η απομακρυσμένη πρόσβαση για τη διαχείριση των εξυπηρετητών θα πρέπει να επιτρέπεται μόνο μετά από έγκριση και να πραγματοποιείται μόνο μέσα από ασφαλή σύνδεση (π.χ. SSL ή VPN σύνδεση).	9.4.4
	Ελλιπή μέτρα προστασίας του web server (π.χ δεν υπάρχει εγκατεστημένο web application firewall)	35		I	A	Έχει εγκατασταθεί σύστημα ελέγχου ασφάλειας του web server όπως web-application firewall;	Θα πρέπει να εφαρμόζονται κατάλληλα μέτρα προστασίας των εξυπηρετητών διαδικτύου (web servers) σε επίπεδο εφαρμογής (π.χ. εφαρμογή web-application firewall).	8.6.2
	Έλλειψη διαδικασίας τακτικού ελέγχου των ρυθμίσεων ασφάλειας και των αρχείων καταγραφής του web server (audit logs)	35		I	A	Υπάρχει διαδικασία τακτικού ελέγχου των ρυθμίσεων ασφάλειας και των αρχείων καταγραφής (audit logs) του web server;	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου των ρυθμίσεων ασφάλειας και των αρχείων καταγραφής (audit logs) του web server.	8.10.2
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων πρωτοκόλλων δικτύου- θυρών	25		I	A	Υπάρχει διαδικασία τακτικού ελέγχου του web server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του web server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Επίθεση άρνησης υπηρεσίας (Denial of Service attack)	Έλλειψη διαμόρφωσης για την προστασία από επιθέσεις Syn flooding				A	Έχει πραγματοποιηθεί κατάλληλη διαμόρφωση για προστασία από επιθέσεις τύπου syn flooding;	Η διαμόρφωση του web server θα πρέπει να είναι κατάλληλη ώστε να είναι ανθεκτικός σε επιθέσεις τύπου syn flooding.	9.4.6
	Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω	25			A	Υπάρχει διαδικασία ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration),	Υπάρχει διαδικασία ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner;	10.2.4

ΛΟΓΙΣΜΙΚΟ ΠΑΡΟΧΗΣ ΙΣΤΟΣΕΛΙΔΩΝ (WEB SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	banner					π.χ. μέσω banner;		
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	25			A	Υπάρχει διαδικασία τακτικού ελέγχου του web server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ)	Θα πρέπει να εφαρμόζεται διαδικασία τακτικού ελέγχου του web server για την πιθανή λειτουργία ανεπιθύμητων υπηρεσιών-θυρών (π.χ. Icmp, smb, netbios κτλ).	9.4.6
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής	40	C	I	A	Η διαδικασία πρόσληψης προσωπικού, λαμβάνει υπόψη την επαγγελματική εμπειρία και εξειδίκευση των διαχειριστών;	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	6.1.2
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας	25	C	I	A	Υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές;	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	6.2.2
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού	35	C	I	A	Υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών;	Πρέπει να υπάρχει έγγραφη τεκμηρίωση διαχείρισης του λογισμικού εφαρμογών.	10.5.1
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	25	C	I	A	Υπάρχει διαδικασία διαχείρισης αλλαγών; Υπάρχουν τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων;	Θα πρέπει να υπάρχει καταγεγραμμένη διαδικασία διαχείρισης αλλαγών (change management process), καθώς και τεχνικά πρότυπα για την ορθή εγκατάσταση και παραμετροποίηση των εφαρμογών.	10.5.1
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	35		I	A	Λαμβάνονται αντίγραφα ασφαλείας της παραμετροποίησης των κρίσιμων συστημάτων;	Θα πρέπει να λαμβάνονται αντίγραφα ασφαλείας των κρίσιμων εφαρμογών (backup), σύμφωνα με καταγεγραμμένη διαδικασία.	12.1.5

ΛΟΓΙΣΜΙΚΟ ΠΑΡΟΧΗΣ ΙΣΤΟΣΕΛΙΔΩΝ (WEB SERVER SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	35	C	I	A	Το σύστημα είναι ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ασφάλειας (update / patch management);	Θα πρέπει να πραγματοποιείται ενημέρωση του λειτουργικού συστήματος με τις τελευταίες ενημερώσεις (updating / patching).	8.1.2
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	40	C	I	A	Εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης;	Θα πρέπει να εφαρμόζεται πολιτική διαχωρισμού αρμοδιοτήτων των διαχειριστών, με βάση την αρχή των ελάχιστων αναγκαίων δικαιωμάτων πρόσβασης.	8.1.3

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
Παρακολούθηση επικοινωνιών (Traffic Monitoring)	Μετάδοση δεδομένων μέσω μη ασφαλών διαύλων	40	C			Έχει ληφθεί μέριμνα ώστε να μην μεταδίδονται εμπιστευτικά δεδομένα από μη ασφαλείς διαύλους; (π.χ. internet, ή ασύρματες συνδέσεις (radio), μικροκυματικές (microwave links) κτλ)	Απαγορεύεται η μετάδοση των δεδομένων μέσω μη ασφαλών / ασφαλισμένων διαδικτυακών (internet) ή ασύρματων συνδέσεων (radio, satellite, microwave links).	9.4.1
	Χρήση δημόσιων δικτύων	30	C			Χρησιμοποιείται ιδιωτικό δίκτυο για την εσωτερική επικοινωνία; Αποφεύγεται η χρήση δικτύων διαμοιραζόμενων με τρίτους για τη μετάδοση εσωτερικών δεδομένων;	Η επικοινωνία μεταξύ των εσωτεριών συστημάτων θα πρέπει να γίνεται μέσω ιδιωτικών και μη διαμοιραζόμενων δικτύων.	9.4.5
	Μετάδοση διαβαθμισμένων δεδομένων στο δίκτυο	20	C			Έχει ληφθεί μέριμνα ώστε εμπιστευτικά δεδομένα ή δεδομένα με εμπορική ή οικονομική σημασία να μην μεταδίδονται στο δίκτυο;	Θα πρέπει να αποφεύγεται η μετάδοση δίκτυο εμπιστευτικών δεδομένωνή δεδομένων με εμπορική ή οικονομική σημασία,	8.8.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							εκτός εάν είναι απολύτως απαραίτητο,	
	Μη υλοποίηση μεταπηδησης συχνοτήτων σε ευρύ φάσμα (frequency hopping spread spectrum)	10	C			Χρησιμοποιείται μεταπηδηση συχνοτήτων σε ευρύ φάσμα στις δορυφορικές επικοινωνίες;	Χρησιμοποιείται μεταπηδηση συχνοτήτων σε ευρύ φάσμα στις δορυφορικές επικοινωνίες;	9.4.1
	Μη χρήση κρυπτογραφίας για τη μετάδοση κρίσιμων δεδομένων	50	C			Γίνεται χρήση κρυπτογραφίας κατά τη μετάδοση διαβαθμισμένων δεδομένων;	Η μετάδοση των διαβαθμισμένων δεδομένων επιτρέπεται μόνο εφόσον εφαρμόζεται στα δεδομένα ισχυρή κρυπτογράφηση.	10.3.1
	Μη ορθή παραμετροποίηση δικτυακού εξοπλισμου	30	C			Υπάρχουν τεχνικά πρότυπα για την παραμετροποίηση των δικτυακών συσκευών;	Η παραμετροποίηση του δικτυακού εξοπλισμου θα πρέπει να πραγματοποιείται σύμφωνα με αναγνωρισμένα τεχνικά πρότυπα.	13.2.1
Εξαπάτηση διεύθυνσης δικτύου (IP Spoofing)	Η αυθεντικοποίηση πραγματοποιείται μόνο βάση της διεύθυνσης δικτύου (IP address)		C	I		Έχει ληφθεί μέριμνα ώστε η αυθεντικοποίηση να μην πραγματοποιείται μόνο βάση της διεύθυνσης δικτύου (IP address);	Για τα κρίσιμα δικτυακά συστήματα, η αυθεντικοποίηση δεν πρέπει να βασίζεται μόνο στη διεύθυνση δικτύου (IP address), αλλά σε ισχυρό	9.4.7

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
							μηχανισμό αυθεντικοποίησης.	
	Έλλειψη ιχνών ασφαλείας (audit logs)		C	I		Εφαρμόζεται διαδικασία τακτικού ελέγχου των συστημάτων προστασίας του δικτύου (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ)	Τα συστήματα και οι μηχανισμοί ασφάλειας δικτύου, θα πρέπει να ελέγχονται τακτικά, με βάση καταγεγραμμένη διαδικασία (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ).	8.10.2
	Έλλειψη Συστήματος Ανίχνευσης Παρείσφρησης (Intrusion Detection System - IDS)		C	I		Υπάρχει Σύστημα Ανίχνευσης Παρείσφρησης (IDS);	Θα πρέπει να υπάρχει εγκατεστημένο Σύστημα Ανίχνευσης Παρείσφρησης (IDS).	9.4.1
Εξαπάτηση φυσικής διεύθυνσης (MAC spoofing)	Η αυθεντικοποίηση πραγματοποιείται μόνο βάση της φυσικής διεύθυνσης (MAC address)		C	I		Έχει ληφθεί μέριμνα ώστε η αυθεντικοποίηση να μην πραγματοποιείται μόνο βάση της	Για τα κρίσιμα δικτυακά συστήματα, η αυθεντικοποίηση δεν πρέπει να βασίζεται μόνο στη φυσική	9.4.6

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						φυσικής διεύθυνσης (MAC address);	διεύθυνση (MAC address).	
	Έλλειψη Συστήματος Ανίχνευσης Παρείσφρησης (Intrusion Detection System - IDS)		C	I		Υπάρχει Σύστημα Ανίχνευσης Παρείσφρησης (IDS);	Θα πρέπει να υπάρχει εγκατεστημένο Σύστημα Ανίχνευσης Παρείσφρησης (IDS).	9.4.1
	Ανεπαρκείς μηχανισμοί παρακολούθησης		C	I		Εφαρμόζεται διαδικασία τακτικού ελέγχου των συστημάτων προστασίας του δικτύου (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ)	Τα συστήματα και οι μηχανισμοί ασφάλειας δικτύου, θα πρέπει να ελέγχονται τακτικά, με βάση καταγεγραμμένη διαδικασία (π.χ. έλεγχος διαμόρφωσης των συστημάτων προστασίας δικτύου, διατήρηση audit logs, έλεγχος audit logs κτλ).	8.10.2
Μη ορθή δρομολόγηση επικοινωνιών	Απουσία κεντρικού συστήματος ελέγχου και εποπτείας του δικτύου		C		A	Υπάρχει κάποιο σύστημα κεντρικού ελέγχου και εποπτείας του δικτύου;	Τα δικτυακά συστήματα θα πρέπει να ελέγχονται μέσω συστήματος κεντρικού ελέγχου και εποπτείας του δικτύου.	8.1.1 / 8.6.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
	Κατάχρηση των θυρών απομακρυσμένης πρόσβασης (remote maintenance ports)		C		A	Λαμβάνονται μέτρα για την προστασία των θυρών απομακρυσμένης πρόσβασης;	Θα πρέπει να λαμβάνονται μέτρα ελέγχου και απομακρυσμένης πρόσβασης των δικτυακών θυρών (π.χ. κλείσιμο θυρών)	9.4.4
	Μη ορθή παραμετροποίηση δικτυακού εξοπλισμου		C		A	Η παραμετροποίηση του δικτυακού εξοπλισμου πραγματοποιείται με βάση τεχνικών προτύπων;	Η παραμετροποίηση του δικτυακού εξοπλισμου θα πρέπει να πραγματοποιείται σύμφωνα με αναγνωρισμένα τεχνικά πρότυπα.	13.2.1
	Μη ορθή παραμετροποίηση δικτυακού εξοπλισμου		C		A	Η παραμετροποίηση του δικτυακού εξοπλισμου ελέγχεται (audits / vulnerability assessments) για την ορθότητα της ανα τακτά χρονικά διαστήματα;	Η παραμετροποίηση του δικτυακού εξοπλισμου ελέγχεται (audits / vulnerability assessments) για την ορθότητα της ανα τακτά χρονικά διαστήματα;	13.2.1
Μη εξουσιοδοτημένη πρόσβαση χρηστών	Η πρόσβαση στην εφαρμογή είναι δυνατή χωρίς κανένα έλεγχο (π.χ. δεν απαιτείται η χρήση κάποιου κωδικού πρόσβασης ή βιομετρικού χαρακτηριστικού ή/και έξυπνης κάρτας)	70	C	I	A	Η πρόσβαση των χρηστών απαιτεί κάποιο είδος αυθεντικοποίησης όπως ένα κωδικό ασφαλείας, τη χρήση μιας έξυπνης κάρτας	Για τη λογική πρόσβαση χρήστη σε σύστημα, απαιτείται κάποιο είδος αυθεντικοποίησης όπως κωδικός ασφαλείας, ή/και	9.2.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						ή τη χρήση κάποιου βιομετρικού χαρακτηριστικού;	χρήση έξυπνης κάρτας ή/και χρήση κάποιου βιομετρικού χαρακτηριστικού.	
	Επιτρέπονται κωδικοί ασφαλείας μικρού μήκους (<8 χαρακτήρες)	30	C	I	A	Έχει ληφθεί μέριμνα ώστε να μην επιτρέπεται η χρήση "μικρών" κωδικών ασφαλείας (π.χ. με λιγότερους από 8 χαρακτήρες);	Δεν θα πρέπει να γίνονται δεκτοί από το σύστημα, κωδικοί ασφαλείας με μήκος μικρότερο από 8 χαρακτήρες.	9.2.2
	Επιτρέπονται κωδικοί ασφαλείας χαμηλής πολυπλοκοτητας (π.χ. χρήση μόνο γραμμάτων ή μόνο αριθμών)	30	C	I	A	Γίνεται έλεγχος της πολυπλοκότητας των κωδικών πρόσβασης;	Θα πρέπι να εφαρμόζεται έλεγχος της πολυπλοκότητας των κωδικών πρόσβασης που χρησιμοποιούνται από λογισμικό εφαρμογής (application layer software).	9.2.2
	Χρησιμοποιούνται κοινόχρηστοι / διαμοιραζόμενοι κωδικοί πρόσβασης στην εφαρμογή (group passwords)	30	C	I	A	Έχει ληφθεί μέριμνα ώστε να μην γίνεται χρήση κοινόχρηστων κωδικών πρόσβασης στο σύστημα; (group passwords)	Απαγορεύται η χρήση κοινόχρηστων κωδικών πρόσβασης σε εφαρμογές (group passwords).	9.2.3
	Οι χρήστες δεν ενημερώνονται εγγράφως/ενυπογράφως για τους κανόνες προστασίας των κωδικών τους (π.χ. μη αποκάλυψη κωδικών σε άλλους χρήστες).	20	C	I	A	Οι χρήστες ενημερώνονται εγγράφως/ενυπογράφως για τους	Οι χρήστες θα πρέπει να ενημερώνονται εγγράφως/ενυπογράφως για τους	9.3.1

ΛΟΓΙΣΜΙΚΟ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΩΣΗΣ (NETWORK SW)								
Απειλές	**Αδυναμίες**		**Συνέπειες**			**Ερωτηματολόγιο**	**Μέτρο Ασφάλειας**	**Αντιστοίχιση με (υπο)πολιτική**
			C	**I**	**A**			
						κανόνες προστασίας των κωδικών τους;	κανόνες προστασίας των κωδικών τους.	
	Το λογισμικό διαχείρισης δικτύου περιέχει τους αρχικούς λογαριασμούς ή/και κωδικούς πρόσβασης (default accounts, default passwords)	25	C	I	A	Έχουν διαγραφεί οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος (default accounts, default passwords);	Θα πρέπει να διαγράφονται οι αρχικοί λογαριασμοί ή/και κωδικοί πρόσβασης του συστήματος; (default accounts, guest accounts, default passwords).	9.2.4
	Χρήση του ίδιου συνθηματικού για περισσότερο από 1 χρόνο	15	C	I	A	Υπάρχει μέγιστο χρονικό όριο χρήσης των συνθηματικών;	Οι κωδικοί πρόσβασης θα πρέπει να ανανεώνονται κάθε 6 μήνες.	9.2.2
	Δεν διατηρούνται τα ίχνη πρόσβασης στην εφαρμογή (access logs)	15	C	I	A	Η εφαρμογή διατηρεί αρχεία καταγραφής για την πρόσβαση και τις ενέργειες που πραγματοποιούνται στο σύστημα (audit logs);	Οι κρίσιμες εφαρμογές θα πρέπει να διατηρούν διατηρεί αρχεία καταγραφής της πρόσβασης και των ενεργειών (audit logs), για επαρκές χρονικό διάστημα.	8.10.4

8.3 Παράρτημα ΙΙΙ: Ταξονομία STORM

Όλα τα έγγραφα της η-βιβλιοθήκης του STORM είναι κατηγοριοποιημένα με βάση την παρακάτω ταξονομία.

- ✓ **Διεθνές Πλαίσιο:**
  - Έρευνα και Μελέτες
  - Βέλτιστες Πρακτικές
  - Προγράμματα και Πρωτοβουλίες
  - Στατιστικά
  - Σχετικές Αρχές και Οργανισμοί

- ✓ **Ελλάδα:**
  - Έρευνα και Μελέτες
  - Βέλτιστες Πρακτικές
  - Εθνικές Πολιτικές και Πρακτικές
  - Νομοθεσία
  - Προγράμματα και Πρωτοβουλίες
  - Στατιστικά
  - Σχετικές Αρχές και Οργανισμοί
  - Λοιπά

- ✓ **Ευρωπαϊκό Πλαίσιο:**
  - Έρευνα και Μελέτες
  - Βέλτιστες Πρακτικές
  - Κανονιστικό Πλαίσιο
  - Οδηγίες
  - Προγράμματα και Πρωτοβουλίες
  - Στατιστικά
  - Σχετικές Αρχές και Οργανισμοί
  - Λοιπά

- ✓ **Κώδικας ISPS:**
  - Βέλτιστες Πρακτικές του Κώδικα ISPS
  - Κώδικας ISPS και Αναθεωρήσεις
  - Λοιπές Σχετικές Πληροφορίες

- ✓ **Λοιπές Πληροφορίες:**
  - Εγχειρίδια Εργαλείων Ασφάλειας
  - Λοιπά Σχετικά Πρότυπα Ασφάλειας
  - Λοιπές Πληροφορίες Ασφάλεια

8.4 Παράρτημα IV: Πρότυπο αναπαράστασης υπηρεσιών

Βήματα των διαδικασιών που ακολουθεί η η-υπηρεσία:

Περιγράψτε όλα τα βήματα που ακολουθεί η η-υπηρεσία. Αριθμήστε όλα τα βήματα (σειριακά)
Σε κάθε βήμα καθορίστε :

1. τους εμπλεκόμενους φορείς,
2. τα εμπλεκόμενα φυσικά πρόσωπα,
3. τα εμπλεκόμενα η-έγγραφα (που τροφοδοτούνται και παράγονται σε κάθε βήμα)
4. τη σχετική νομοθεσία,
5. το αποτέλεσμα βήματος (έξοδος).

Κατηγορίες για περιγραφή επιχειρησιακών διαδικασιών (συμπληρώστε, προσθέστε, σβήστε σχετικές γραμμές στους παρακάτω πίνακες) :

1. Εμπλεκόμενοι φορείς:

Όνομα Υπηρεσίας:		
Εμπλεκόμενοι φορείς		
Κατηγορία	**Τύπος Οργανισμού**	**Τμήμα**
Κυβερνητικός (Εθνικός)		
Κυβερνητικός (Ευρωπαϊκός)		
Κυβερνητικός (Παγκόσμιος)		
Ιδιωτικός (Εθνικός)		
Ιδιωτικός		

(Ευρωπαϊκός)		
Άλλος		

2. Εμπλεκόμενα φυσικά πρόσωπα:

Όνομα Υπηρεσίας:	
Εμπλεκόμενα φυσικά πρόσωπα	
Τύπος	**Περιγραφή**
Διοικητικός υπάλληλος (εντός οργανισμού)	
Διοικητικός υπάλληλος (εκτός οργανισμού)	
Υπάλληλος/οι (εντός οργανισμού)	
Υπάλληλος/οι (εκτός οργανισμού)	
Εξωτερικός χρήστης Α	
Εξωτερικός χρήστης Β	
…..	

3. Εμπλεκόμενα έγγραφα:

Όνομα Υπηρεσίας:		
Εμπλεκόμενα έγγραφα		
Τύπος	**Όνομα εγγράφου**	**Εκδότης**
Κυβερνητικό (Εθνικό)		
Κυβερνητικό (Ευρωπαϊκό)		
Κυβερνητικό (Παγκόσμιο)		
Ιδιωτικό (Εθνικό)		

Ιδιωτικό (Εθνικό)		
Ιδιωτικό (Ευρωπαϊκό)		
Ενδο-οργανωτικό		
Προσωπικό		
Άλλο		

4. Σχετική νομοθεσία που υπόκειται αυτή η η-υπηρεσία:

Όνομα Υπηρεσίας:		
Σχετική νομοθεσία που υπόκειται αυτή η η-υπηρεσία		
Τύπος (Νόμος / Προεδρικό Διάταγμα / Άλλο)	**Όνομα εγγράφου / ΦΕΚ**	

5. Αποτελέσματα η-υπηρεσίας:

Όνομα Υπηρεσίας:	
Αποτελέσματα η-υπηρεσίας	
Βήμα	**Αποτελέσματα – έξοδος του βήματος**

8.5 Παράρτημα V: Υπόδειγμα αναφορών μεθοδολογίας STORM-RM

8.5.1 Λίστα αγαθών και αλληλεξαρτήσεων

Ομάδες Χρηστών STORM-RM		
Ομάδα	**Περιγραφή**	**Βάρος Ομάδας**
Διοίκηση	Η ομάδα αυτή περιλαμβάνει τα μέλη της Διοίκησης, πχ. Προϊστάμενος Πληροφορικής κλπ	
Ομάδα ασφάλειας	Η ομάδα αυτή περιλαμβάνει τα μέλης της ομάδας Ασφάλειας του οργανισμού, π.χ. Προϊστάμενος Ασφάλειας, Εσωτερικός Ελεγκτής, κλπ.	
Διαχειριστές	Η ομάδα αυτή περιλαμβάνει τους διαχειριστές των ΠΣ, π.χ. Διαχειριστές Δικτύων, Διαχειριστές Εφαρμογών κλπ.	
Τελικοί Χρήστες	Περιλαμβάνει τους τελικούς χρήστες του ΠΣ, οι οποίοι μπορεί να είναι είτε Εσωτερικοί είτε Εξωτερικοί (π.χ. συνεργάτες, προμηθευτές)	

Χρήστες ΠΣ						
Επώνυμο	**Όνομα**	**Ειδικότητα**	**Ρόλος στον οργανισμό**	**Τηλέφωνο**	**Γραφείο**	**STORM-RM ομάδα**

Συνολικός Πίνακας Αγαθών			
Η-Υπηρεσία:		**Περιγραφή υπηρεσίας**	
Αγαθό	**Περιγραφή**	**Κατηγορία Αγαθού**	**Τοποθεσία**
Η-Υπηρεσία:		**Περιγραφή υπηρεσίας**	
Αγαθό	**Περιγραφή**	**Κατηγορία Αγαθού**	**Τοποθεσία**

8.5.2 Αναφορά Ανάλυσης Επικινδυνότητας

1. Αποτίμηση Επιπτώσεων

1.1. Ατομική Αποτίμηση Αγαθού

Α/Α		**Όνομα Αγαθού**		**Υπηρεσία**	
Απώλεια Διαθεσιμότητας					
ΕΠΙΠΤΩΣΕΙΣ					
ΑΠΟΤΙΜΗΣΗ (1-5)					
Απώλεια Εμπιστευτικότητας					
ΕΠΙΠΤΩΣΕΙΣ					
ΑΠΟΤΙΜΗΣΗ (1-5)					
Απώλεια Ακεραιότητας					
ΕΠΙΠΤΩΣΕΙΣ					
ΑΠΟΤΙΜΗΣΗ (1-5)					

1.2. Ομαδική Αποτίμηση Αγαθών

Ομάδα:			**Βάρος Ομάδας:**						**Υπηρεσία**
Αγαθό	**Απώλεια Διαθεσιμότητας**		**Απώλεια Ακεραιότητας**		**Απώλεια Εμπιστευτικότητας**		**Συνολικός Ομαδικός Βαθμός**		
	Βαθμός	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	

1.3. Συνολική αποτίμηση αγαθών

Αγαθό	**Απώλεια Διαθεσιμότητας**		**Απώλεια Ακεραιότητας**		**Απώλεια Εμπιστευτικότητας**		**Συνολικός Βαθμός**		**Υπηρεσία**
	Βαθμός	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	**Βαθμός**	**Επίπεδο**	

2. Αποτίμηση Απειλών

2.1. Ατομική Αποτίμηση Απειλών

Α/Α		**Αγαθό:**	
ΑΠΕΙΛΗ	**Επίπεδο Απειλής (ΠΧ - ΠΥ)**		**Βαθμός Απειλής (1-5)**

2.2. Ομαδική Αποτίμηση Απειλών

Ομάδα:		**Βάρος Ομάδας:**		**Αγαθό:**	
ΑΠΕΙΛΗ	**Επίπεδο Απειλής (ΠΧ - ΠΥ)**				**Βαθμός Απειλής (1-5)**

2.3. Συνολική Αποτίμηση Απειλών

Αγαθό:		
ΑΠΕΙΛΗ	**Επίπεδο Απειλής (ΠΧ - ΠΥ)**	**Βαθμός Απειλής (1-5)**
Αγαθό		
ΑΠΕΙΛΗ	**Επίπεδο Απειλής (ΠΧ - ΠΥ)**	**Βαθμός Απειλής (1-5)**

3. Αποτίμηση Αδυναμιών

3.1. Ατομική Αποτίμηση Αδυναμιών

Α/Α		**Αγαθό:**		**Απειλή:**	
ΑΔΥΝΑΜΙΑ	**Επίπεδο Αδυναμίας (Χ – Υ)**		**Βαθμός Αδυναμίας (1-3)**		

3.2. Ομαδική Αποτίμηση Αδυναμιών

Ομάδα:		**Βάρος Ομάδας:**		**Αγαθό:**		**Απειλή:**	
ΑΔΥΝΑΜΙΑ	**Επίπεδο Αδυναμίας (Χ – Υ)**			**Βαθμός Αδυναμίας (1-3)**			

3.3. Συνολική Αποτίμηση Αδυναμιών

Αγαθό:		**Απειλή:**	
ΑΔΥΝΑΜΙΑ	**Επίπεδο Αδυναμίας (Χ - Υ)**	**Βαθμός Αδυναμίας (1-3)**	
Αγαθό:		**Απειλή:**	
ΑΔΥΝΑΜΙΑ	**Επίπεδο Αδυναμίας (Χ – Υ)**	**Βαθμός Αδυναμίας (1-3)**	

4. Αποτελέσματα Επικινδυνότητας

4.1. Πίνακας αποτελεσμάτων ανά αγαθό

	Απειλή:								**Αγαθό:**							
Υπηρεσία	**Αποτίμηση Επιπτώσεων**								**Αποτίμηση Απειλών**		**Αποτίμη Αδυναμιών**		**Επικινδυνότητα**			
	Απώλεια Διαθεσιμότητας		**Απώλεια Ακεραιότητας**		**Απώλεια Εμπιστευτικότητας**		**Συνολικός Βαθμός**									
	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο Απειλής	Βαθμός Απειλής	Επίπεδο Αδυναμίας	Βαθμός Αδυναμίας	R_{un}	R_{mod}	R_{dis}	R

4.2. Πίνακας αποτελεσμάτων ανά απειλή

	Απειλή:																
Αγαθό	**Υπηρεσία**	**Αποτίμηση Επιπτώσεων**								**Αποτίμηση Απειλών**		**Αποτίμη Αδυναμιών**		**Επικινδυνότητα**			
		Απώλεια Διαθεσιμότητας		**Απώλεια Ακεραιότητας**		**Απώλεια Εμπιστευτικότητας**		**Συνολικός Βαθμός**									
		Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	Επίπεδο	Βαθμός	R_{un}	R_{mod}	R_{dis}	R

8.5.3 Αναφορά κατάλληλων μέτρων προστασίας

Στον συγκεκριμένο πίνακα συμπληρώνονται τα αποτελέσματα του βήματος 6.2: Επιλογή κατάλληλων μέτρων ασφάλειας της μεθοδολογίας STORM-RM. Συγκεκριμένα για κάθε αγαθό του υπό εξέταση ΠΣ καταγράφεται το μέτρο ασφάλειας και η υπο-πολιτική ασφάλειας (σύμφωνα με το Παράρτημα ΙΙ) καθώς και συμπληρώνεται ο βαθμός υλοποίησής τους με μία από τις καταστάσεις:

- ✓ άμεση υλοποίηση,
- ✓ προτεινόμενο για υλοποίηση,
- ✓ υπό συζήτηση,
- ✓ μη εφαρμόσιμο.

Μέτρα προστασίας			
Αγαθό	**Μέτρο**	**Υπο-πολιτική ασφάλειας**	**Βαθμός υλοποίησης**