Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Συγκριτική Μελέτη Ανάλυσης Επικινδυνότητας

Ευτυχία Χαλβατζή

Επιβλέπων: Δρ. Σωκράτης Κάτσικας
Καθηγητής Παν. Πειραιώς

Μάιος 2014

Εξεταστική Επιτροπή

Σωκράτης Κάτσικας,
Καθηγητής
Πανεπιστήμιο Πειραιώς

.....

Κωνσταντίνος Λαμπρινουδάκης
Επίκουρος Καθηγητής
Πανεπιστήμιο Πειραιώς

.....

Χρήστος Ξενάκης
Επίκουρος Καθηγητής
Πανεπιστήμιο Πειραιώς

.....

Πίνακας περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν με οποιονδήποτε τρόπο στην επιτυχή εκπόνηση αυτής της διπλωματικής εργασίας. Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Σωκράτη Κάτσικα για την επίβλεψη αυτής της διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω. Ήταν πάντα διαθέσιμος να μου προσφέρει τις γνώσεις και την εμπειρία του.

Στη συνέχεια, θα ήθελα να ευχαριστήσω ιδιαίτερα τον επίκουρο καθηγητή κ. Κωνσταντίνο Λαμπρινουδάκη, για το χρόνο του και τις πολύτιμες συμβουλές που μου παρείχε στην αρχή αυτής της διπλωματικής εργασίας.

Νιώθω επίσης την ανάγκη να ευχαριστήσω τον κ. Ευάγγελο Ρεκλείτη, υποψήφιο διδάκτορα του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, για την αποσαφήνιση ορισμένων σημείων της μεθόδου Cramm και γενικότερα για τις συμβουλές που μου παρείχε κατά τις φορές που ήρθαμε σε επικοινωνία.

Τέλος, θα ήθελα να ευχαριστήσω θερμά τα αγαπημένα μου πρόσωπα, τους φίλους μου και ιδιαίτερα τους γονείς μου, για την αμέριστη συμπαράστασή τους και την στήριξη των επιλογών μου.

Περίληψη

Η ραγδαία ανάπτυξη των τεχνολογιών πληροφορικής και η εκτεταμένη χρήση τους στο επιχειρησιακό περιβάλλον έχει διευκολύνει στο μέγιστο τη διεξαγωγή των επιχειρησιακών λειτουργιών, αλλά ταυτόχρονα έχει εισάγει πολλά σημαντικά ζητήματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων μιας επιχείρησης. Τα ζητήματα αυτά σχετίζονται κυρίως με τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των επιχειρησιακών πληροφοριών απέναντι στους κινδύνους που ελλοχεύουν και απειλούν τις τρεις αυτές βασικές αρχές ασφάλειας.

Οι προκλήσεις της εποχής στην οποία ζούμε αφορούν στη συμμόρφωση με νομικές και κανονιστικές διατάξεις, στη χρήση νέων τεχνολογιών, καθώς και στον ιδιαίτερα αυξημένο πλήθος νέων κινδύνων και χρηστών (κυρίως μη εκπαιδευμένων) σε ζητήματα ασφάλειας. Τα περιστατικά ασφάλειας συνεχώς αυξάνονται και αυτό οδηγεί στην αναζήτηση λύσεων για την προφύλαξη των δεδομένων, καθιστώντας πιο αναγκαίο από ποτέ το έργο της προστασίας των πληροφοριακών συστημάτων. Τη λύση στο παραπάνω πρόβλημα έρχεται να δώσει η ανάλυση επικινδυνότητας η οποία βοηθάει στον εντοπισμό, την εκτίμηση και την αξιολόγηση των κινδύνων, καθώς και στην παροχή της λήψης κατάλληλων αποφάσεων σε ότι αφορά τις ενέργειες που χρειάζεται να γίνουν για την αποτροπή ή τη μείωση του κινδύνου σε αποδεκτά επίπεδα.

Η παρούσα διπλωματική εργασία ασχολείται με την ανάλυση και διαχείριση της επικινδυνότητας και συγκεκριμένα με τη μελέτη και σύγκριση δύο μεθόδων ανάλυσης επικινδυνότητας. Μέσω αυτής της διαδικασίας δίνεται η δυνατότητα προσδιορισμού των κρίσιμων αγαθών – περιουσιακών στοιχείων (assets) ενός συστήματος, των δυνητικών απειλών (threats), των ευπαθειών (vulnerabilities) και προτείνονται κάποια αντίμετρα – μέτρα προστασίας (countermeasures) τα οποία εξασφαλίζουν την ασφαλέστερη λειτουργία του συστήματος.

Το σύστημα που χρησιμοποιήθηκε για τη μελέτη είναι ένα υπαρκτό πληροφοριακό σύστημα μιας εταιρείας του Ελλαδικού χώρου από την οποία έχει ζητηθεί να μην ανακοινωθεί η επωνυμία της. Η μελέτη έγινε με τη χρήση των μεθόδων CRAMM (CCTA Risk Analysis and Management Method) και OCTAVE Allegro (Operational Critical Threat, Asset, and Vulnerability Evaluation).

Αρχικά γίνεται μία περιγραφή της υποδομής που μελετήθηκε, περιγράφοντας αναλυτικά τα περιουσιακά στοιχεία της εν λόγω εταιρείας, μελετώνται οι απειλές που υφίσταται τα σύστημα και τα σημεία ευπάθειας που αυτά παρουσιάζουν και ακολούθως υπολογίζεται ο βαθμός

επικινδυνότητας του Πληροφοριακού Συστήματος. Στη συνέχεια αναπτύσσεται ένα ολοκληρωμένο σχέδιο ασφάλειας για την εταιρεία, το οποίο περιλαμβάνει τόσο τα προτεινόμενα αντίμετρα, όσο και την πολιτική ασφάλειας της εταιρείας. Τέλος παρουσιάζεται μία σύγκριση αυτών των δύο μεθόδων.

Abstract

The rapid development of information technology and its widespread use in the operational environment has facilitated maximum operational efficiency, but, at the same time, it has introduced many important issues concerning the security of information systems of an enterprise. These issues relate mainly to ensuring confidentiality, integrity and availability of business information against the risks lurking and threatening those three basic security principles.

The challenges of the times in which we live are related to compliance with laws and regulations, the use of new technologies, and in a particularly high number of new threats and new users on security issues (mostly untrained). Security incidents are increasing and this leads to finding solutions for the preservation of the data, making more necessary than ever the task of protecting information systems. The solution to the above problem is risk analysis which helps in identifying, assessing and evaluating the risks and the provision of adequate decisions (measures) in terms of the actions that need to be done to prevent or reduce the risk to acceptable levels.

This thesis deals with the analysis and management of risk and specifically to the study and comparison of two methods of risk analysis. This process enables the identification of the critical assets of a system, the potential threats, vulnerabilities and proposes some protection measures (countermeasures) that ensure the secure operation of the system.

The system that we used for the study is an existing IT system of a Greek company. The company management requested not to reveal the company's identity. The study was performed using the methods, namely CRAMM (CCTA Risk Analysis and Management Method) and OCTAVE Allegro (Operational Critical Threat, Asset and Vulnerability Evaluation).

Firstly, a description of the infrastructure that has been studied is given, whereby the assets of the company are described in detail; then we study the threats that the systems face and the relevant vulnerabilities. Subsequently we calculate the degree of risk of the Information System and we develop a comprehensive security plan for the company, that includes both the proposed countermeasures and the security policy of the company. Finally, we provide a comparison of these two risk analysis methods.

Κεφάλαιο 1

Εισαγωγή

Είναι φανερό ότι ζούμε σε μία εποχή όπου όλα κινούνται προς την ψηφιοποίηση. Όλες οι εταιρείες ανεξάρτητα από το πεδίο δραστηριότητάς τους χρησιμοποιούν σε καθημερινή βάση αυτοματοποιημένα συστήματα Τεχνολογιών Πληροφορικής καθιστώντας το Πληροφοριακό τους Σύστημα κρίσιμο στοιχείο της υποδομής τους. Για την επίτευξη της αποτελεσματικής λειτουργίας οι εταιρείες θα πρέπει να διασφαλίσουν την επιχειρησιακή τους συνέχεια, ελαχιστοποιώντας τις πιθανότητες πρόκλησης ζημιάς και μεγιστοποιώντας παράλληλα την απόδοση των επενδύσεων και των επιχειρησιακών ευκαιριών.

Η διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας είναι ένα σημαντικό συστατικό ενός επιτυχημένου προγράμματος για την ασφάλεια των πληροφοριακών συστημάτων. Ο κύριος στόχος της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας δεν είναι μόνο η προστασία των περιουσιακών στοιχείων (assets) αλλά και η προστασία του οργανισμού σε ότι αφορά στην ικανότητά του να εκτελεί την αποστολή του. Ως εκ τούτου, η διαδικασία διαχείρισης του κινδύνου δεν θα πρέπει να αντιμετωπίζεται ως μια τεχνική λειτουργία, αλλά ως βασική λειτουργία της διαχείρισης της εταιρείας.

1. Έννοιες και Ορισμοί

Στην παρούσα μελέτη χρησιμοποιούνται διάφορες έννοιες που αφορούν στην Ασφάλεια Πληροφοριακών Συστημάτων και ειδικότερα στην Ανάλυση και Διαχείριση της Επικινδυνότητας. Ορισμένες από τις πιο συχνά χρησιμοποιούμενες έννοιες [1], [2] παρατίθενται στον παρακάτω πίνακα (Πίνακας 1).

Βασικές Έννοιες	Ορισμοί
Πληροφοριακό Σύστημα - Π.Σ. (Information System IS)	Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας εταιρείας ή ενός οργανισμού.
Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.

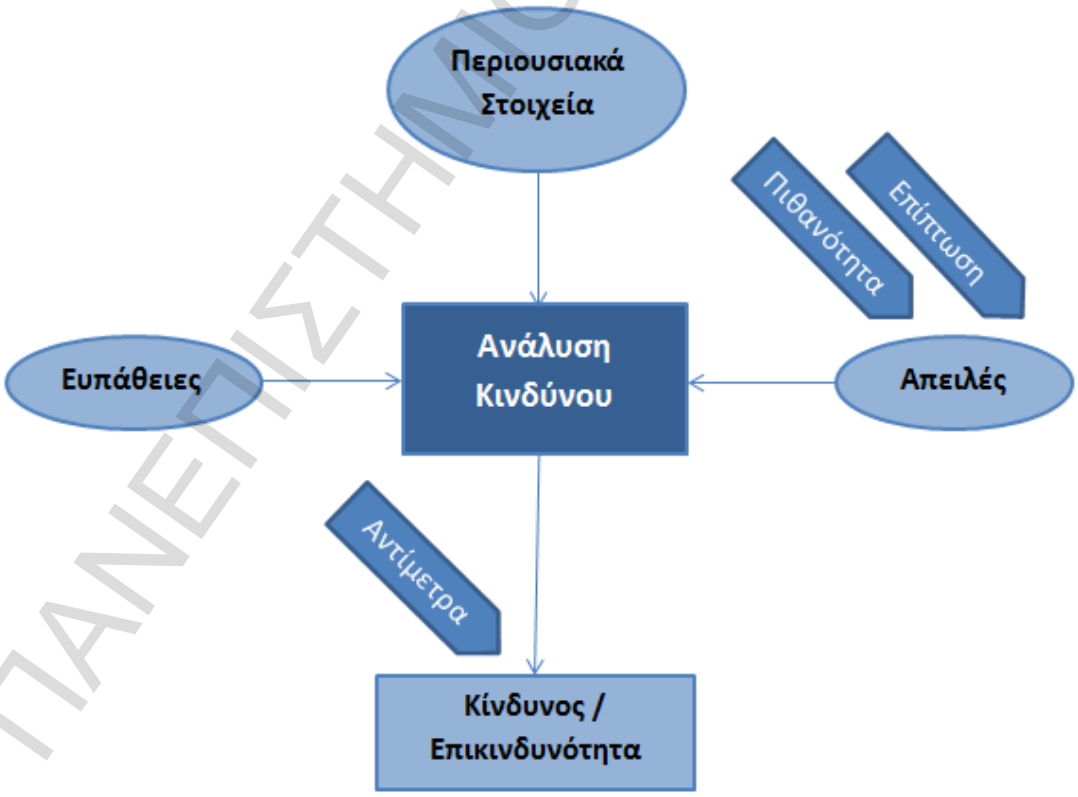
Βασικές Έννοιες	Ορισμοί
Ασφάλεια Πληροφοριακού Συστήματος (IS Security)	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται, για να προστατευθούν τόσο τα στοιχεία του Πληροφοριακού Συστήματος όσο και ολόκληρο το Πληροφοριακό Σύστημα από τυχαία ή σκόπιμη απειλή.
Εμπιστευτικότητα (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.
Αυθεντικοποίηση (Authentication)	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της γνησιότητας της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.
Απειλή (Threat)	Μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος.
Ζημιά (Damage)	Η απώλεια, μερική ή ολική, της αξίας ενός περιουσιακού στοιχείου-αγαθού.
Παραβίαση (Breach)	Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες: αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
Περιστατικό (Incident)	Ένα γεγονός, το οποίο έχει ως συνέπεια μία παραβίαση ή που αποτελεί μία απόπειρα παραβίασης ή που θέτει σε κίνδυνο την ασφάλεια ενός Πληροφοριακού Συστήματος.
Ευπάθεια – Αδυναμία (Vulnerability)	Σημείο ενός Πληροφοριακού Συστήματος που μπορεί να επιτρέψει να συμβεί μία παραβίαση.
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης.
Επικινδυνότητα- Κίνδυνος (Risk)	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.
Μέτρο Προστασίας –Αντίμετρο (Countermeasures)	Μέτρο σχεδιασμένο για να εμποδίσει μία παραβίαση ή να μειώσει μία αδυναμία-σημείο ευπάθειας ή να μειώσει τις δυνητικές επιπτώσεις.
Πολιτική Ασφάλειας (Security Policy)	Περιγραφή σε γενικό-αφαιρετικό 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 περιουσιακών στοιχείων.

Βασικές Έννοιες	Ορισμοί
Σχέδιο Ασφαλείας (Security Plan)	Περιγράφει τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται ή πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων που αναφέρονται στην πολιτική ασφαλείας, όπως επίσης και οι απαραίτητες ενέργειες για την υλοποίησή τους.
Σχέδιο Ανάκαμψης από καταστροφές (Disaster Recovery and Contingency Plan)	Αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/εισβολές, κ.λπ. Το Σχέδιο αυτό συμπληρώνει το Σχέδιο Ασφαλείας τους.

Πίνακας 1: Έννοιες και Ορισμοί

2. Ανάλυση Κινδύνων –Επικινδυνότητας

Η πιθανή απώλεια των αγαθών – περιουσιακών στοιχείων (assets) μιας εταιρείας ή ενός οργανισμού λόγω της εκμετάλλευσης μιας ευπάθειας από μια απειλή, ονομάζεται κίνδυνος ασφάλειας (security risk).



Εικόνα 1: Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών.

Σκοπός της ανάλυσης κινδύνου (risk analysis) είναι ο υπολογισμός της πιθανότητας εμφάνισης ενός ανεπιθύμητου γεγονότος και των επιπτώσεων που μπορεί να έχει αυτός ο κίνδυνος σε περίπτωση εκδήλωσής του. Έχοντας καλή γνώση του κινδύνου, μπορεί κάποιος να αποφασίσει ευκολότερα και σωστότερα για το αν θα αποδεχτεί τον κίνδυνο, έτσι όπως έχει αποτιμηθεί, ή αν θα προβεί σε διορθωτικές ενέργειες που θα τον αποτρέψουν ή θα τον μειώσουν σε αποδεκτά επίπεδα, διασφαλίζοντας την προστασία των περιουσιακών στοιχείων του Πληροφοριακού Συστήματος. Στην παρούσα μελέτη παρουσιάζονται οι τρόποι σύμφωνα με τους οποίους θα εντοπιστούν, θα εκτιμηθούν και θα μειωθούν οι κίνδυνοι αυτοί.

Ο κίνδυνος για την ασφάλεια (και ο υπολειπόμενος κίνδυνος) είναι το βασικό στοιχείο της αξιολόγησης κινδύνων της ασφάλειας πληροφοριών, διότι είναι το αποκορύφωμα όλων των άλλων εκτιμήσεων, υπολογισμών και αναλύσεων. Τα υπόλοιπα στοιχεία είναι απλά απαιτούμενα ώστε να καταλήξουμε στην μέτρηση του κινδύνου ασφάλειας.

Αναφορικά με τους κινδύνους ασφάλειας υπάρχουν πολλοί κρίσιμοι παράγοντες που πρέπει να ληφθούν υπόψη. Ο σημαντικότερος από αυτούς και αυτός που θα μας απασχολήσει αυτή τη στιγμή είναι ο τρόπος που παρουσιάζεται ένας κίνδυνος, καθώς και η προέλευσή του. Γενικότερα υπάρχουν πολλές προσεγγίσεις σύμφωνα με τις οποίες μπορεί να παρουσιαστεί ένας κίνδυνος. Οι προσεγγίσεις αυτές διαχωρίζονται σε ποσοτικές ή ποιοτικές [3], [4]:

Η ***ποσοτική ανάλυση*** σχετίζεται με συγκεκριμένους τύπους και υπολογισμούς που οριοθετούν την αξία του κινδύνου ασφάλειας. Μια ποσοτική προσέγγιση στον προσδιορισμό και την παρουσίαση του κινδύνου ασφάλειας έχει το πλεονέκτημα της αντικειμενικότητας και της έκφρασης σε απόλυτα χρηματικά μεγέθη. Παρόλα αυτά, τέτοιες ποσοτικές εκτιμήσεις μπορεί να είναι σχετικά πολύπλοκες και οι ακριβείς τιμές των μεταβλητών που χρησιμοποιούνται στους τύπους των υπολογισμών, είναι δύσκολο να καθοριστούν.

Η ***ποιοτική ανάλυση*** βασίζεται σε υποκειμενικές εκτιμήσεις της αξίας των περιουσιακών στοιχείων, των απειλών, των ευπαθειών, και τελικά του κινδύνου. Μια ποιοτική προσέγγιση στον προσδιορισμό και την παρουσίαση του κινδύνου ασφάλειας έχει το πλεονέκτημα της εύκολης εφαρμογής. Επιπλέον, σε πολλές περιπτώσεις προσφέρει ικανοποιητική προσέγγιση του κινδύνου.

Μεταξύ των δύο προσεγγίσεων, η ποσοτική ανάλυση ήταν αρχικά πιο δημοφιλής, όμως τα τελευταία χρόνια άρχισε να προτιμάται η ποιοτική ανάλυση, διότι απαιτεί λιγότερο χρόνο και προσπάθεια για υλοποίηση. Στην παρούσα μελέτη και οι δύο μέθοδοι που παρουσιάζονται είναι ποιοτικές.

<table>
<tr><th>Έννοια</th><th colspan="2">Ορισμός</th></tr>
<tr><td rowspan="3">Ποσοτική Ανάλυση Κινδύνου

(Quantitative Risk)</td><td colspan="2">Μέθοδος προσδιορισμού και παρουσίασης των κίνδυνων ασφάλειας Πληροφοριακών Συστημάτων που βασίζεται σε συγκεκριμένους τύπους και υπολογισμούς για τον καθορισμό της αξίας των κινδύνων.</td></tr>
<tr><td>Πλεονεκτήματα</td><td>Μειονεκτήματα</td></tr>
<tr><td>Αντικειμενική εκτίμηση: Ο κίνδυνος ασφάλειας εκφράζεται σε καθαρό χρηματικό ποσό. Ο κίνδυνος μπορεί να γίνει κατανοητός από τη Διοίκηση της εταιρείας.</td><td>Οι υπολογισμοί των κινδύνων είναι πολύπλοκοι: είναι δύσκολο να καθοριστούν ακριβείς τιμές. Απαιτείται πολύς χρόνος για την ανάλυση.</td></tr>
<tr><td rowspan="3">Ποιοτική Ανάλυση Κινδύνου

(Qualitative Risk)</td><td colspan="2">Μέθοδος προσδιορισμού και παρουσίασης των κίνδυνων ασφάλειας Πληροφοριακών Συστημάτων που βασίζεται σε υποκειμενικές μετρήσεις της αποτίμησης των περιουσιακών στοιχείων, των απειλών, των ευπαθειών και τελικά του συνολικού κινδύνου.</td></tr>
<tr><td>Πλεονεκτήματα</td><td>Μειονεκτήματα</td></tr>
<tr><td>Είναι εύκολα κατανοητή και παρέχει μιαικανοποιητική εκτίμηση του κινδύνου ασφάλειας. Επιπλέον, είναι αρκετά ευέλικτη και απαιτεί λιγότερο χρόνο και λιγότερους πόρους.</td><td>Είναι υποκειμενική εκτίμηση. Δεν γίνεται μεγάλη προσπάθεια για την αναγνώριση της αντικειμενικής αξίας των περιουσιακών στοιχείων.</td></tr>
</table>

Πίνακας 2: Πλεονεκτήματα / Μειονεκτήματα Ποιοτικής και Ποσοτικής Ανάλυσης

3. Μέθοδοι Ανάλυσης και Διαχείρισης Επικινδυνότητας

Αρκετές φορές ο όγκος των περιουσιακών στοιχείων ενός προς εξέταση συστήματος, είναι αρκετά μεγάλος, με αποτέλεσμα η διαδικασία να είναι δύσκολη για τον αναλυτή. Γι' αυτό το σκοπό υπάρχουν πολλά μοντέλα αξιολόγησης του κινδύνου και κάθε μέρα εμφανίζονται όλο και περισσότερα, έχοντας όλα τον ίδιο βασικό στόχο, αλλά προσεγγίζοντάς τον με διαφορετικό τρόπο. Μερικές προσεγγίσεις μπορούν να εφαρμοστούν σε όλους τους τύπους κινδύνων, ενώ άλλες αφορούν συγκεκριμένους κινδύνους.

Μία εταιρεία πρέπει να επιλέξει την πιο κατάλληλη μέθοδο με βάση το πεδίο δραστηριότητας, την πολυπλοκότητα των Πληροφοριακών Συστημάτων, την εμπειρία των αναλυτών, τον υπάρχοντα προϋπολογισμό για την ασφάλεια των πληροφοριακών συστημάτων και την γενικότερη κουλτούρα της.

Στη παρούσα μελέτη παρουσιάζεται η συγκριτική αξιολόγηση της μεθόδου CRAMM με την μέθοδο OCTAVE Allegro, έτσι ώστε να γίνει η επιλογή της πιο κατάλληλης για το Πληροφοριακό Σύστημα (εφεξής Π.Σ.) της εταιρείας.

Κεφάλαιο 2

Η Μέθοδος CRAMM

Η CRAMM (CCTA Risk Analysis and Management Methodology) [5], [6], είναι μία μέθοδος ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (Central Computer and Telecommunications Agency) του Ηνωμένου Βασιλείου το 1987, για να παρέχει στις κρατικές υπηρεσίες της χώρας ένα τρόπο για τον έλεγχο της ασφάλειας των πληροφοριακών συστημάτων. Μπορεί να εφαρμοστεί σε όλους τους τύπους των συστημάτων και σε όλα τα στάδια του κύκλου ζωής ενός Πληροφοριακού Συστήματος. Επίσης διαθέτει αυτοματοποιημένο εργαλείο λογισμικού [7] το οποίο υποστηρίζει όλα τα στάδια της εφαρμογής της.

2.1. Στάδια Μεθόδου

Η μεθοδολογία αποτελείται από τρία βασικά στάδια και το καθένα από αυτά περιλαμβάνει κάποια βασικά βήματα τα οποία περιγράφονται παρακάτω [8], [9]:

Στάδιο 1: Προσδιορισμός και Αξιολόγηση των Περιουσιακών Στοιχείων (Identification and Valuation of Assets)

Το πρώτο στάδιο αναφέρεται στον Προσδιορισμό και την Αξιολόγηση των Στοιχείων του Πληροφοριακού Συστήματος που χρήζουν προστασίας και αποτελείται από τα εξής βήματα:

Βήμα 1.1: Περιγραφή Πληροφοριακών Συστημάτων και Εγκαταστάσεων

Τα στοιχεία που απαιτούν προστασία είναι κυρίως τα δεδομένα, το λογισμικό και το υλικό του Π.Σ. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση. Για παράδειγμα, τα δεδομένα τυγχάνουν επεξεργασίας από το λογισμικό, το οποίο υποστηρίζεται από στοιχεία του υλικού, όπως υπολογιστές, δικτυακός εξοπλισμός και περιφερειακά. Η προστασία των δεδομένων προϋποθέτει την προστασία του λογισμικού και του υλικού όπου αυτά αποθηκεύονται και επεξεργάζονται.

Βήμα 1.2: Αποτίμηση Περιουσιακών Στοιχείων Πληροφοριακού Συστήματος

Ο στόχος αυτού του βήματος είναι ο προσδιορισμός της σπουδαιότητας που έχουν τα δεδομένα για τον οργανισμό. Έτσι, μπορούμε να εντοπίσουμε εκείνες τις κατηγορίες δεδομένων που χρήζουν ιδιαίτερης προστασίας και συγκεκριμένα το είδος της προστασίας που απαιτείται.

Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την Επίπτωση (impact) που θα είχε η απώλεια των δεδομένων. Συγκεκριμένα εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις της καταστροφής, της μη-εξουσιοδοτημένης μεταβολής (modification), της αποκάλυψης (disclosure) και της μη-διαθεσιμότητας (unavailability). Για κάθε περίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται αριθμητικά με βάση κλίμακα 1-10 και με χρήση οδηγιών (guidelines) που παρέχει η μέθοδος. Στη συνέχεια η CRAMM, μέσω του αυτοματοποιημένου εργαλείου, υπολογίζει την έμμεση αξία (implied value) των στοιχείων των πληροφοριακών συστημάτων.

Βήμα 1.3: Επιβεβαίωση και Επικύρωση της Αποτίμησης

Η αποτίμηση των στοιχείων του Π.Σ. αποτελεί κρίσιμο παράγοντα για τη διεξαγωγή της Ανάλυσης Επικινδυνότητας. Σε αυτό το σημείο ο αναλυτής παρουσιάζει με τη μορφή έκθεσης τα αποτελέσματα του πρώτου σταδίου σε αρμόδια στελέχη της εταιρείας και γίνεται επικύρωση των αποτελεσμάτων.

Στάδιο 2: Ανάλυση Επικινδυνότητας (Risk Analysis)

Το δεύτερο στάδιο αφορά στην Ανάλυση της Επικινδυνότητας του Π.Σ. Τα επιμέρους βήματα του σταδίου είναι τα εξής:

Βήμα 2.1: Προσδιορισμός των Απειλών που αφορούν κάθε Περιουσιακό Στοιχείο

Η μέθοδος σε αυτό το σημείο επικεντρώνεται στον προσδιορισμό συγκεκριμένων Απειλών για κάθε περιουσιακό στοιχείο του Π.Σ. Η CRAMM παρέχει έναν ενδεικτικό κατάλογο Απειλών, καθώς και συστάσεις για το ποιες κατηγορίες Περιουσιακών Στοιχείων ενός Π.Σ. απειλούνται συνήθως από τη συγκεκριμένη Απειλή. Με αυτό τον τρόπο, σε περίπτωση όπου ένα από τα περιουσιακά στοιχεία του Π.Σ. αντιμετωπίζει μία Απειλή, τότε υπολογίζεται ότι και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια Απειλή. Αυτό κάνει

την δουλειά του αναλυτή πιο εύκολη, καθώς δεν χρειάζεται να υπολογίζει ο ίδιος όλες τις συσχετίσεις.

Βήμα 2.2: Εκτίμηση Απειλών και Αδυναμιών

Για κάθε συνδυασμό Απειλής - Περιουσιακού Στοιχείου γίνεται εκτίμηση του μεγέθους της Απειλής και της σοβαρότητας των Αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίησή της. Η εκτίμηση της Απειλής γίνεται αυτόματα από το εργαλείο και ακολουθεί την κλίμακα 1-5 (very low, low, medium, high, very high), με βάση τις απαντήσεις που δόθηκαν σε δομημένα ερωτηματολόγια που έχουν παραχθεί από την CRAMM. Αντίστοιχα για τις Αδυναμίες, συμπληρώνονται από τον αναλυτή τα ερωτηματολόγια των Αδυναμιών και υπολογίζεται η σοβαρότητα της Αδυναμίας στην κλίμακα 1-3 (low, medium, high). Οι απαντήσεις που θα δοθούν στα ερωτηματολόγια προκύπτουν από τα στοιχεία που συλλέγουν οι αναλυτές από τους χρήστες του συστήματος. Το εργαλείο παρέχει ερωτηματολόγια για κάθε συνδυασμό Απειλής-Αγαθού. Οι απαντήσεις των ερωτηματολογίων εισάγονται στο εργαλείο και εκείνο υπολογίζει το επίπεδο των Απειλών και των Αδυναμιών. Επίσης, παρέχει τη δυνατότητα στους αναλυτές να αλλάξουν τις τιμές που υπολογίστηκαν αυτόματα.

Βήμα 2.3: Υπολογισμός Επικινδυνότητας Συνδυασμών Περιουσιακό Στοιχείο – Απειλή - Αδυναμία

Η CRAMM υπολογίζει το Βαθμό Επικινδυνότητας για κάθε συνδυασμό Περιουσιακού Στοιχείου – Απειλής - Αδυναμίας. Δεν έχουμε, δηλαδή, απλώς ένα Βαθμό Επικινδυνότητας για το Π.Σ. στο σύνολό του, αλλά έχουμε συγκεκριμένη αποτίμηση της επικινδυνότητας για κάθε επιμέρους συνδυασμό Περιουσιακού Στοιχείου – Απειλής - Αδυναμίας. Για το σκοπό αυτό, χρησιμοποιούνται τόσο τα αποτελέσματα της εκτίμησης των Απειλών και των Αδυναμιών, όσο και το μοντέλο του συστήματος που έχει δημιουργηθεί από το πρώτο στάδιο. Έτσι, ο Βαθμός Επικινδυνότητας λαμβάνει υπόψη και τη συσχέτιση μεταξύ των Περιουσιακών Στοιχείων του Π.Σ. Ουσιαστικά ο Βαθμός Επικινδυνότητας απεικονίζει τις απαιτήσεις ασφάλειας για κάθε Περιουσιακό Στοιχείο του Π.Σ., καθώς μεγαλύτερη επικινδυνότητα συνεπάγεται και υψηλότερη απαίτηση για ασφάλεια. Ο Βαθμός Επικινδυνότητας υπολογίζεται από το εργαλείο και ακολουθεί την κλίμακα 1-7. Σε αυτό το σημείο ο αναλυτής έχει τη δυνατότητα να παρέμβει και να αλλάξει κάποιες τιμές, αν το θεωρεί σκόπιμο. Το πλήθος των συνδυασμών Αγαθού-Απειλής

και κυρίως η πολυπλοκότητα της αλληλοσυσχέτισης των Αγαθών στα πλαίσια ενός Π.Σ., κάνουν πρακτικά αδύνατο τον εμπειρικό και χειρογραφικό υπολογισμό της επικινδυνότητας.

Βήμα 2.4: Αποτίμηση Βαθμού Επικινδυνότητας

Ο αναλυτής μπορεί να χρησιμοποιήσει τις αναφορές που παράγει το λογισμικό της CRAMM και το εργαλείο back-track για να εξετάσει συνολικά το βαθμό επικινδυνότητας. Σε περίπτωση που κριθεί ότι χρειάζεται να γίνουν κάποιες αλλαγές, τότε ο αναλυτής έχει τη δυνατότητα είτε να αλλάξει τις τιμές της επικινδυνότητας, είτε να αλλάξει τις τιμές που έχουν προκύψει από την εκτίμηση των απειλών και αδυναμιών και να υπολογίσει εκ νέου την επικινδυνότητα. Ο Βαθμός Επικινδυνότητας θα χρησιμοποιηθεί στο επόμενο στάδιο για την επιλογή των Αντιμέτρων.

Στάδιο 3: Διαχείριση Επικινδυνότητας (Risk Management)

Με βάση τα αποτελέσματα της Ανάλυσης Επικινδυνότητας του δεύτερου σταδίου η CRAMM παράγει ένα προτεινόμενο Σχέδιο Ασφάλειας (security plan). Αυτό αποτελείται από μία σειρά Αντιμέτρων, τα οποία θεωρούνται απαραίτητα για τη Διαχείριση της Επικινδυνότητας και θα πρέπει να εφαρμοστούν στο Π.Σ.. Έτσι, το τρίτο στάδιο περιλαμβάνει τον προσδιορισμό των προτεινόμενων αντιμέτρων και το Σχέδιο Ασφάλειας των Πληροφοριακών Συστημάτων:

Βήμα 3.1: Προσδιορισμός Προτεινόμενων Αντιμέτρων

Το λογισμικό της CRAMM διαθέτει μία βάση με τεχνικά, διοικητικά και οργανωτικά αντίμετρα. Τα αντίμετρα επιλέγονται αυτόματα από την προτεινόμενη βάση και χωρίζονται σε ομάδες ανάλογα με το είδος των Απειλών και των Περιουσιακών Στοιχείων του Π.Σ.

Βήμα 3.2: Σχέδιο Ασφάλειας Πληροφοριακού Συστήματος

Κατά τη διάρκεια του συγκεκριμένου βήματος, ο αναλυτής συγγράφει το Σχέδιο Ασφάλειας, που περιλαμβάνει το Σχέδιο Πολιτικής Ασφάλειας, τα Μέτρα Ασφάλειας και την Στρατηγική για την εφαρμογή του Σχεδίου Ασφάλειας.

2.2. Εφαρμογή της Μεθόδου CRAMM

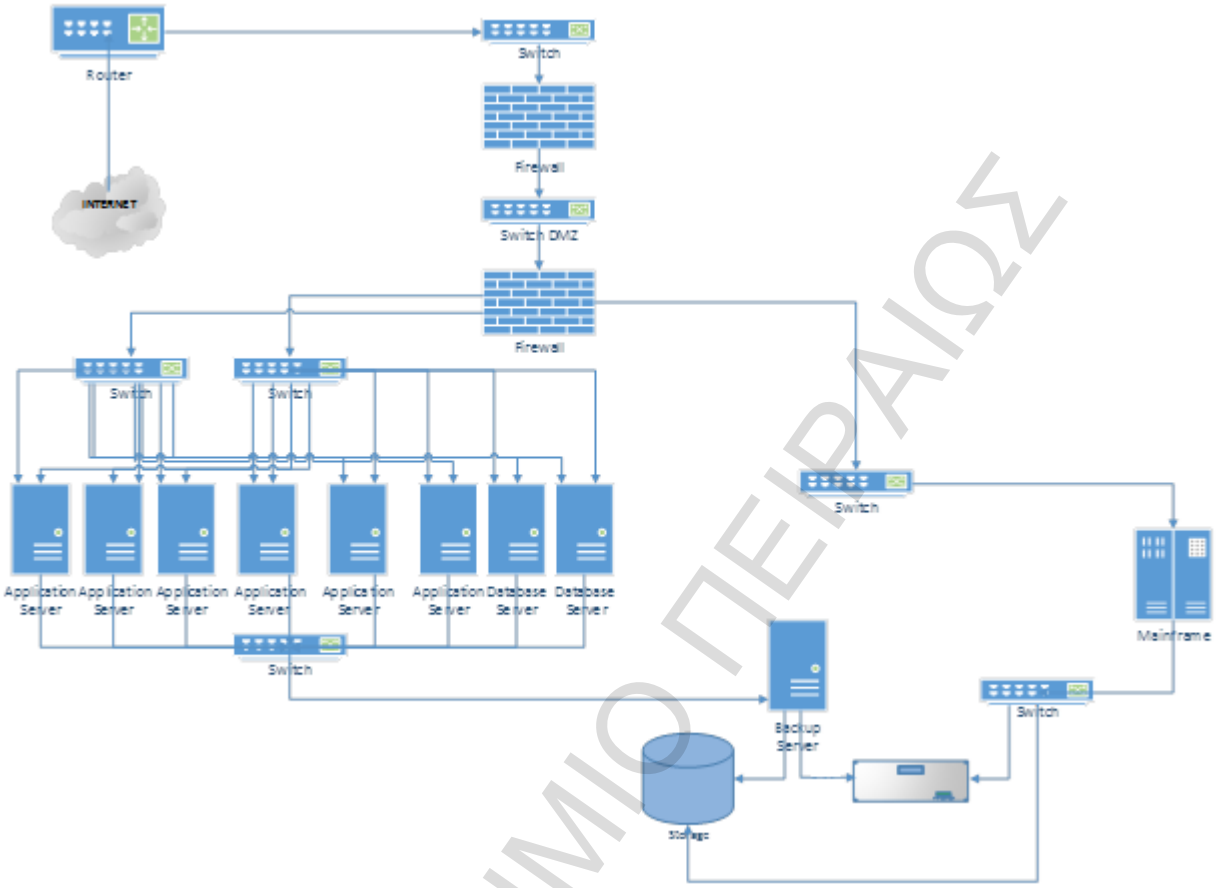
Για την συλλογή των απαραίτητων στοιχείων του Π.Σ. υπήρξε ένας κύκλος συνεντεύξεων με τα αρμόδια άτομα της εταιρείας, έτσι ώστε να είμαστε σε θέση να κατανοήσουμε το Π.Σ., συνεπώς και τα περιουσιακά στοιχεία του και να καθορίσουμε το εύρος της μελέτης. Εξαιτίας του μεγάλου μεγέθους του Π.Σ. έχουν επιλεγεί μόνο συγκεκριμένα συστήματα για μελέτη. Σε αυτό το στάδιο γίνεται καταγραφή του υλικού, του λογισμικού και των εγκαταστάσεων της εταιρείας.

2.2.1. Πληροφοριακό Σύστημα

Υλικός Εξοπλισμός (Hardware)

Το αρχικό και πιο σημαντικό βήμα είναι να καθορίσουμε τον υλικό εξοπλισμό του Π.Σ., δηλαδή τους υπολογιστές, το δίκτυο, τα μέσα αποθήκευσης κ.τ.λ. Η φυσική αρχιτεκτονική του δικτύου απεικονίζεται στην Εικόνα 2.

- Mainframe της IBM Z10, λειτουργικό σύστημα z/OS (zero downtime).
- Δύο Εξυπηρετητές Βάσεων Δεδομένων (Database servers) DELL PowerEdge R 900 Redhat Enterprise Linux 4.6 64 bit, σε διάταξη active-active.
- Τέσσερεις Εξυπηρετητές εφαρμογών (Application Servers) DELL PowerEdge 2950 Redhat Enterprise Linux 4.6 64 bit, σε διάταξη active-active.
- Ένας Εξυπηρετητής Εφαρμογών (Application server) Windows 2008 R2.
- Δύο συστήματα ασφαλείας Microsoft’s Threat management Gateway (TMG), που προσφέρουν firewall.
- Ένα σύστημα ασφαλείας Check Point το οποίο χρησιμοποιείται ως Proxy και ως URL filtering.
- Δύο μεταγωγείς (switches) Cisco 3750.
- Πέντε μεταγωγείς (switches) Dell Power Connect 2708, εκ των οποίων οι τρεις λειτουργούν και ως δρομολογητές.
- Δύο συσκευές λήψης αντιγράφων ασφάλειας, NetBackup 7.5 της εταιρείας Symantec.
- Τρείς μονάδες αδιάλειπτης παροχής ισχύος (UPS) Chloride 70-Net, μέγιστης υποστηριζόμενης ισχύς 50-60 kVA.
- Μία γεννήτρια πετρελαίου Sunlight μοντέλο SIS-160KVA SOUNDPROUFED 1500/G.



Εικόνα 2: Αρχιτεκτονική Δικτύου

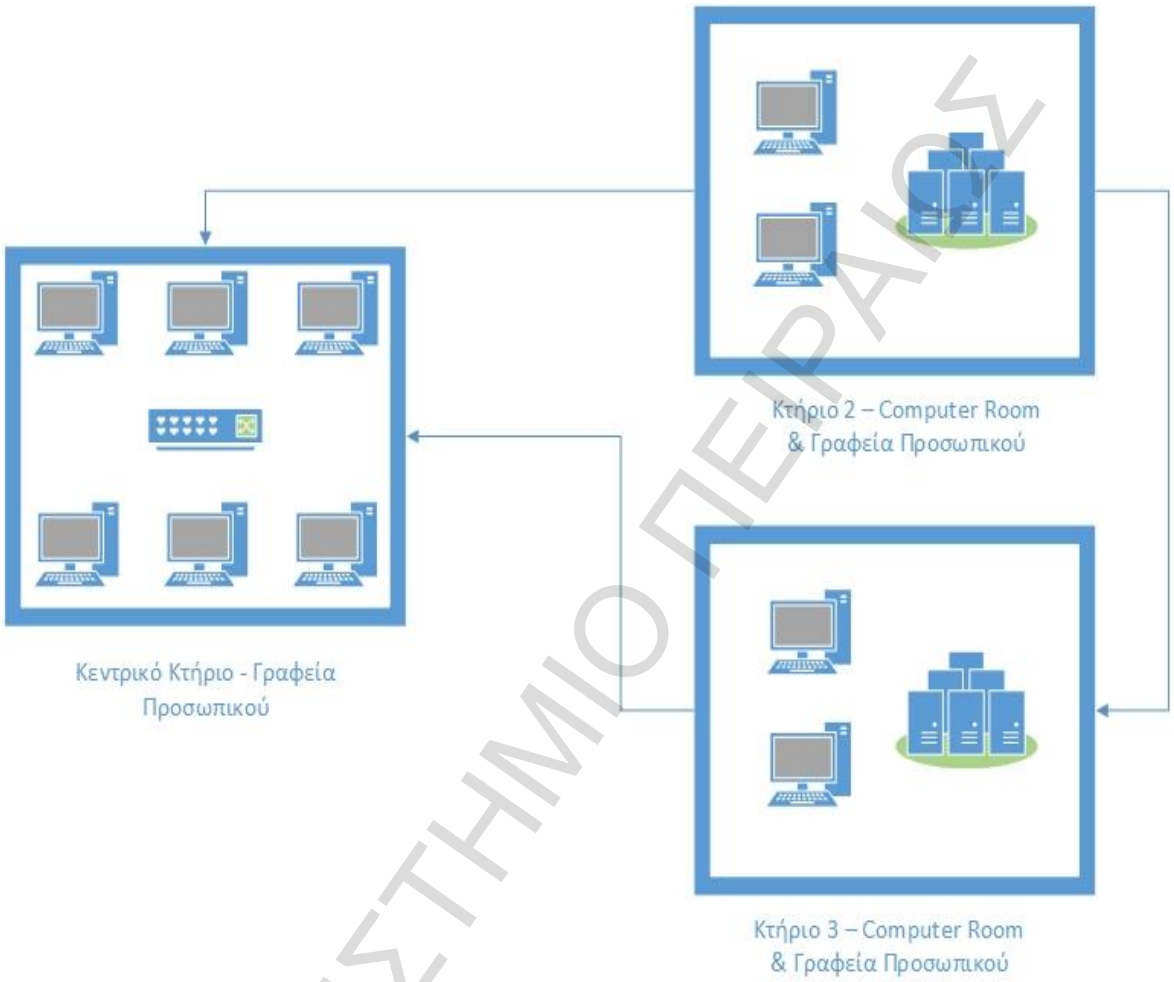
Κτηριακές Εγκαταστάσεις

Οι τοποθεσίες που περιλαμβάνονται στη μελέτη απεικονίζονται στην Εικόνα 3. Στη μελέτη έχουν συμπεριληφθεί:

- το κεντρικό κτήριο της εταιρείας, στο οποίο υπάρχουν μόνο γραφεία προσωπικού,
- το δεύτερο κτήριο, στο οποίο υπάρχει ένα computer room και κάποια γραφεία προσωπικού και
- το τρίτο κτήριο της εταιρείας, όπου στεγάζεται το δεύτερο computer room με εφεδρικά συστήματα (disaster site) και γραφεία προσωπικού.

Επίσης, υπάρχουν και κάποια επιπλέον κτήρια που δεν έχουν συμπεριληφθεί στη μελέτη καθώς είναι ίδια με το κεντρικό κτήριο, οπότε δεν κρίθηκε αναγκαία η περιγραφή τους. Ο

καθορισμός των κτηριακών εγκαταστάσεων απαιτείται καθώς στην παρούσα μελέτη λαμβάνονται υπόψη και οι κίνδυνοι από φυσικές και περιβαλλοντικές καταστροφές.



Εικόνα 3: Κτηριακές Εγκαταστάσεις

Λογισμικό – Εφαρμογές

Το Π.Σ. που μελετάται αποτελείται από αρκετές εφαρμογές, αλλά στην παρούσα μελέτη αποφασίστηκε να συμπεριληφθούν οι ακόλουθες τέσσερις πιο σημαντικές:

- Εφαρμογή του Συστήματος Πελατών,
- Εφαρμογή του Συστήματος Οικονομικής και Λογιστικής Διαχείρισης,
- Εφαρμογή του Συστήματος Διαχείρισης Εγγράφων και Πρωτοκόλλου,
- Εφαρμογή του Συστήματος Διαχείρισης Προσωπικού.

1. Σύστημα Πελατών

Το σύστημα πελατών θεωρείται το πιο κρίσιμο σύστημα της εταιρείας. Η εφαρμογή του συστήματος πελατών έχει δημιουργηθεί ειδικά για τη συγκεκριμένη εταιρεία και σκοπός της είναι η υποστήριξη των λειτουργικών απαιτήσεων της Διεύθυνσης Πωλήσεων. Συγκεκριμένα, η εφαρμογή περιλαμβάνει τα εξής:

- Διαχείριση πελατών,
- Διαχείριση μετρητών,
- Πληρωμή και παρακολούθηση πληρωμών (λογαριασμών),
- Τιμολόγηση και έκδοση λογαριασμού,
- Παρακολούθηση διακοπών-αποκοπών,
- Παρακολούθηση ενδείξεων,
- Λογιστική παρακολούθηση,
- Έκδοση αναφορών και στατιστικών,
- Είσπραξη εισφορών για θυγατρικές εταιρείες.

2. Σύστημα Οικονομικής και Λογιστικής Διαχείρισης

Σκοπός του συστήματος είναι να υποστηρίξει το Οικονομικό και Λογιστικό τμήμα της εταιρείας, έτσι ώστε να καλύπτονται οι λειτουργικές του απαιτήσεις όσον αφορά τα ακόλουθα:

- Κατάρτιση και εκτέλεση του προϋπολογισμού της εταιρείας,
- Αξιοποίηση όλων των δυνατοτήτων για τη δημιουργία και απόκτηση εσόδων,
- Βεβαίωση των επιβαλλόμενων προστίμων, τελών, δικαιωμάτων και εισφορών,
- Διαχείριση και εκτέλεση προμηθειών,
- Καταγραφή της περιουσίας της εταιρείας,
- Λογιστική και ταμειακή διαχείριση της εταιρείας,
- Τήρηση και συμφωνία των τραπεζικών λογαριασμών,
- Τήρηση του διπλογραφικού συστήματος,
- Διαχείριση αποθηκών και παγίων.

Οι παραπάνω λειτουργικές απαιτήσεις που διαθέτει το σύστημα Οικονομικής και Λογιστικής διαχείρισης καλύπτονται μέσω των ακόλουθων εφαρμογών:

- Γενική – Αναλυτική Λογιστική
- Διαχείριση Προϋπολογισμού
- Διαχείριση Κεφαλαίων
- Διαχείριση Εισπράξεων / Πληρωμών
- Διαχείριση Προμηθειών / Αποθήκης
- Διαχείριση Πάγιων Στοιχείων
- Τήρηση Λογιστικών Βιβλίων και Καταστάσεων
- Λογιστική Διαχείριση Έργων.

3. Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου

Σκοπός του συστήματος Διαχείρισης Εγγράφων και Πρωτοκόλλου είναι η υποστήριξη των λειτουργικών απαιτήσεων της γραμματείας του Μηχανογραφικού Κέντρου της εταιρείας. Το ίδιο σύστημα χρησιμοποιείται από όλες τις γραμματείες της εταιρείας. Μέσω της εφαρμογής γίνεται πρωτοκόλληση εισερχόμενων και εξερχόμενων εγγράφων, έτσι ώστε να εξασφαλίζεται η ορθή απόδοση μοναδιαίου αριθμού πρωτοκόλλου στα έγγραφα και ακολουθεί δρομολόγηση αυτών σε συγκεκριμένους αποδέκτες ή σε ομάδες αποδεκτών. Επιπλέον, γίνεται έλεγχος για διπλές αριθμήσεις και διπλές καταχωρήσεις εγγράφων.

4. Σύστημα Διαχείρισης Προσωπικού

Σκοπός του συστήματος Διαχείρισης Προσωπικού είναι η υποστήριξη των λειτουργικών απαιτήσεων του τμήματος Προσωπικού της εταιρείας. Το τμήμα αυτό είναι υπεύθυνο για την αποτελεσματική διεκπεραίωση όλων των θεμάτων του προσωπικού και της μισθοδοσίας του. Η εφαρμογή αυτή έχει δημιουργηθεί ειδικά για τις ανάγκες τις εταιρείας και αφορά τις ακόλουθες λειτουργίες:

- Μηχανογραφική τήρηση των προσωπικών μητρώων και έκδοση πιστοποιητικών υπηρεσιακών μεταβολών των υπαλλήλων.
- Μηχανογραφική τήρηση αρχείων διορισμού, πρόσληψης, μονιμοποίησης, μετακίνησης, προαγωγής, λύσης υπαλληλικής σχέσης και συνταξιοδότησης προσωπικού.
- Μηχανογραφική τήρηση σύμβασης προσωπικού, κρατήσεις, ταμεία, φορολογικά στοιχεία, προϋπηρεσία, άδειες, συντάξεις.

- Διαχείριση κατάταξης των υπαλλήλων σε μισθολογική κλίμακα και διαχείριση μισθοδοσίας προσωπικού. Εκκαθάριση αποδοχών (τακτικές, επιδόματα, ασθενείας, υπερωρίες, αποζημίωσης, αναδρομικών).

Δεδομένα

Για να μπορέσει η CRAMM να επεξεργαστεί τα δεδομένα που συμπεριλαμβάνονται στη μελέτη, είναι απαραίτητη η ταξινόμησή τους στις εξής κατηγορίες:

- Οικονομικά (Financial)
- Προσωπικά (Personal)
- Επιχειρησιακά Ευαίσθητα (Commercially Sensitive)
- Σχετικά με την ασφάλεια (Safety Related) και
- Όλα τα υπόλοιπα (Other Data Types)

Τα δεδομένα που τυγχάνουν επεξεργασίας από τις εφαρμογές έχουν καταταγεί σε ομάδες όπως φαίνονται στον πίνακα 3.

Εφαρμογές	Ομάδες Δεδομένων	Κατηγοριοποίηση Δεδομένων
Σύστημα Πελατών	Οικονομικά Δεδομένα (Data Financial)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα iv. Άλλο τύπο δεδομένων (π.χ. Μετρήσεις πελατών)
Σύστημα Οικονομικής & Λογιστικής Διαχείρησης	Οικονομικά Δεδομένα 2 (Data Financial 2)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα iv. Άλλο τύπο δεδομένων (π.χ. Δεδομένα διαχείρισης αποθήκης)
Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου	Δεδομένα Διαχείρισης Πληροφοριών (Data Management Information)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα
Σύστημα Διαχείρισης Προσωπικού	Δεδομένα Μισθοδοσίας (Data Payroll)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα

Πίνακας 3:Ταξινόμηση Δεδομένων

Παρόλο που το σύστημα Οικονομικής και Λογιστικής Διαχείρισης και το Σύστημα Πελατών διαχειρίζονται οικονομικά δεδομένα, η κατηγοριοποίηση πρέπει να γίνει διαφορετικά καθώς περιλαμβάνουν διαφορετικά δεδομένα και χρήζουν διαφορετικού επιπέδου ασφάλειας, οπότε θα πρέπει να δημιουργηθούν δύο ομάδες δεδομένων.

2.2.2. Αποτίμηση των Περιουσιακών Στοιχείων του Πληροφοριακού Συστήματος

Σε αυτό το σημείο γίνεται η αποτίμηση των δεδομένων, με βάση τις επιπτώσεις της απώλειας της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητάς τους. Ακολουθεί η αποτίμηση του λογισμικού με τον ίδιο τρόπο και η αποτίμηση του υλικού με βάση το κόστος αντικατάστασης. Για την αποτίμηση δεν λαμβάνονται υπόψη τα υφιστάμενα μέτρα ασφάλειας, αλλά ούτε και η πιθανότητα εκδήλωσης μιας απειλής. Αυτό που λαμβάνεται υπόψη είναι η επίπτωση που θα έχει για την εταιρεία η πραγματοποίηση μιας απειλής.

Η μέθοδος CRAMM περιέχει κάποιους πίνακες αποτίμησης με βάση τους οποίους γίνεται η αξιολόγηση ακολουθώντας μία αριθμητική κλίμακα 1-10. Στην περίπτωση όπου οι πιθανές επιπτώσεις ενός περιουσιακού στοιχείου εντάσσονται σε παραπάνω από μία κατηγορίες, τότε λαμβάνεται υπόψη η κατηγορία με το μεγαλύτερο βαθμό.

Στους πίνακες που ακολουθούν εμφανίζονται τα αποτελέσματα αυτού του σταδίου για τις τέσσερις ομάδες δεδομένων που περιγράφηκαν προηγουμένως. Οι περιπτώσεις που μελετήθηκαν θεωρούνται οι πιο σημαντικές κατά τη γνώμη των αρμόδιων στελεχών της εταιρείας.

2.2.2.1. Αποτίμηση Δεδομένων

1η Ομάδα – Οικονομικά Δεδομένα

Η πρώτη ομάδα αφορά στα δεδομένα που τυγχάνουν επεξεργασίας από το Σύστημα Πελατών. Τα δεδομένα αυτά περιλαμβάνουν κυρίως οικονομικά στοιχεία, προσωπικά στοιχεία πελατών, δεδομένα λογαριασμών και τιμολογίων, επιταγές προμηθευτών κ.ά.

Η ***απώλεια της διαθεσιμότητας*** των δεδομένων αυτών έχει ως αποτέλεσμα σοβαρή οικονομική απώλεια για την εταιρεία. Πιθανόν να υπάρξουν σοβαρές κυρώσεις, καθώς δεν θα είναι εφικτή η είσπραξη εισφορών για τις θυγατρικές εταιρείες και επιπλέον προκύπτει παύση εισροής εσόδων.

Η ***απώλεια της ακεραιότητας*** των δεδομένων μπορεί να επηρεάσει τα οικονομικά και εμπορικά συμφέροντα της εταιρείας. Ειδικότερα, σε περίπτωση ολικής καταστροφής παύει η κύρια λειτουργία της εταιρείας, επηρεάζοντας έτσι και άλλες εταιρείες που εξαρτώνται από τις παρεχόμενες υπηρεσίες του συστήματος πελατών (π.χ. θυγατρικές). Στις περιπτώσεις ύπαρξης λαθών εκτιμάται ότι θα υπάρξει οικονομική απώλεια λαμβάνοντας υπόψη περιπτώσεις λαθών σε λογαριασμούς και σε εισπράξεις τελών για θυγατρικές εταιρείες. Τέλος, σε περιπτώσεις εκτεταμένη ύπαρξη λαθών ή/και σκόπιμη αλλοίωση των δεδομένων, όπου μπορεί να υπάρξουν αλλαγές σε μετρήσεις, εξοφλητικά τιμολόγια κ.τ.λ., έχει ως αποτέλεσμα οικονομική απώλεια για την εταιρεία.

Η ***απώλεια της εμπιστευτικότητας*** αμαυρώνει τη φήμη της εταιρείας, γεγονός το οποίο συνεπάγεται και την πιθανή πτώση της μετοχής.

Κατηγορία Επίπτωσης		**Μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία**	**Βαθμός Αποτίμησης**
Απώλεια Διαθεσιμότητας Δεδομένων	1 ημέρα	Οικονομική Απώλεια	2
	1 μήνα	Οικονομική Απώλεια	6
Απώλεια Ακεραιότητας Δεδομένων	Ολική Καταστροφή	Οικονομικά & Εμπορικά συμφέροντα	7
	Εκτεταμένη Ύπαρξη Λαθών	Οικονομική Απώλεια	3
	Σκόπιμη Αλλοίωση	Οικονομική Απώλεια	4
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Απώλεια καλής φήμης	5

Πίνακας 4: Αποτίμηση 1ης ομάδας Δεδομένων.

2η Ομάδα – Οικονομικά Δεδομένα 2

Η δεύτερη ομάδα περιλαμβανει τα δεδομένα του σύστηματος Οικονομικής και Λογιστικής Διαχείρισης. Στο σύστημα αυτό περιλαμβάνονται προσωπικά δεδομένα, συμβάσεις προμηθευτών, δάνεια, επιταγές, δεδομένα διαχείρισης αποθηκών κ.ά.

Η ***απώλεια της διαθεσιμότητας*** των δεδομένων είναι ένα μείζον θέμα και μπορεί να προκαλέσει από οικονομική απώλεια μέχρι και αδυναμία τηρήσης των νομικών και κανονιστικών απαιτήσεων, διότι είναι αδύνατη η αποπλήρωμη δανείων και επιταγών προς τρίτους και επιπλέον μπορεί να υπάρξουν μηνύσεις εις βάρος της εταιρείας.

Η ***απώλεια της ακεραιότητας*** των δεδομένων σε περίπτωση ολικής καταστροφής συνεπάγεται τη μη ολοκλήρωση των οικονομικών υποχρεώσεων της εταιρείας προς τρίτους και τη μη ολοκλήρωση κρίσιμων εργασιών που απαιτούνται, όπως προμήθειες, διαγωνισμοί κ.τ.λ., επηρεάζοντας την ομαλή λειτουργία της εταιρείας.

Η ***απώλεια της εμπιστευτικότητας*** επηρεάζει την καλή εικόνα της εταιρείας, καθώς περιλαμβάνονται επιχειρησιακά ευαίσθητα δεδομένα, τα οποία δεν πρέπει να είναι διαθέσιμα στο ευρύ κοινό. Η ύπαρξη λαθών και η σκόπιμη αλλοίωση δεν έχουν αποτιμηθεί, καθώς γίνεται επικύρωση της ορθότητας των δεδομένων με βάσει τα χειρόγραφα πριν την τελική υποβολή.

Κατηγορία Επίπτωσης		**Μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία**	**Βαθμός Αποτίμησης**
Απώλεια Διαθεσιμότητας Δεδομένων	1 εβδομάδα	Οικονομική Απώλεια	1
	1 μήνα	Αδυναμία τήρησης Νομικών & Κανονιστικών Απαιτήσεων	4
Απώλεια Ακεραιότητας Δεδομένων	Ολική Καταστροφή	Δυσχέρεια Διοίκησης & Επιχειρηματικών Λειτουργιών	6
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Απώλεια καλής φήμης	3

Πίνακας 5: Αποτίμηση 2^{ης} ομάδας Δεδομένων

3^{η} Ομάδα - Δεδομένα Διαχείρισης Πληροφοριών

Η τρίτη ομάδα αφορά στα εισερχόμενα και εξερχόμενα έγγραφα της εταιρείας, τα οποία πρωτοκολλούνται από τις γραμματείες και δρομολογούνται κατάλληλα.

Η ***απώλεια της διαθεσιμότητας*** των δεδομένων δεν έχει σημαντική επίπτωση για την εταιρεία, καθώς η διαδικασία μπορεί να επιτελεστεί με χειρόγραφο τρόπο μέχρι την αποκατάσταση της ομαλής λειτουργίας.

Η ***απώλεια της ακεραιότητας*** *των δεδομένων* σε περίπτωση ολικής καταστροφής θα επιφέρει οικονομική απώλεια, η οποία προκύπτει από το κόστος επαναφοράς του συστήματος και επανεισαγωγής των χειρόγραφων δεδομένων. Η ύπαρξη λαθών στα δεδομένα πρωτοκόλλου δεν αποτιμάται, διότι τα δεδομένα φυλάσσονται και σε χειρόγραφη μορφή και πριν την επικύρωσή τους επιβεβαιώνεται η ορθότητά τους.

Η ***απώλεια της εμπιστευτικότητας***, λαμβάνοντας υπόψη την αποκάλυψη των δεδομένων σε προσωπικό της εταιρείας, επηρεάζει τη φήμη της αλλά καθώς τα δεδομένα δεν είναι εμπιστευτικά η επίπτωση θα είναι πολύ μικρή. Η αποκάλυψη των δεδομένων σε τρίτους έχει σημαντική επίπτωση, διότι μπορεί να οδηγήσει σε δυσφήμιση της εταιρείας.

Κατηγορία Επίπτωσης		**Μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία**	**Βαθμός Αποτίμησης**
Απώλεια Διαθεσιμότητας Δεδομένων	2 εβδομάδες	Οικονομική Απώλεια	1
Απώλεια Ακεραιότητας Δεδομένων	Ολική Καταστροφή	Οικονομική Απώλεια	2
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε προσωπικό της εταιρείας	Απώλεια καλής φήμης	2
	Αποκάλυψη των δεδομένων σε τρίτους	Απώλεια καλής φήμης	5

Πίνακας 6: Αποτίμηση 3ης ομάδας Δεδομένων

4η Ομάδα - Δεδομένα Μισθοδοσίας

Η τέταρτη ομάδα περιλαμβάνει τα δεδομένα που σχετίζονται με τη μισθοδοσία, όπως προσωπικά στοιχεία υπαλλήλων, επαγγελματική θέση, προϋπηρεσία, άδειες, επιδόματα, μεταθέσεις κ.τ.λ.

Η ***απώλεια της διαθεσιμότητας*** των δεδομένων συνεπάγεται την αδυναμία πληρωμής του προσωπικού, κάτι το οποίο μπορεί να οδηγήσει σε μηνύσεις εναντίον της εταιρείας.

Η ***απώλεια της ακεραιότητας*** των δεδομένων σε περίπτωση ολικής καταστροφής μπορεί να επιφέρει οικονομική απώλεια στην εταιρεία που προκύπτει από το κόστος επανεισαγωγής των χειρόγραφων δεδομένων. Η περίπτωση σκόπιμης αλλοίωσης έχει ως αποτέλεσμα το οικονομικό όφελος του ατόμου που έκανε την αλλοίωση και επιπλέον την οικονομική απώλεια για την εταιρεία.

Η ***απώλεια της εμπιστευτικότητας***, λαμβάνοντας υπόψη την περίπτωση της αποκάλυψης των δεδομένων σε τρίτους μπορεί να οδηγήσει σε ενόχληση πολλών ατόμων και παραβίαση της νομοθεσίας, καθώς περιλαμβάνονται εμπιστευτικά και ευαίσθητα δεδομένα του προσωπικού. Η περίπτωση αποκάλυψης αυτών σε εσωτερικούς χρήστες δεν έχει αξιολογηθεί διότι έχει την ίδια επίπτωση με την αποκάλυψη σε τρίτους.

Κατηγορία Επίπτωσης		Μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία	Βαθμός Αποτίμησης
Απώλεια Διαθεσιμότητας Δεδομένων	Περισσότερο από 2 εβδομάδες	Αδυναμία τήρησης Νομικών & Κανονιστικών Απαιτήσεων	4
Απώλεια Ακεραιότητας Δεδομένων	Ολική Καταστροφή	Οικονομική Απώλεια	3
	Σκόπιμη Αλλοίωση	Οικονομική Απώλεια	3
Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε τρίτους	Αποκάλυψη Προσωπικών Πληροφοριών	4

Πίνακας 7: Αποτίμηση 4ης ομάδας Δεδομένων

2.2.2.2. Αποτίμηση Υλικού

Παρόλο που η αξία των δεδομένων έχει συχνά περισσότερη σημασία για την εκτίμηση επικινδυνότητας, πρέπει να υπολογιστεί και η αξία των υλικών στοιχείων καθώς αυτά συμβάλλουν στα μέτρα για τον υπολογισμό των κινδύνων και στην επιλογή των αντιμέτρων. Τα υλικά στοιχεία αποτιμώνται με βάση τη χρηματική τους αξία σε περίπτωση αντικατάστασής τους. Στον πίνακα 8 παρουσιάζεται η αποτίμηση των υλικών περιουσιακών στοιχείων της εταιρείας. Το κόστος αντικατάστασης εκφράζεται σε ευρώ και αφορά τη συνολική ποσότητα κάθε κατηγορίας περιουσιακού στοιχείου.

Περιουσιακό Στοιχείο	Ποσότητα	Βαθμός Αποτίμησης	Κόστος Αντικατάστασης
Φορητός Υπολογιστής	8	2	5600
Dumb Terminal	5	2	1000
Σταθμός Εργασίας	50	4	50000
Δρομολογητής / Μεταγωγέας (Switch)	6	4	5800
Εκτυπωτής	5	2	1500
Εξυπηρετητής εφαρμογής του Συστήματος Λογιστικής & Οικονομικής Διαχείρισης	4	2	4500
Εξυπηρετητής εφαρμογής του Συστήματος Πελατών	1	8	3000000
Εξυπηρετητής εφαρμογής του Συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	1	2	2200

Περιουσιακό Στοιχείο	Ποσότητα	Βαθμός Αποτίμησης	Κόστος Αντικατάστασης
Εξυπηρετητής εφαρμογών του Συστήματος Διαχείρισης Προσωπικού	1	2	2200
Εξυπηρετητής Βάσεων Δεδομένων	2	2	2200

Πίνακας 8: Αποτίμηση Υλικού.

2.2.2.3. Αποτίμηση Λογισμικού

Για την αποτίμηση του λογισμικού ακολουθήθηκε ο ίδιος τρόπος αποτίμησης με τα δεδομένα. Ο πίνακας 9 απεικονίζει τα αποτελέσματα της αποτίμησης.

Φυσική Καταστροφή Λογισμικού	Μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία	Βαθμός Αποτίμησης
Λογισμικό του Συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Οικονομική Απώλεια	7
Λογισμικό του Συστήματος Πελατών	Οικονομική Απώλεια	8
Λογισμικό του Συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Οικονομική Απώλεια	2
Λογισμικό του Συστήματος Διαχείρισης Προσωπικού	Οικονομική Απώλεια	1

Πίνακας 9: Αποτίμηση Λογισμικού

2.2.3. Εκτίμηση Επικινδυνότητας

Ο βαθμός επικινδυνότητας είναι συνάρτηση τριών παραγόντων: της επίπτωσης, της αξίας των περιουσιακών στοιχείων και του επιπέδου των αδυναμιών:

Πιθανότητα = Απειλή x Αδυναμία

Επικινδυνότητα = Πιθανότητα x Επίπτωση

Για να γίνει η αποτίμηση των απειλών που αντιμετωπίζει το Π.Σ. έχουν δοθεί από τα αρμόδια στελέχη της εταιρείας απαντήσεις στα ερωτηματολόγια που παράγει η CRAMM. Επιπλέον, έχουν πραγματοποιηθεί επιτόπιοι έλεγχοι για τον εντοπισμό των αδυναμιών του Π.Σ. Η πιθανότητα πραγματοποίησης των απειλών αξιολογείται στην κλίμακα 1-5 (πολύ χαμηλή, χα-

μηλή, μέτρια, υψηλή, πολύ υψηλή) και η αξιολόγηση του επιπέδου ευπάθειας για κάθε συνδυασμό απειλής – περιουσιακού στοιχείου αξιολογείται στην κλίμακα 1-3 (χαμηλή, μέτρια, υψηλή). Η συσχέτιση των απειλών με τα περιουσιακά στοιχεία ή τις ομάδες αυτών μπορεί να γίνει είτε με συσχετισμό μιας απειλής σε ένα περιουσιακό στοιχείο ή σε μία ομάδα περιουσιακών στοιχείων, είτε με το συσχετισμό ενός περιουσιακού στοιχείου σε μία ή περισσότερες απειλές. Στην παρούσα μελέτη η συσχέτιση έχει πραγματοποιηθεί συσχετίζοντας κάθε απειλή με ένα ή περισσότερα περιουσιακά στοιχεία.

2.2.3.1. Αποτελέσματα Αποτίμησης

Στον πίνακα 10 που ακολουθεί παρουσιάζονται τα αποτελέσματα της αποτίμησης των σημαντικότερων απειλών που αντιμετωπίζει το Π.Σ.

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας
Πλαστοπροσωπία από Εσωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Πελατών	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Υψηλή	Υψηλή
Πλαστοπροσωπία από Παρόχους Υπηρεσιών	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Πελατών	Πολύ Χαμηλή	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή	Μέτρια
Πλαστοπροσωπία από Εξωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Υψηλή	Χαμηλή
	Λογισμικό του συστήματος Πελατών	Υψηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Χαμηλή

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Μέτρια	Χαμηλή
Διακοπή Ηλεκτροδότησης	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Πολύ υψηλή	Μέτρια
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Εφαρμογής)	Πολύ υψηλή	Μέτρια
	Υλικό του συστήματος Πελατών	Πολύ υψηλή	Μέτρια
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ υψηλή	Μέτρια
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Πολύ υψηλή	Μέτρια
Αστοχία Κλιματισμού	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Υψηλή	Μέτρια
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Εφαρμογής)	Υψηλή	Μέτρια
	Υλικό του συστήματος Πελατών	Υψηλή	Μέτρια
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Υψηλή	Μέτρια
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Υψηλή	Μέτρια
Αστοχία Λογισμικού Εφαρμογών	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Πελατών	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Χαμηλή	Χαμηλή
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Χαμηλή	Χαμηλή
Σφάλμα Συντήρησης Υλικού	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Μέτρια	Υψηλή
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Μέτρια	Υψηλή

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας
	(Εξυπηρετητής Εφαρμογής)		
	Υλικό του συστήματος Πελατών	Μέτρια	Υψηλή
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Υψηλή
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Μέτρια	Υψηλή
Σφάλμα Συντήρησης Λογισμικού	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Πελατών	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή	Μέτρια
Λάθος Χρήστη	Οικονομικά Δεδομένα	Πολύ Υψηλή	Μέτρια
	Οικονομικά Δεδομένα 2	Πολύ Υψηλή	Μέτρια
	Δεδομένα Μισθοδοσίας	Μέτρια	Μέτρια
	Δεδομένα Διαχείρισης Πληροφοριών	Μέτρια	Μέτρια
Φωτιά	Κεντρικό κτήριο	Πολύ Χαμηλή	Υψηλή
	Κτήριο 2	Πολύ Χαμηλή	Υψηλή
	Κτήριο 3	Πολύ Χαμηλή	Υψηλή
Πλημμύρα	Κεντρικό κτήριο	Υψηλή	Μέτρια
	Κτήριο 2	Υψηλή	Μέτρια
	Κτήριο 3	Πολύ Χαμηλή	Χαμηλή
Κλοπή από Εσωτερικούς Χρήστες	Σταθμοί Εργασίας	Πολύ Υψηλή	Μέτρια
	Δρομολογητές (Switches)	Πολύ Υψηλή	Μέτρια
	Εκτυπωτές	Πολύ Υψηλή	Μέτρια

Πίνακας 10: Αποτελέσματα Αποτίμησης

2.2.3.2. Εκτίμηση Επικινδυνότητας

Στον πίνακα 11 που ακολουθεί παρουσιάζεται ο βαθμός επικινδυνότητας για κάθε περιουσιακό στοιχείο του Π.Σ. Ο βαθμός επικινδυνότητας υπολογίζεται στην κλίμακα 1-7.

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας	Βαθμός Επικινδυνότητας
Πλαστοπροσωπία από Εσωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Υψηλή	Υψηλή	4
	Λογισμικό του συστήματος Πελατών	Πολύ Υψηλή	Υψηλή	4
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Υψηλή	5
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Υψηλή	Υψηλή	4
Πλαστοπροσωπία από Παρόχους Υπηρεσιών	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Χαμηλή	Μέτρια	2
	Λογισμικό του συστήματος Πελατών	Πολύ Χαμηλή	Υψηλή	2
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ Χαμηλή	Μέτρια	3
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή	Μέτρια	2
Πλαστοπροσωπία από Εξωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Υψηλή	Χαμηλή	3
	Λογισμικό του συστήματος Πελατών	Υψηλή	Μέτρια	2

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας	Βαθμός Επικινδυνότητας
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Χαμηλή	4
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Μέτρια	Χαμηλή	3
Διακοπή Ηλεκτροδότησης	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Πολύ υψηλή	Μέτρια	1
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Εφαρμογών)	Πολύ υψηλή	Μέτρια	1
	Υλικό του συστήματος Πελατών	Πολύ υψηλή	Μέτρια	1
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ υψηλή	Μέτρια	1
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Πολύ υψηλή	Μέτρια	1
Αστοχία Κλιματισμού	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Υψηλή	Μέτρια	2
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Εφαρμογών)	Υψηλή	Μέτρια	2
	Υλικό του συστήματος Πελατών	Υψηλή	Μέτρια	2
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Υψηλή	Μέτρια	2
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Υψηλή	Μέτρια	2

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας	Βαθμός Επικινδυνότητας
Αστοχία Λογισμικού Εφαρμογών	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Υψηλή	Υψηλή	2
	Λογισμικό του συστήματος Πελατών	Πολύ Υψηλή	Υψηλή	1
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Χαμηλή	Χαμηλή	2
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Χαμηλή	Χαμηλή	2
Σφάλμα Συντήρησης Υλικού	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Βάσεων Δεδομένων)	Μέτρια	Υψηλή	3
	Υλικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης (Εξυπηρετητής Εφαρμογών)	Μέτρια	Υψηλή	2
	Υλικό του συστήματος Πελατών	Μέτρια	Υψηλή	2
	Υλικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Υψηλή	3
	Υλικό του συστήματος Διαχείρισης Προσωπικού	Μέτρια	Υψηλή	3
Σφάλμα Συντήρησης Λογισμικού	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Χαμηλή	Μέτρια	1
	Λογισμικό του συστήματος Πελατών	Πολύ Χαμηλή	Μέτρια	1
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ Χαμηλή	Μέτρια	1
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή	Μέτρια	1
Λάθος Χρήστη	Οικονομικά Δεδομένα	Πολύ Υψηλή	Μέτρια	3
	Οικονομικά Δεδομένα 2	Πολύ Υψηλή	Μέτρια	2

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας	Βαθμός Επικινδυνότητας
	Δεδομένα Μισθοδοσίας	Μέτρια	Μέτρια	2
	Δεδομένα Διαχείρισης Πληροφοριών	Μέτρια	Μέτρια	3
Φωτιά	Κεντρικό κτήριο	Πολύ Χαμηλή	Υψηλή	5
	Κτήριο 2	Πολύ Χαμηλή	Υψηλή	4
	Κτήριο 3	Πολύ Χαμηλή	Υψηλή	4
Πλημμύρα	Κεντρικό κτήριο	Υψηλή	Μέτρια	5
	Κτήριο 2	Υψηλή	Μέτρια	3
	Κτήριο 3	Πολύ Χαμηλή	Χαμηλή	2
Κλοπή από Εσωτερικούς Χρήστες	Σταθμοί Εργασίας	Πολύ Υψηλή	Μέτρια	4
	Δρομολογητές (Switches)	Πολύ Υψηλή	Μέτρια	3
	Εκτυπωτές	Πολύ Υψηλή	Μέτρια	3

Πίνακας 11: Αποτελέσματα Βαθμού Επικινδυνότητας.

Οι πιο κρίσιμες από τις παραπάνω απειλές είναι εκείνες οι οποίες έχουν το μεγαλύτερο βαθμό επικινδυνότητας (τέσσερα και πέντε). Όσο μεγαλύτερος είναι ο βαθμός επικινδυνότητας, τόσο μεγαλύτερη είναι και η ανάγκη για υλοποίηση μέτρων προστασίας. Αρχικά λαμβάνονται μέτρα για τα περιουσιακά στοιχεία που παρουσιάζουν μεγαλύτερο βαθμό επικινδυνότητας και έπειτα για τα περιουσιακά στοιχεία με μικρότερο βαθμό επικινδυνότητας. Ουσιαστικά, θα πρέπει να ληφθούν μέτρα για όλες τις απειλές που εντοπίστηκαν, έτσι ώστε να είναι εφικτή η προστασία ολόκληρου του Π.Σ.

2.2.4. Αντίμετρα

Στα παραπάνω αποτελέσματα δεν έχουν ληφθεί υπόψη τα ήδη εγκατεστημένα μέτρα προστασίας (π.χ. disaster site). Έτσι, σε αυτό το σημείο έρχεται ο υπολογισμός των αντιμέτρων - μέτρων προστασίας που είναι και το τρίτο βήμα της μεθοδολογίας.

Η CRAMM περιλαμβάνει μία δομημένη βάση από τεχνικά, οργανωτικά και διοικητικά μέτρα προστασίας, γνωστή και ως βιβλιοθήκη μέτρων προστασίας. Μέσω του λογισμικού της CRAMM μπορεί να γίνει η αυτόματη επιλογή μιας λίστας προτεινόμενων αντιμέτρων, με βάση τα αποτελέσματα της ανάλυσης κινδύνου. Τα προτεινόμενα μέτρα προστασίας συγκρίνονται με

τα υπάρχοντα και είναι πάντα προτιμότερο να παραμένει κάποιο από τα υπάρχοντα παρά να αντικαθίσταται από κάποιο ισοδύναμό του [9].

Ένα μέτρο προστασίας μπορεί να βρίσκεται σε μία από τις ακόλουθες καταστάσεις:

- Εγκατεστημένο,
- Προς εγκατάσταση,
- Προς υλοποίηση,
- Προτεινόμενο προς υλοποίηση,
- Έχει ήδη καλυφθεί (από κάποιο άλλο μέτρο),
- Αποδεκτός εναπομένων βαθμός κινδύνου (το μέτρο δεν εγκαθίσταται),
- Υπό συζήτηση,
- Μη εφαρμόσιμο.

Στη συνέχεια παρουσιάζονται τα μέτρα προστασίας που πρόκειται να υλοποιηθούν, τα προτεινόμενα προς υλοποίηση, τα μέτρα που είναι υπό συζήτηση και τα μέτρα για τα οποία έχει οριστεί ως αποδεκτός ο εναπομένων βαθμός κινδύνου. Εξαιτίας του μεγάλου όγκου των μέτρων προστασίας, δεν έχουν ληφθεί υπόψη τα μέτρα που είναι εγκατεστημένα, τα μέτρα που είναι προς εγκατάσταση, τα μέτρα που έχουν καλυφθεί ήδη και τα μέτρα που δεν είναι δυνατόν να εφαρμοστούν.

Μέτρα Προστασίας	Κατάσταση
Λογικός Έλεγχος Πρόσβασης	
Διακριτός Έλεγχος Πρόσβασης	
Μηχανισμός ελέγχου πρόσβασης που μπορεί να δείξει ποιος έχει αιτηθεί πρόσβαση για κάποιο αρχείο.	Προτεινόμενο προς υλοποίηση
Μηχανισμός ελέγχου πρόσβασης που να υποδεικνύει σε ποια αρχεία μπορεί να έχει πρόσβαση ο κάθε χρήστης.	Προτεινόμενο προς υλοποίηση
Δικαιώματα πρόσβασης ανάλογα με τους ρόλους	
Τα δικαιώματα πρόσβασης να μπορούν να ανακληθούν εγκαίρως.	Προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Ευθύνη Περιουσιακών Στοιχείων	
Η ακρίβεια του αρχείου καταγραφών ή απογραφής να ελέγχεται τουλάχιστον κάθε έξι μήνες.	Αποδεκτός εναπομένων βαθμός κινδύνου
Κάθε πρόσωπο που αποχωρεί θα πρέπει να υπογράφει δήλωση επιστροφής όλων των περιουσιακών στοιχείων που ανήκουν στον οργανισμό.	Προτεινόμενο προς υλοποίηση
Εγγραφή χρηστών	
Θα πρέπει να ανακοινώνονται γραπτώς τα δικαιώματα πρόσβασης των χρηστών.	Προτεινόμενο προς υλοποίηση
Οι χρήστες θα πρέπει να υπογράφουν δήλωση που θα βεβαιώνει ότι κατανοούν και αποδέχονται τα δικαιώματά τους.	Προτεινόμενο προς υλοποίηση
Τα δικαιώματα των χρηστών που άλλαξαν θέση ή απομακρύνθηκαν από τον οργανισμό, θα πρέπει να απενεργοποιούνται άμεσα.	Προς υλοποίηση
Επισκόπηση Δικαιωμάτων Πρόσβασης Χρηστών	
Τα δικαιώματα πρόσβασης θα πρέπει να επανελέγχονται ανά τακτά χρονικά διαστήματα.	Προς υλοποίηση
Τα δικαιώματα πρόσβασης των απλών χρηστών θα πρέπει να επανελέγχονται τουλάχιστον κάθε έξι μήνες.	Προς υλοποίηση
Έλεγχος της λίστας προνομιακών χρηστών τουλάχιστον μια φορά κάθε τρεις μήνες.	Προτεινόμενο προς υλοποίηση
Απαριθμήσεις	
Καταγραφή Περιστατικών	
Καταγραφή των αρχείων που έχουν προσπελαστεί.	Προτεινόμενο προς υλοποίηση
Προσμέτρηση των χρόνων απενεργοποίησης όλων των σταθμών εργασίας.	Αποδεκτός εναπομένων βαθμός κινδύνου
Έλεγχος	
Ανασκόπηση των αρχείων καταγραφής περιστατικών	
Αναθεώρηση των λογαριασμών με αυξημένη πρόσβαση.	Προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Ανασκόπηση των αποτυχιών πρόσβασης.	Προτεινόμενο προς υλοποίηση
Ανασκόπηση των τάσεων που υπάρχουν, βάσει του αριθμού επιτυχημένων log-ons.	Αποδεκτός εναπομένων βαθμός κινδύνου
Ανασκόπηση των τάσεων που υπάρχουν για τη χρήση του συστήματος από τους απομακρυσμένους σταθμούς εργασίας.	Υπό συζήτηση
Έλεγχος του αρχείου συμβάντων τουλάχιστον μια φορά τον μήνα.	Προς υλοποίηση
Διερεύνηση Περιστατικών	
Μετά το πέρας της έρευνας θα πρέπει να δοθεί αναφορά των αποτελεσμάτων στα ανώτερα διευθυντικά στελέχη.	Προς υλοποίηση
Καταγραφή κατευθυντήριων οδηγιών για τη διερεύνηση των παραβιάσεων ασφάλειας.	Προτεινόμενο προς υλοποίηση
Με την αναφορά ενός περιστατικού, θα πρέπει να εκτελείται άμεσα μια έκθεση της διαδρομής του ελέγχου που πραγματοποιήθηκε.	Προτεινόμενο προς υλοποίηση
Η έκθεση της διαδρομής του ελέγχου που πραγματοποιήθηκε θα πρέπει να αποθηκευτεί με τρόπο που δεν θα είναι δυνατή η αλλοίωση των περιεχομένων της.	Προτεινόμενο προς υλοποίηση
Προστασία Ενάντια σε Κακόβουλα Λογισμικά	
Πρόληψη Ενάντια σε Κακόβουλα Λογισμικά	
Καθορισμός πολιτικής για την αντιμετώπιση σκόπιμης εισαγωγής κακόβουλου λογισμικού.	Προτεινόμενο προς υλοποίηση
Εξασφάλιση ότι η πληροφόρηση για την απειλή από κακόβουλο λογισμικό έχει δοθεί στο σύνολο του προσωπικού.	Προτεινόμενο προς υλοποίηση
Απομάκρυνση Κακόβουλου λογισμικού	
Παροχή εκπαίδευσης στο καθορισμένο προσωπικό για τον εντοπισμό και την απομάκρυνση κακόβουλου λογισμικού.	Προτεινόμενο προς υλοποίηση
Mobile Computing και Τηλεργασία	
Mobile Computing	
Προετοιμασία οδηγιών για τους κινδύνους και την πρόληψη αυτών όταν χρησιμοποιούνται υπηρεσίες mobile computing.	Προτεινόμενο προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Οδηγίες που θα καλύπτουν το είδος ελέγχων που θα πρέπει να εφαρμόζονται στις περιπτώσεις mobile computing.	Προτεινόμενο προς υλοποίηση
Οδηγίες και συμβουλές για τη χρήση των υπηρεσιών αυτών σε δημόσιους χώρους.	Προτεινόμενο προς υλοποίηση
Οδηγίες και συμβουλές για τους αποθηκευτικούς χώρους που φυλάσσονται οι συσκευές mobile computing, όταν δεν χρησιμοποιούνται.	Αποδεκτός εναπομένων βαθμός κινδύνου
Ασφάλεια του εξοπλισμού που βρίσκεται εκτός των εγκαταστάσεων	
Επαρκής ασφαλιστική κάλυψη ώστε να υπάρχει προστασία του εξοπλισμού που κινείται εκτός του χώρου του οργανισμού.	Υπό συζήτηση
Λειτουργίες Ελέγχου	
Παρακολούθηση Δραστηριοτήτων	
Ενημέρωση του προσωπικού ότι οι δραστηριότητες τους ελέγχονται.	Προτεινόμενο προς υλοποίηση
Διαχείριση Εξωτερικών Δραστηριοτήτων	
Οι διαδικασίες για τον έλεγχο της ασφάλειας θα πρέπει να καθορίζονται στη σύμβαση.	Αποδεκτός εναπομένων βαθμός κινδύνου
Σχεδιασμός Επιχειρησιακής Συνέχειας	
Ανάκαμψη της επιχείρησης	
Δημιουργία πλάνων επιχειρησιακής συνέχειας (Business Continuity Plans - BCP).	Προς υλοποίηση
Διαχείριση της διαδικασίας επιχειρησιακής συνέχειας.	Προς υλοποίηση
Διατήρηση του σχεδίου επιχειρησιακής συνέχειας.	Προς υλοποίηση
Επιχειρησιακή Συνέχεια και Ανάλυση των επιπτώσεων	
Η στρατηγική επιχειρησιακής συνέχειας θα πρέπει να βασίζεται σε μια αξιολόγηση του κινδύνου (Risk Assessment).	Προς υλοποίηση
Προσδιορισμός κινδύνων που μπορεί να προκαλέσουν διακοπή στην επιχειρησιακή διαδικασία.	Προς υλοποίηση
Εκτίμηση των επιπτώσεων.	Προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Η αξιολόγηση κινδύνου να καλύπτει όλες τις επιχειρησιακές διαδικασίες	Προς υλοποίηση
Να καθοριστεί μια υψηλού επιπέδου στρατηγική συνέχειας.	Προς υλοποίηση
Η στρατηγική πρέπει να εγκριθεί από τα ανώτερα διευθυντικά στελέχη.	Προς υλοποίηση
Τεκμηρίωση και εφαρμογή των Πλάνων Επιχειρησιακής Συνέχειας	
Τα σχέδια επιχειρησιακής συνέχειας θα πρέπει να επιτρέπουν την αποκατάσταση της λειτουργίας της επιχείρησης εντός των απαιτούμενων χρονικών ορίων μετά από διακοπή σε μια επιχειρησιακή διαδικασία.	Προς υλοποίηση
Τα σχέδια να περιλαμβάνουν τα άτομα που ορίζονται ως αρμόδια για την υποβοήθηση της διαδικασίας ανάκτησης.	Προς υλοποίηση
Να οριστούν και να τεκμηριωθούν διαδικασίες έκτακτης ανάγκης που να επιτρέπουν την ανάκτηση και την αποκατάσταση εντός των απαιτούμενων χρονικών ορίων.	Προς υλοποίηση
Το προσωπικό πρέπει να εκπαιδευτεί σχετικά με τις διαδικασίες έκτακτης ανάγκης και τη διαχείριση κρίσεων.	Προτεινόμενο προς υλοποίηση
Η διαδικασία σχεδιασμού να επικεντρωθεί στην επίτευξη των απαιτούμενων επιχειρησιακών στόχων.	Προτεινόμενο προς υλοποίηση
Έλεγχος των Σχεδίων Επιχειρησιακής Συνέχειας	
Να γίνονται τακτικοί έλεγχοι των σχεδίων επιχειρησιακής συνέχειας.	Προτεινόμενο προς υλοποίηση
Να καθοριστεί το είδος των ελέγχων που θα διεξάγονται.	Προτεινόμενο προς υλοποίηση
Τα Σχέδια να επικαιροποιηθούν ώστε να αντανακλούν τυχόν ευρήματα από τους ελέγχους.	Προτεινόμενο προς υλοποίηση
Διατήρηση Σχεδίων Επιχειρησιακής Συνέχειας	
Τα Σχέδια Επιχειρησιακής Συνέχειας θα πρέπει να συντηρούνται.	Προτεινόμενο προς υλοποίηση
Τα Σχέδια Επιχειρησιακής Συνέχειας θα πρέπει να αντανακλούν τις επιχειρησιακές αλλαγές.	Προτεινόμενο προς υλοποίηση
Τα Σχέδια θα πρέπει να ανανεώνονται ώστε να περιλαμβάνουν τις αλλαγές του προσωπικού.	Προτεινόμενο προς υλοποίηση
Τα Σχέδια θα πρέπει να αναθεωρούνται ώστε να περιλαμβάνουν τις μεταβολές των πληροφοριακών συστημάτων.	Προτεινόμενο προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Τα Σχέδια θα πρέπει να περιλαμβάνουν τυχόν νομικές ή κανονιστικές αλλαγές.	Προτεινόμενο προς υλοποίηση
Τα Σχέδια θα πρέπει να περιλαμβάνουν τις εξαγορές ή τις συγχωνεύσεις εταιριών.	Προτεινόμενο προς υλοποίηση
Διαχείριση Κρίσεων	
Θα πρέπει να υπάρχει σχέδιο διαχείρισης μιας κρίσης.	Προτεινόμενο προς υλοποίηση
Το σχέδιο διαχείρισης της κρίσης θα πρέπει να ορίζει το ποιός είναι αρμόδιος για τον χειρισμό της κρίσης, καθώς και τους αναπληρωτές του.	Προτεινόμενο προς υλοποίηση
Το σχέδιο διαχείρισης της κρίσης θα πρέπει να ορίζει τους χειρισμούς που θα πρέπει να γίνουν κατά την αναγνώριση της ύπαρξης μιας κρίσης.	Προτεινόμενο προς υλοποίηση
Το σχέδιο διαχείρισης της κρίσης θα πρέπει να ορίζει το ποιός διευκρινίζει ότι το σχέδιο αυτό έχει ενεργοποιηθεί.	Προτεινόμενο προς υλοποίηση
Το σχέδιο διαχείρισης της κρίσης θα πρέπει να καθορίζει την ακολουθία των εντολών που δίνονται όταν αυτό ενεργοποιηθεί.	Προτεινόμενο προς υλοποίηση
Το σχέδιο διαχείρισης της κρίσης θα πρέπει να καθορίζει τον τρόπο επικοινωνίας που θα πρέπει να έχουν οι άνθρωποι που εμπλέκονται με αυτό.	Προτεινόμενο προς υλοποίηση
Φυσική Ασφάλεια Κτηρίων	
Ταυτότητες εισόδου προσωπικού	
Να δοθεί οδηγία ώστε το προσωπικό να φέρει πάντα πάνω του το πάσο εισόδου.	Αποδεκτός εναπομένων βαθμός κινδύνου
Το προσωπικό να είναι προσεκτικό προς τα άτομα που δεν φορούν την ταυτότητά τους.	Αποδεκτός εναπομένων βαθμός κινδύνου
Έλεγχος Εισβολής στο Κτήριο	
Θα πρέπει να υπάρχει συναγερμός που θα ενεργοποιείται εξωτερικά.	Προς υλοποίηση
Θα πρέπει να ηχεί ο συναγερμός όταν υπάρχει εισβολέας.	Προς υλοποίηση
Ο συναγερμός να ενεργοποιεί ένα έντονο εναλλασσόμενο φως (strobe light).	Προς υλοποίηση
Θα πρέπει να υπάρχουν αισθητήρες στα σημεία εισόδου.	Προς υλοποίηση

Μέτρα Προστασίας	Κατάσταση
Η κατάσταση των αισθητήρων να απεικονίζεται σε έναν πίνακα ελέγχου.	Προς υλοποίηση
Ο πίνακας ελέγχου θα πρέπει να προστατεύεται από μη εξουσιοδοτημένη χρήση.	Προς υλοποίηση
Ο συναγερμός θα πρέπει να ενεργοποιείται, ακόμα και αν αυτός που εισχωρεί στην εταιρεία έχει γνώση τέτοιων συστημάτων.	Προς υλοποίηση
Ο συναγερμός να συνδέεται με το τοπικό αστυνομικό τμήμα, ή άλλον φορέα προστασίας.	Υπό συζήτηση
Αισθητήρες κίνησης θα πρέπει να είναι τοποθετημένοι σε όλο κτήριο.	Υπό συζήτηση
Έλεγχος Επισκεπτών	
Οι επισκέπτες θα πρέπει να προμηθεύονται πάσο ή κάποια ένδειξη ότι είναι επισκέπτες.	Προτεινόμενο προς υλοποίηση
Θα πρέπει να υπάρχει οδηγία, οι επισκέπτες να φέρουν το πάσο τους καθ' όλη τη διάρκεια που παραμένουν στο κτήριο.	Προτεινόμενο προς υλοποίηση
Το προσωπικό να είναι προσεκτικό προς τους επισκέπτες που δεν φορούν την ταυτότητά τους.	Προτεινόμενο προς υλοποίηση
Έλεγχος Κτηρίου	
Οι φύλακες θα πρέπει να υποβάλλονται σε έλεγχο.	Προτεινόμενο προς υλοποίηση
Έλεγχος Χώρου	
Όταν χρησιμοποιείται μια εξωτερική εταιρεία φύλαξης, θα πρέπει τουλάχιστον να έχει καλή φήμη.	Προτεινόμενο προς υλοποίηση
Προστασία Κλοπής	
Πρόληψη Κλοπής	
Οι συνδυασμοί των χρηματοκιβωτίων και των κλειδαριών θα πρέπει να αλλάζονται κάθε 6 μήνες.	Προτεινόμενο προς υλοποίηση
Θα πρέπει να υπάρχουν συχνές περιπολίες ασφαλείας.	Προτεινόμενο προς υλοποίηση
Προστασία από τη Φωτιά	
Εκκένωση σε Περίπτωση Φωτιάς	

Μέτρα Προστασίας	Κατάσταση
Να επιδεικνύεται στο προσωπικό το σχέδιο εκκένωσης του κτηρίου από φωτιά.	Προτεινόμενο προς υλοποίηση
Πρόληψη και Έλεγχος	
Τα έπιπλα θα πρέπει να είναι σχεδιασμένα ώστε να αντιστέκονται στη φωτιά.	Υπό συζήτηση
Προσωπικό	
Επιλογή προσλήψεων	
Όταν το εποχιακό προσωπικό το αναλαμβάνει εξωτερικός εργολάβος, θα πρέπει να αναφέρεται ρητά στο συμβόλαιό του ότι έχει την ευθύνη για τη σωστή επιλογή του προσωπικού.	Προτεινόμενο προς υλοποίηση
Όροι και Προϋποθέσεις Πρόσληψης	
Οι όροι και οι προϋποθέσεις πρόσληψης θα πρέπει να ορίζουν την ευθύνη του υπαλλήλου για την ασφάλεια των πληροφοριών.	Προτεινόμενο προς υλοποίηση
Η ευθύνη του υπαλλήλου για την ασφάλεια των πληροφοριών θα πρέπει να καλύπτει το σύνολο της εργασιακής του περιόδου.	Προτεινόμενο προς υλοποίηση
Η ευθύνη του υπαλλήλου για την ασφάλεια των πληροφοριών θα πρέπει να καλύπτει μια συγκεκριμένη περίοδο μετά το τέλος της εργασιακής του σύμβασης.	Προτεινόμενο προς υλοποίηση
Οι συνέπειες της αγνόησης των υποχρεώσεων ασφαλείας από τον χρήστη θα πρέπει να ορίζονται.	Προτεινόμενο προς υλοποίηση
Η ευθύνη για την ασφάλεια των πληροφοριών θα πρέπει να επεκτείνεται και έξω από τα όρια του οργανισμού.	Προτεινόμενο προς υλοποίηση
Υπάλληλοι, εργολάβοι και τρίτα μέρη, θα πρέπει να είναι ενήμεροι για τις προϋποθέσεις ασφαλείας και τις νομικές υποχρεώσεις τους μετά το τέλος / την αλλαγή της εργασίας τους.	Προτεινόμενο προς υλοποίηση
Ασφάλεια στην Περιγραφή των Θέσεων Εργασίας	
Οι συμβάσεις εργασίας θα πρέπει να περιλαμβάνουν πλήρη περιγραφή της θέσης.	Αποδεκτός εναπομένων βαθμός κινδύνου
Δήλωση συμμόρφωσης με το καθεστώς μη αποκάλυψης / πολιτική απορρήτου της εταιρείας.	Προτεινόμενο προς υλοποίηση
Συμφωνία Εμπιστευτικότητας	

Μέτρα Προστασίας	Κατάσταση
Να υπογραφεί Συμφωνία Εμπιστευτικότητας με όλο το προσωπικό.	Προτεινόμενο προς υλοποίηση
Ο εργολάβος θα πρέπει να υπογράψει τη Συμφωνία Εμπιστευτικότητας, σχετικά με την ανάθεση της σύμβασης.	Προτεινόμενο προς υλοποίηση
Η εμπιστευτική συμφωνία θα πρέπει να ελέγχεται όταν υπάρχουν αλλαγές στους όρους πρόσληψης ή στα συμβόλαια εργασίας.	Προτεινόμενο προς υλοποίηση
Νομοθεσία Προστασίας Δεδομένων	
Εκπαίδευση στην Προστασία Δεδομένων	
Περιοδική εκπαίδευση συμμόρφωσης στην προστασία δεδομένων.	Προτεινόμενο προς υλοποίηση
Ο Υπεύθυνος Προστασίας Δεδομένων θα πρέπει να διασφαλίσει ότι οι νεοπροσλαμβανόμενοι υπάλληλοι έχουν εκπαιδευτεί κατάλληλα κατά την προετοιμασία τους.	Προτεινόμενο προς υλοποίηση
Ο Υπεύθυνος Προστασίας Δεδομένων θα πρέπει να διασφαλίσει ότι όλα τα μέλη του προσωπικού λαμβάνουν περιοδική εκπαίδευση στη προστασία δεδομένων.	Προτεινόμενο προς υλοποίηση
Έλεγχοι Συμμόρφωσης	
Έλεγχοι Συμμόρφωσης	
Έλεγχος ενσωμάτωσης των κατάλληλων αντιμέτρων.	Προτεινόμενο προς υλοποίηση
Υπεύθυνος ελέγχου, ώστε να πιστοποιεί τη συμμόρφωση των πολιτικών και των διαδικασιών που ακολουθούνται.	Προτεινόμενο προς υλοποίηση

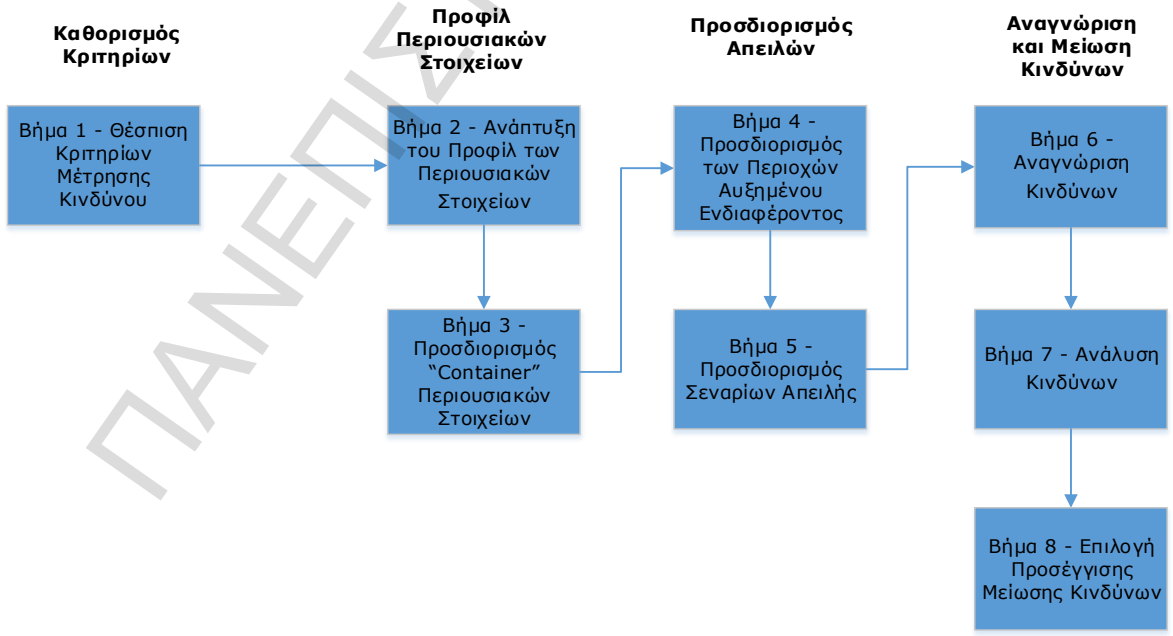
Πίνακας 12: Μέτρα προστασίας

Κεφάλαιο 3

Η μέθοδος OCTAVE Allegro

Η μέθοδος OCTAVE Allegro [10] έχει σχεδιαστεί για να επιτρέπει ευρεία αξιολόγηση του περιβάλλοντος του λειτουργικού κινδύνου μίας εταιρείας / ενός οργανισμού, με στόχο την παραγωγή πιο ισχυρών αποτελεσμάτων, χωρίς την ανάγκη για εκτεταμένη γνώση εκτίμησης του κινδύνου. Η προσέγγιση αυτή εστιάζει στον τρόπο με τον οποίο χρησιμοποιούνται τα περιουσιακά στοιχεία, το πού είναι αποθηκευμένα, πώς μεταφέρονται και υπόκεινται σε επεξεργασία, και πώς είναι εκτεθειμένα σε απειλές και ευπάθειες. Σε αντίθεση με την CRAMM, η OCTAVE Allegro δεν διαθέτει κάποιο εργαλείο, αλλά βασίζεται σε κατευθυντήριες οδηγίες, φύλλα εργασίας, και ερωτηματολόγια, με βάση τα οποία γίνεται η μελέτη.

Η μεθοδολογία αποτελείται από οκτώ βήματα που οργανώνονται σε τέσσερις φάσεις, όπως απεικονίζεται στην Εικόνα 4. Στη φάση 1, ο οργανισμός αναπτύσσει τα κριτήρια μέτρησης του κινδύνου σύμφωνα με τις οργανωτικές οδηγίες. Στη φάση 2 δημιουργούνται τα προφίλ των περιουσιακών στοιχείων και τα "containers" αυτών και καθορίζονται τα όριά τους. Στη φάση 3, προσδιορίζονται οι απειλές για το περιουσιακό στοιχείο. Στη φάση 4, προσδιορίζονται και αναλύονται οι κίνδυνοι για τα περιουσιακά στοιχεία και αναπτύσσεται η προσέγγιση για τον μετριασμό του κινδύνου.



Εικόνα 4: Βήματα και Φάσεις της Octave Allegro [10]

Παρακάτω περιγράφονται τα οκτώ βήματα της μεθοδολογίας Octave Allegro:

Βήμα 1: Θέσπιση Κριτηρίων Μέτρησης Κινδύνου (Establish Risk Measurement Criteria**)**

Το πρώτο βήμα καθορίζει το σύνολο των κριτηρίων που θα χρησιμοποιηθούν για την αξιολόγηση των επιπτώσεων κινδύνου. Τα κριτήρια μέτρησης του κινδύνου είναι ένα σύνολο ποιοτικών μέτρων έναντι των οποίων οι επιπτώσεις ενός κινδύνου μπορούν να σημειωθούν και να αποτελέσουν τη βάση μιας αξιολόγησης κινδύνου των περιουσιακών στοιχείων Επίσης, σε αυτό το βήμα μία εταιρεία / ένας οργανισμός πρέπει να αναγνωρίσει ποιες επιπτώσεις είναι πιο σημαντικές για τους επιχειρησιακούς στόχους. Για παράδειγμα, σε κάποιες εταιρείες μπορεί να είναι πιο σημαντικό το αντίκτυπο στη σχέση τους με τους πελάτες, από ότι η κανονιστική συμμόρφωση. Η μέθοδος παρέχει ένα σύνολο από φύλλα εργασίας (worksheets1-7) για τη δημιουργία αυτών των κριτηρίων για τις διάφορες επιπτώσεις.

Βήμα 2: Ανάπτυξη του Προφίλ των Αγαθών - Περιουσιακών Στοιχείων (Develop an Information Asset Profile)

Στο δεύτερο βήμα, αρχίζει η διαδικασία δημιουργίας ενός προφίλ για τα περιουσιακά στοιχεία μιας εταιρείας / ενός οργανισμού. Το προφίλ είναι μια αναπαράσταση των πληροφοριών ενός περιουσιακού στοιχείου, οι οποίες περιγράφουν τα μοναδικά χαρακτηριστικά του, τις ιδιότητες και την αξία του. Η διαδικασία δημιουργίας προφίλ, εξασφαλίζει ότι ένα περιουσιακό στοιχείο περιγράφεται με σαφήνεια και συνέπεια, ότι υπάρχει ένας σαφής καθορισμός των ορίων του περιουσιακού στοιχείου και ότι οι απαιτήσεις ασφάλειάς του ορίζονται επαρκώς. Το προφίλ για κάθε περιουσιακό στοιχείο καταγράφεται σε ένα ανεξάρτητο φύλλο εργασίας (worksheet) που αποτελεί τη βάση για τον προσδιορισμό των κινδύνων και απειλών στα επόμενα στάδια.

Βήμα 3: Προσδιορισμός "Container" Αγαθών - Περιουσιακών Στοιχείων (Identify Information Asset Container)

Τα "Containers" περιγράφουν τα μέρη όπου αποθηκεύονται, μεταφέρονται και υφίστανται επεξεργασία οι πληροφορίες των περιουσιακών στοιχείων. Οι πληροφορίες δεν βρίσκονται μόνο σε containers εντός των ορίων μιας εταιρείας / ενός οργανισμού, αλλά συχνά βρίσκονται σε χώρους που δεν είναι στον άμεσο έλεγχο της εταιρείας. Κάθε κίνδυνος που αναγνωρίζεται για το περιουσιακό στοιχείο επηρεάζει και τα containers αυτού.

Για παράδειγμα, πολλές εταιρείες αναθέτουν κάποιο μέρος των πληροφοριακών υποδομών τους σε παρόχους υπηρεσιών. Οι πάροχοι υπηρεσιών διαχειρίζονται τα αντικείμενα που περιέχουν τις πληροφορίες των περιουσιακών στοιχείων της εταιρείας. Εάν ένας πάροχος υπηρεσιών δεν είναι ενήμερος για τις απαιτήσεις ασφάλειας ενός περιουσιακού στοιχείου, ενδέχεται οι έλεγχοι που είναι αναγκαίοι για την προστασία του να μην είναι επαρκής, εκθέτοντας το περιουσιακό στοιχείο σε κίνδυνο.

Έτσι, για την απόκτηση ενός επαρκούς προφίλ κινδύνου ενός περιουσιακού στοιχείου, μια εταιρεία πρέπει να προσδιορίσει όλες τις τοποθεσίες όπου τα περιουσιακά στοιχεία αποθηκεύονται, μεταφέρονται, ή υποβάλλονται σε επεξεργασία, έστω και αν δεν βρίσκονται στον άμεσο έλεγχο της. Σε αυτό το βήμα, εντοπίζονται όλα τα containers στα οποία αποθηκεύεται, μεταφέρεται ή υπόκειται σε επεξεργασία ένα περιουσιακό στοιχείο, είτε είναι εσωτερικά της εταιρείας, είτε έχει ανατεθεί σε κάποιον πάροχο, προσδιορίζοντας έτσι τα όρια και τις μοναδικές συνθήκες που πρέπει να εξεταστούν για τον κίνδυνο.

Βήμα 4: Προσδιορισμός των Περιοχών Αυξημένου Ενδιαφέροντος (Identify Areas of Concern)

Στο τέταρτο βήμα, αρχίζει η διαδικασία εντοπισμού των κινδύνων μέσω του προβληματισμού για τις πιθανές συνθήκες ή καταστάσεις που μπορεί να απειλήσουν το περιουσιακό στοιχείο της εταιρείας. Ο σκοπός αυτού του βήματος δεν είναι να καταγράψει μια πλήρη λίστα με όλες τις πιθανές απειλές για ένα περιουσιακό στοιχείο αλλά να αποδώσει γρήγορα τις καταστάσεις που έρχονται αμέσως στο μυαλό της ομάδας ανάλυσης.

Βήμα 5: Προσδιορισμός Σεναρίων Απειλής (Identify Threat Scenarios)

Στο πρώτο μέρος του πέμπτου βήματος, οι τομείς ενδιαφέροντος που έχουν καθοριστεί στο προηγούμενο βήμα, επεκτείνονται σε σενάρια απειλών, τα οποία περιγράφουν με λεπτομέρεια τις ιδιότητες μιας απειλής. Όμως, η συλλογή των απειλών με βάση τους τομείς ενδιαφέροντος που προκαλούν ανησυχία, δεν αποτελεί απαραίτητα μια καλή εκτίμηση των πιθανών απειλών για το περιουσιακό στοιχείο της εταιρείας. Έτσι, στο δεύτερο μέρος του πέμπτου βήματος, εξετάζεται ένα ευρύ φάσμα επιπρόσθετων απειλών.

Βήμα 6: Αναγνώριση Κινδύνων (Identify Risks)

Στο έκτο βήμα, εντοπίζονται οι συνέπειες που θα υπάρξουν σε μία εταιρεία, εάν πραγματοποιηθεί μια απειλή, ολοκληρώνοντας έτσι την εικόνα του κινδύνου. Μια απειλή μπορεί να έχει πολλές πιθανές επιπτώσεις σε μία εταιρεία Για παράδειγμα, η διακοπή του συστήματος "e-commerce" μιας εταιρείας μπορεί να επηρεάσει τη φήμη της σε σχέση με τους πελάτες της, καθώς και την οικονομική της θέση. Οι δραστηριότητες που περιλαμβάνονται σε αυτό το βήμα εξασφαλίζουν ότι έχουν ληφθεί υπόψη οι διάφορες επιπτώσεις του κινδύνου.

Ο υπολογισμός του κινδύνου προκύπτει από την παρακάτω σχέση:

Κίνδυνος = Απειλή (κατάσταση) + Επίπτωση (Συνέπεια)
Κίνδυνος = [Βήμα 4 και 5] + [Βήμα 6]

Βήμα 7: Ανάλυση Κινδύνων (Analyze Risks)

Στο έβδομο βήμα, γίνεται μια απλή ποσοτική μέτρηση του βαθμού στον οποίο η εταιρεία επηρεάζεται από μια απειλή. Ο βαθμός κινδύνου υπολογίζεται λαμβάνοντας υπόψη το εύρος των συνεπειών που θα υπάρξουν για την εταιρεία, σε σχέση με την κρισιμότητα που θα έχει σε κάθε τομέα και με την πιθανότητα εμφάνισής του.

Με άλλα λόγια, αν η φήμη είναι πιο σημαντική, οι κίνδυνοι που έχουν αντίκτυπο στη φήμη, θα σημειώσουν υψηλότερες βαθμολογίες από τους κινδύνους που έχουν αντίκτυπο σε άλλη περιοχή. Με την ιεράρχηση των κριτηρίων των επιπτώσεων, η εταιρεία, εξασφαλίζει ότι οι κίνδυνοι θα ταξινομηθούν με βάση τις ανάγκες της

Για τον υπολογισμό του κινδύνου προστίθεται ο βαθμός προτεραιότητας που έχει οριστεί στο φύλλο εργασίας 7 (worksheet 7), με τον βαθμό επίπτωσης (Χαμηλός (1), Μεσαίος (2),Υψηλός (3)). Ο συνολικός βαθμός κινδύνου προκύπτει από το άθροισμα των βαθμών κινδύνου. Στον πίνακα 13 που ακολουθεί παρουσιάζεται ένα παράδειγμα υπολογισμού του κινδύνου.

Περιοχή επίπτωσης	Προτεραιότητα	Βαθμός Επίπτωσης	Βαθμός Κινδύνου
Φήμη	4	Μεσαίος (2)	**8**
Οικονομικά	5	Χαμηλός (1)	**5**
Παραγωγικότητα	3	Χαμηλός (1)	**3**
Ασφάλεια και Υγεία	1	Χαμηλός (1)	**1**
Πρόστιμα / Αγωγές	2	Υψηλός (3)	**6**
		Συνολικός Βαθμός	**23**

Πίνακας 13: Υπολογισμός Κινδύνου.

Βήμα 8: Επιλογή Προσέγγισης Μείωσης Κινδύνων (Select Mitigation Approach)

Το όγδοο βήμα είναι το τελικό βήμα της μεθόδου, όπου η εταιρεία καθορίζει ποιοί από τους κινδύνους που έχουν εντοπιστεί απαιτούν μετριασμό και αναπτύσσει μια στρατηγική για την αντιμετώπισή τους. Αρχικά γίνεται ταξινόμηση των κινδύνων με βάση τον συνολικό βαθμό κινδύνου που υπολογίστηκε στο προηγούμενο βήμα (Βήμα 7).

Στον πίνακα που ακολουθεί ταξινομούνται οι απειλές με βάση τη συνολική βαθμολογία τους και την πιθανότητα να συμβούν και χωρίζονται σε τέσσερις ομάδες επικινδυνότητας. Για παράδειγμα, αν η συνολική βαθμολογία ενός κινδύνου είναι 32 και η πιθανότητα εμφάνισης είναι υψηλή, τότε η απειλή κατατάσσεται στην ομάδα 1

Πιθανότητα	**Βαθμολογία**		
	30 - 45	**16 - 29**	**0 - 15**
Υψηλή	Ομάδα 1	Ομάδα 2	Ομάδα 2
Μεσαία	Ομάδα 2	Ομάδα 2	Ομάδα 3
Χαμηλή	Ομάδα 3	Ομάδα 3	Ομάδα 4

Πίνακας 14: Κατηγοριοποίηση Απειλών

Ανάλογα με την ομάδα (1 - 4) στην οποία ανήκει κάθε απειλή καθορίζεται ο τρόπος αντιμετώπισής της. Ο τρόπος αντιμετώπισης (Αποδοχή, Αναβολή, Μείωση, Μεταφορά) περιγράφεται στον πίνακα που ακολουθεί (Πίνακας 15).

Ομάδα	Προσέγγιση Μείωσης
Ομάδα 1	Μείωση
Ομάδα 2	Μείωση ή Αναβολή
Ομάδα 3	Αναβολή ή Αποδοχή
Ομάδα 4	Αποδοχή

Πίνακας 15: Προσέγγιση Μείωσης Κινδύνου

Για τους κινδύνους που έχουν γίνει αποδεκτοί είναι σημαντικό να πραγματοποιηθεί ένας επανέλεγχος των επιπτώσεων, με σκοπό την αποφυγή αποδοχής κρίσιμων κινδύνων και έπειτα ακολουθείται η στρατηγική για τον μετριασμό τους.

3.1 Εφαρμογή της Μεθόδου OCTAVE Allegro

Πριν το πρώτο βήμα της μεθόδου κρίνεται αναγκαίος ο προσδιορισμός του κρίσιμου περιουσιακού στοιχείου - αγαθού (critical asset), ο καθορισμός του οποίου προέκυψε έπειτα από συνεντεύξεις -ερωτηματολόγια με το αρμόδιο προσωπικό της εταιρείας Το Σύστημα Πελατών επιλέχτηκε ως κρίσιμο περιουσιακό στοιχείο του Π.Σ. γιατί κρίνεται απαραίτητο για τη συνέχιση της επιχειρηματικής δραστηριότητας της εταιρείας καθώς αποτελεί μοναδική πηγή εσόδων. Εν συνεχεία γίνεται ανάλυση της επικινδυνότητας για το κρίσιμο περιουσιακό στοιχείο (Σύστημα Πελατών) αλλά και για τα ακόλουθα βασικά περιουσιακά στοιχεία του Π.Σ.:

- Σύστημα Οικονομικής και Λογιστικής Διαχείρισης
- Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου
- Σύστημα Διαχείρισης Προσωπικού

3.1.1 Κρίσιμο Περιουσιακό Στοιχείο – Σύστημα Πελατών

Καθορισμός Κριτηρίων Μέτρησης Κινδύνου

AllegroWorksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Φήμη ***(Προσωπικό)***	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή ή καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια ή δαπάνη για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται μεγάλη προσπάθεια ή δαπάνη για να αποκατασταθεί.
Φήμη ***(Προμηθευτές, Εξωτερικοί Συνεργάτες)***	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια ή δαπάνη για την αποκατάσταση της φήμης της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μεγάλη προσπάθεια ή δαπάνη, για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται πάρα πολύ. Το κόστος αποκατάστασης υπερβαίνει το ποσό των 5.000€ για να αποκατασταθεί.
Φήμη ***(Πελάτες – Ευρύ κοινό)***	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται πολύ μεγάλη προσπάθεια ή δαπάνη, το κόστος της οποίας υπερβαίνει το ποσό των 5.000€ για να αποκατασταθεί.	Η φήμη της εταιρείας καταστρέφεται. Το κόστος αποκατάστασης υπερβαίνει το ποσό των 15.000€ για να αποκατασταθεί.

Allegro Worksheet 2	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΙΚΟΝΟΜΙΚΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Λειτουργικά Έξοδα	Αύξηση μικρότερη του 5% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση μεταξύ 5% και 10% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση περισσότερο από 10% σε ετήσιες λειτουργικές δαπάνες.
Απώλεια Εσόδων	Ετήσια οικονομική απώλεια μικρότερη των 1.000.000€.	Ετήσια οικονομική απώλεια μεταξύ 1.000.000€ και 10.000.000€.	Ετήσια οικονομική απώλεια μεγαλύτερη από 10.000.000€.

Allegro Worksheet 3	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ώρες Εργασίας ***Προσωπικού.***	Οι ώρες εργασίας του προσωπικού δεν αυξάνονται περισσότερο από 5%.	Οι ώρες εργασίας του προσωπικού αυξάνονται μεταξύ 5% και 20%.	Οι ώρες εργασίας του προσωπικού αυξάνονται περισσότερο από 20%.
Ώρες Εργασίας ***Εξειδικευμένου Προσωπικού (Τεχνικοί, Προγραμματιστές, Προνομιούχοι Χρήστες)***	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται ελάχιστα.	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται μεταξύ 10% και 15%.	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται περισσότερο από 15%.
Ώρες Εργασίας ***Ανώτερων Στελεχών:***	Οι ώρες εργασίας των ανωτέρων στελεχών δεν αυξάνονται περισσότερο από 2%.	Οι ώρες εργασίας των ανωτέρων στελεχών αυξάνονται μεταξύ 2% και 5%.	Οι ώρες εργασίας των ανωτέρων στελεχών αυξάνονται περισσότερο από 5%.

Allegro Worksheet 4	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ασφάλειας και υγείας	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 5	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Πρόστιμα - Αγωγές	Επιβολή προστίμων – αγωγών μικρότερη από 5.000€.	Επιβολή προστίμων – αγωγών μεταξύ 5.000€ και 50.000€ .	Επιβολή προστίμων – αγωγών μεγαλύτερων από μεγαλύτερων από 50.000€.

Allegro Worksheet 6	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ορίζονται από τον χρήστη	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 7	ΠΡΟΤΕΡΑΙΟΠΟΙΗΣΗ ΤΩΝ ΠΕΡΙΟΧΩΝ ΕΠΙΠΤΩΣΕΩΝ
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**ΠΕΡΙΟΧΕΣ ΕΠΙΠΤΩΣΕΩΝ**
3	**ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
4	**ΟΙΚΟΝΟΜΙΚΑ**
1	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
-	**ΥΓΕΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ**
2	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ**
-	**ΟΡΙΖΕΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ**

1 χαμηλός βαθμός επίπτωσης
4 μέγιστος βαθμός επίπτωσης

Ανάπτυξη του Προφίλ των Περιουσιακών Στοιχείων

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΟΥ ΠΕΡΙΟΥΣΙΑΚΟΥ ΣΤΟΙΧΕΙΟΥ	
(1) Κρίσιμο Περιουσιακό Στοιχείο	**(2) Αιτιολογία Επιλογής**	**(3) Περιγραφή**
Σύστημα Πελατών	Η εφαρμογή του συστήματος Πελατών έχει δημιουργηθεί ειδικά για τη συγκεκριμένη εταιρεία και σκοπός της είναι η υποστήριξη των λειτουργικών απαιτήσεων του τμήματος Πωλήσεων.	Το περιουσιακό στοιχείο περιλαμβάνει τις ακόλουθες πληροφορίες που είναι απαραίτητες για την εύρυθμη λειτουργία της εταιρείας • Διαχείριση πελατών / μετρητών • Πληρωμή και παρακολούθηση πληρωμών • Τιμολόγηση και έκδοση λογαριασμού • Παρακολούθηση διακοπών-αποκοπών / ενδείξεων • Λογιστική παρακολούθηση • Έκδοση αναφορών και στατιστικών • Είσπραξη εισφορών για θυγατρικές εταιρείες
(4)Ιδιοκτήτης/ες		
Αντώνιος Παπαδόπουλος		
(5) Απαιτήσεις Ασφάλειας		
❑ **Εμπιστευτικότητα**	Μόνο το εξουσιοδοτημένο προσωπικό και σε εξαιρετικές περιπτώσεις άτομα από τα ανώτερα στελέχη και το τεχνικό προσωπικό μπορούν να δουν αυτές τις πληροφορίες.	
❑ **Ακεραιότητα**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει αυτές τις πληροφορίες.	
❑ **Διαθεσιμότητα**	Αυτό το περιουσιακό στοιχείο πρέπει να είναι διαθέσιμο για το προσωπικό για τη διεκπεραίωση των εργασιών τους, όπως: διαχείριση πελατών, πληρωμή λογαριασμών / τιμολογίων, καθώς και για είσπραξη εισφορών.	
❑ **Άλλο**	Αυτό το αγαθό δεν έχει ιδιαίτερες απαιτήσεις κανονιστικής συμμόρφωσης.	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας		
❑ Εμπιστευτικότητα	❑ Ακεραιότητα	✓ **Διαθεσιμότητα** ❑ Άλλο

Προσδιορισμός "Container" Περιουσιακών Στοιχείων

Allegro Worksheet 9a	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΤΕΧΝΙΚΑ)
ΕΣΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Το σύστημα Πελατών αποτελείται από το "mainframe Z10" της IBM, με λειτουργικό σύστημα z/OS (zero downtime), και δύο συσκευές λήψης αντιγράφων.	Τμήμα Πληροφορικής
Εσωτερικό δίκτυο εταιρείας: Όλες οι συναλλαγές που αφορούν το σύστημα Πελατών γίνονται εντός του κλειστού εσωτερικού δικτύου (intranet).	Τμήμα Πληροφορικής Τμήμα Δικτύων
Σταθμοί εργασίας και κάποια "dumb" τερματικά	Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
-	-

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΦΥΣΙΚΑ)
ΕΣΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Ταινίες και δίσκοι αντιγράφων ασφαλείας στα οποία αποθηκεύονται στο τέλος κάθε ημέρας και στο τέλος κάθε εβδομάδας τα δεδομένα του συστήματος.	Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
-	-

Allegro Worksheet 9c	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΟΝΟΜΑ/ΡΟΛΟΙ/ΑΡΜΟΔΙΟΤΗΤΕΣ		**ΤΜΗΜΑ / ΤΟΜΕΑΣ**
Προσωπικό Πληροφορικής και Δικτύων		Τμήμα Πληροφορικής
		Τμήμα Δικτύων
Διοικητικό προσωπικό & Οικονομικό προσωπικό		Οικονομικό Τμήμα
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΠΡΟΜΗΘΕΥΤΕΣ, ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΕΡΓΑΤΕΣ Κ.Τ.Λ.		**ΟΡΓΑΝΙΣΜΟΣ**
Κατασκευαστές / προμηθευτές		IBM

Προσδιορισμός των Συνθηκών που λαμβάνονται υπόψη / Σεναρίων Απειλής και Αναγνώριση Κινδύνων

Allegro - Worksheet 10		**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**		
	Περιουσιακό Στοιχείο	**Σύστημα Πελατών**		
Κίνδυνοι Περιουσιακών Στοιχείων	Τομείς Ενδιαφέροντος	***Πλαστοπροσωπία ταυτότητας χρήστη***		
Απειλή	**(1) Δράστης** (Actor)	Δυσαρεστημένος υπάλληλος / εξωτερικός συνεργάτης ή κάποιος που ενεργεί εις βάρος της εταιρείας.		
	(2) Μέσα (Means)	Εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη ή εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου.		
	(3) Κίνητρο (Motive)	Αποκόμιση οικονομικού οφέλους, ηθική ικανοποίηση.		
	(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ **Τροποποίηση**	❑ Καταστροφή ❑ Διακοπή	
	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν υποκλέπτοντας την ταυτότητα κάποιου εξουσιοδοτημένου χρήστη.		
	(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία	❑ Χαμηλή
(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
Εκτιμάται ότι θα υπάρξει οικονομική απώλεια για την εταιρεία λαμβάνοντας υπόψη περιπτώσεις λαθών σε λογαριασμούς / τιμολόγια και σε εισπράξεις τελών για θυγατρικές εταιρείες. Επιπλέον, μπορεί ο εισβολέας να αποκομίσει κέρδος αλλάζοντας τις χρεώσεις του λογαριασμού του. Σε περίπτωση αποκάλυψης πληροφοριών επηρεάζεται η φήμη της εταιρείας και ενδέχεται να υπάρξουν νομικές κυρώσεις.		Φήμη – Εμπιστοσύνη Πελατών	Υψηλός	9
		Οικονομικά	Υψηλός	12
		Παραγωγικότητα	-	0
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	Μεσαίος	4
		Ορίζονται από τον χρήστη	-	0
			Συνολικός Βαθμός Κινδύνου	**25**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Σύστημα Πελατών	• Καταγραφή αρχείων που έχουν προσπελαστεί. • Κρυπτογράφηση των κωδικών πρόσβασης. • Μηχανισμός κλειδώματος λογαριασμού έπειτα από τρεις αποτυχημένες προσπάθειες.		
Εσωτερικό Δίκτυο	• Μηχανισμός ασφάλειας που μπορεί να δείξει ποιος έχει αιτηθεί πρόσβαση σε κάποιο αρχείο. • Έλεγχος δραστηριοτήτων χρηστών και ενημέρωση ότι η κίνηση τους καταγράφεται. • Ανασκόπηση αποτυχημένων προσπαθειών πρόσβασης.		
Όλο το εμπλεκόμενο προσωπικό	• Ενημέρωση χρηστών σε θέματα ασφάλειας και ειδικότερα στη δημιουργία ισχυρών κωδικών.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Πελατών**	
		Τομείς Ενδιαφέροντος	***Εισαγωγή Κακόβουλου Κώδικα***	
		(1) Δράστης (Actor)	***"Hacker"***	
		(2) Μέσα (Means)	Με την αποστολή κάποιου "email" ή δίνοντας κάποιο αποσπώμενο δίσκο σε υπάλληλο της εταιρείας.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας (SecurityRequirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εισαγωγή κακόβουλου κώδικα, καθώς το σύστημα ενδέχεται να μην είναι διαθέσιμο.	
		(6) Πιθανότητα (Probability)	❑ **Υψηλή**	✓ **Μεσαία** ❑ **Χαμηλή**
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Μπορεί να επιφέρει οικονομική απώλεια στην εταιρεία, που προκύπτει από το κόστος αποκατάστασης του συστήματος και από τις εργατοώρες που θα χρειαστούν για τον έλεγχο ορθότητας των δεδομένων.		Φήμη - Εμπιστοσύνη πελατών	Μεσαίος / 6
			Οικονομικά	Υψηλός / 12
			Παραγωγικότητα	Μεσαίος / 2
			Ασφάλεια και Υγεία	- / 0
			Πρόστιμα και Αγωγές	- / 0
			Ορίζονται από τον χρήστη	- / 0
			Συνολικός Βαθμός Κινδύνου	**20**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Λήψη μέτρων έτσι ώστε να μην υπάρχει δυνατότητα χρήσης αποσπώμενων συσκευών, εκτός από εξαιρετικές περιπτώσεις, και ύστερα από άδεια του Υπεύθυνου Ασφάλειας. • Δημιουργία Πολιτικής Αναφοράς και Διαχείρισης Περιστατικών Ασφάλειας.		
Όλο το εμπλεκόμενο προσωπικό	• Ανακοίνωση και αποδοχή των πολιτικών. • Ευαισθητοποίηση σε θέματα που αφορούν το Κακόβουλο Λογισμικό.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Πελατών**	
		Τομείς Ενδιαφέροντος	***Φωτιά***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος που έχει πρόσβαση σε χώρους κοντινούς του computer room. Ανυπαρξία ελέγχου / συντήρησης.	
		(2) Μέσα (Means)	Πετώντας κάποιο εύφλεκτο υλικό.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	✓ **Καταστροφή** ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εκδήλωση φωτιάς, καθώς υπάρχει πιθανότητα καταστροφής του computer room. Η εταιρεία διαθέτει σύστημα πυρανίχνευσης αλλά δεν γίνεται ο προκαθορισμένος έλεγχος αυτού και επιπλέον δεν διαθέτει αυτόματο σύστημα πυρόσβεσης.	
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία** ❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Σε περίπτωση καταστροφής του συστήματος, θα πρέπει να δημιουργηθεί εκ νέου σε κάποια άλλη τοποθεσία, γιατί διαφορετικά δημιουργείται πρόβλημα ρευστότητας με αποτέλεσμα την πιθανή αδυναμία εκπλήρωσης των χρηματικών υποχρεώσεων της εταιρείας. Επιπλέον, μπορεί να μην είναι εφικτή η τήρηση των νομικών υποχρεώσεων, καθώς η εταιρεία θα αδυνατεί να τηρήσει τις συμβάσεις με τις τράπεζες. Εάν η καταστροφή του συστήματος γίνει γνωστή στο κοινό αμαυρώνεται η φήμη της εταιρείας.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός	9
			Οικονομικά	Υψηλός	12
			Παραγωγικότητα	Υψηλός	3
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	Υψηλός	6
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**30**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Computer Room, λοιποί χώροι	• Να γίνει εγκατάσταση αυτόματου συστήματος πυρόσβεσης. • Να γίνεται ο προκαθορισμένος έλεγχος του συστήματος πυρανίχνευσης.		
Όλο το προσωπικό	• Απαγόρευση καπνίσματος σε κλειστούς χώρους. • Εκπαίδευση προσωπικού σε περιπτώσεις πυρκαγιάς.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Πελατών**	
		Τομείς Ενδιαφέροντος	***Διακοπή Ηλεκτροδότησης***	
		(1) Δράστης (Actor)	-	
		(2) Μέσα (Means)	-	
		(3) Κίνητρο (Motive)	-	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς χωρίς ρεύμα υπάρχει διακοπή της λειτουργίας του συστήματος. Το σύστημα διαθέτει μονάδες αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS) και γεννήτρια πετρελαίου.	
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία** ❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Μπορεί να μειώσει την παραγωγικότητα για όσο διάστημα δεν ηλεκτροδοτείται το σύστημα. Σε περίπτωση μη λειτουργίας των UPS ή της γεννήτριας, μπορεί να υπάρξει βλάβη σε κάποιο συστατικό του συστήματος επιφέροντας οικονομικό κόστος που προκύπτει από την αντικατάσταση του.		Φήμη - Εμπιστοσύνη πελατών	- / 0
			Οικονομικά	Χαμηλός / 4
			Παραγωγικότητα	Υψηλός / 3
			Ασφάλεια και Υγεία	- / 0
			Πρόστιμα και Αγωγές	- / 0
			Ορίζονται από τον χρήστη	- / 0
				Συνολικός Βαθμός Κινδύνου / **7**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	✓ **Αναβολή**	❑ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Υπεύθυνος Συντήρησης Εξο-πλισμού	• Τακτικός έλεγχος της σωστής λειτουργίας των UPS και της γεννήτριας.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Πελατών**	
		Τομείς Ενδιαφέροντος	***Κλοπή Υλικού / Εξοπλισμού / Δεδομένων***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος, επισκέπτης.	
		(2) Μέσα (Means)	Θα μπορούσε οποιοσδήποτε υπάλληλος ή επισκέπτης έχοντας πρόσβαση στις εγκαταστάσεις να κλέψει αποσπώμενες συσκευές η κασέτες αποθήκευσης εφεδρικών αντιγράφων που περιέχουν δεδομένα του συγκεκριμένου συστήματος. Επίσης αποκτώντας πρόσβαση σε κάποιο σταθμό εργασίας ή στο δίκτυο (κατά τη μεταφορά αρχείων) μπορεί να κλαπούν ηλεκτρονικά αρχεία του συγκεκριμένου συστήματος.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση και Οικονομικό όφελος.	
		(4) Αποτέλεσμα (Outcome)	✓ **Αποκάλυψη** ❑ Τροποποίηση	❑ Καταστροφή ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν, καθώς η πρόσβαση στους χώρους δεν ελέγχεται και οι χρήστες δεν κλειδώνουν τα γραφεία και τους σταθμούς εργασίας τους πριν την αποχώρηση τους από το χώρο. Δεν γίνεται χρήση ασφαλούς πρωτοκόλλου κατά τη μεταφορά αρχείων. Παρόλο που η είσοδος στο computer room επιτρέπεται μόνο με χρήση μαγνητικών καρτών, η πόρτα ανοίγει τραβώντας τη με δύναμη χωρίς να ενεργοποιείται κάποιος συναγερμός.	
		(6) Πιθανότητα (Probability)	✓ Υψηλή	Μεσαία	Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Η αποκάλυψη δεδομένων θα μπορούσε να οδηγήσει σε απώλεια καλής φήμης για την εταιρεία. Επίσης, μπορεί να υπάρξουν αγωγές εις βάρος της εταιρείας σε περίπτωση που κλαπούν δεδομένα που περιέχουν προσωπικά στοιχεία πελατών, δεδομένα λογαριασμών και τιμολογίων, στοιχεία προμηθευτών κ.ά.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός	9
			Οικονομικά	Υψηλός	12
			Παραγωγικότητα	-	-
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	Υψηλός	6
			Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου					**27**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Δημιουργία πολιτικής Φυσικής Ασφάλειας και Φυσικής Πρόσβασης • Ανακοίνωση της πολιτικής και αποδοχή της. • Να γίνεται έλεγχος της απογραφής τουλάχιστον μία φορά κάθε 6 μήνες. • Αντικατάσταση του πρωτοκόλλου ftp με πιο ασφαλές πρωτόκολλο (π.χ. sftp).		
Όλο το προσωπικό	• Κάθε εργαζόμενος λύνοντας τη σχέση εργασίας του με την εταιρεία να υποχρεούται να υπογράψει μια δήλωση που να αναφέρει ότι έχει επιστρέψει όλα τα περιουσιακά στοιχεία που ανήκουν στην εταιρεία		
Computer Room	• Να ελεγχθεί η σωστή λειτουργία του συστήματος καρτών για την πρόσβαση στο computer room και να εγκατασταθεί μηχανισμός συναγερμού σε περίπτωση βίαιης εισόδου στο χώρο.		
Φύλακες	• Να γίνεται έλεγχος σε τσάντες / σάκους κ.τ.λ. κατά την είσοδο και έξοδο από το χώρο έτσι ώστε, να αποφευχθεί η κλοπή υλικού. • Να επιτρέπεται η είσοδος ακολουθώντας την πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης.		

3.1.2 Σύστημα Οικονομικής και Λογιστικής Διαχείρισης

Καθορισμός Κριτηρίων Μέτρησης Κινδύνου

Allegro Worksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Φήμη (Προσωπικό)	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια ή δαπάνη για την αποκατάσταση της φήμης της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια ή δαπάνη για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ. Και απαιτείται μεγάλη προσπάθεια για να αποκατασταθεί.
Φήμη (Προμηθευτές, Εξωτερικοί Συνεργάτες)	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια ή δαπάνη για την αποκατάσταση της φήμης της.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται πολύ μεγάλη προσπάθεια ή δαπάνη, το κόστος της οποίας υπερβαίνει το ποσό των 2.000€.	Η φήμη της εταιρείας επηρεάζεται πάρα πολύ. Το κόστος αποκατάστασης υπερβαίνει το ποσό των 5.000€ για να αποκατασταθεί.
Φήμη (Ευρύ κοινό)	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια ή δαπάνη για την αποκατάσταση της φήμης της.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται πολύ μεγάλη προσπάθεια ή δαπάνη για να αποκατασταθεί.	Η φήμη της εταιρείας καταστρέφεται. Το κόστος αποκατάστασης υπερβαίνει το ποσό των 10.000€ για να αποκατασταθεί.

Allegro Worksheet 2	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΙΚΟΝΟΜΙΚΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Λειτουργικά Έξοδα	Αύξηση μικρότερη του 2% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση μεταξύ 2% και 5% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση περισσότερο από 5% σε ετήσιες λειτουργικές δαπάνες.
Απώλεια Εσόδων	Ετήσια οικονομική απώλεια μικρότερη των 10.000€.	Ετήσια οικονομική απώλεια μεταξύ 10.000€ και 20.000€.	Ετήσια οικονομική απώλεια μεγαλύτερη από 20.000€.

Allegro Worksheet 3	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ – ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ώρες Εργασίας Προσωπικού	Οι ώρες εργασίας του προσωπικού δεν αυξάνονται περισσότερο από 2%	Οι ώρες εργασίας του προσωπικού αυξάνονται μεταξύ 2% και 10%	Οι ώρες εργασίας του προσωπικού αυξάνονται περισσότερο από 10%
Ώρες Εργασίας Εξειδικευμένου Προσωπικού (Τεχνικοί, Προγραμματιστές, Προνομιούχοι Χρήστες)	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται ελάχιστα	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται μεταξύ 2% και 5%	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται περισσότερο από 5%
Ώρες Εργασίας Ανώτερων Στελεχών	Οι ώρες εργασίας των ανωτέρων στελεχών δεν αυξάνονται.	Οι ώρες εργασίας των ανωτέρων στελεχών αυξάνονται μεταξύ 1% και 5%	Οι ώρες εργασίας των ανωτέρων στελεχών αυξάνονται περισσότερο από 5%

Allegro Worksheet 4	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ασφάλεια και υγεία	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 5	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Πρόστιμα - Αγωγές	Επιβολή προστίμων - αγωγών μικρότερη από 5.000€.	Επιβολή προστίμων – αγωγών μεταξύ 5.000€ και 30.000€ .	Επιβολή προστίμων – αγωγών μεγαλύτερων από μεγαλύτερων από 30.000€.

Allegro Worksheet 6	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ορίζονται από τον χρήστη	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 7	ΠΡΟΤΕΡΑΙΟΠΟΙΗΣΗ ΤΩΝ ΠΕΡΙΟΧΩΝ ΕΠΙΠΤΩΣΕΩΝ
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**ΠΕΡΙΟΧΕΣ ΕΠΙΠΤΩΣΕΩΝ**
1	**ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
4	**ΟΙΚΟΝΟΜΙΚΑ**
2	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
-	**ΥΓΕΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ**
3	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ**
-	**ΟΡΙΖΕΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ**

1 χαμηλός βαθμός επίπτωσης
4 μέγιστος βαθμός επίπτωσης

Ανάπτυξη του Προφίλ των Περιουσιακών Στοιχείων

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΟΥ ΠΕΡΙΟΥΣΙΑΚΟΥ ΣΤΟΙΧΕΙΟΥ	
(1) Κρίσιμο Περιουσιακό Στοιχείο	**(2) Αιτιολογία Επιλογής**	**(3) Περιγραφή**
Σύστημα Οικονομικής & Λογιστικής Διαχείρισης	Το σύστημα Οικονομικής και Λογιστικής Διαχείρισης δημιουργήθηκε για να καλύψει τις λειτουργικές απαιτήσεις του Οικονομικού και Λογιστικού τμήματος.	Το περιουσιακό στοιχείο περιλαμβάνει όλες τις ακόλουθες εφαρμογές: • Γενικής – Αναλυτικής Λογιστικής • Διαχείρισης Προϋπολογισμού • Διαχείρισης Κεφαλαίων • Διαχείρισης Εισπράξεων Πληρωμών • Διαχείρισης Προμηθειών - Αποθήκης • Διαχείρισης Πάγιων Στοιχείων • Τήρηση Λογιστικών Βιβλίων & Καταστάσεων • Λογιστικής Διαχείρισης Έργων
(4)ιδιοκτήτης/ες		
Σεραφείμ Δημητρακόπουλος		
(5) Απαιτήσεις Ασφάλειας		
❑ **Εμπιστευτικότητα**	Μόνο το εξουσιοδοτημένο προσωπικό του Οικονομικού και Λογιστικού τμήματος και σε εξαιρετικές περιπτώσεις κάποια άτομα από τα ανώτερα στελέχη και από το εξειδικευμένο προσωπικό μπορούν να δουν αυτές τις πληροφορίες	
❑ **Ακεραιότητα**	Μόνο το εξειδικευμένο προσωπικό του Οικονομικού και Λογιστικού τμήματος μπορεί να τροποποιήσει αυτές τις πληροφορίες.	
❑ **Διαθεσιμότητα**	Το σύστημα θα πρέπει να είναι διαθέσιμο για να καλύψει τις λειτουργικές απαιτήσεις του Οικονομικού και Λογιστικού τμήματος	
❑ **Άλλο**	Αυτό το αγαθό δεν έχει ιδιαίτερες απαιτήσεις κανονιστικής συμμόρφωσης-	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας		
❑ Εμπιστευτικότητα	✓ **Ακεραιότητα**	❑ Διαθεσιμότητα ❑ Άλλο

Προσδιορισμός "Container" Περιουσιακών Στοιχείων

Allegro Worksheet 9a	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΤΕΧΝΙΚΑ)	
ΕΣΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ "CONTAINER"		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Το σύστημα Οικονομικής &Λογιστικής Διαχείρισης αποτελείται από τέσσερεις εξυπηρετητές εφαρμογών (Application Servers) DELL poweredge 2950 Redhat Enterprise Linux 4.6 64bit και δύο εξυπηρετητές βάσεων δεδομένων (Database servers) DELL poweredge R 900 Redhat Enterprise Linux 4.6 64bit,		Οικονομικό Τμήμα
Εσωτερικό δίκτυο εταιρείας: Όλες οι συναλλαγές που αφορούν το σύστημα γίνονται εντός του κλειστού εσωτερικού δικτύου (intranet).		Τμήμα Πληροφορικής
		Τμήμα Δικτύων
Σταθμοί εργασίας		Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ "CONTAINER"		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΦΥΣΙΚΑ)	
ΕΣΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ "CONTAINER"		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Ταινίες και δίσκοι αντιγράφων ασφαλείας στα οποία αποθηκεύονται στο τέλος κάθε ημέρας και στο τέλος κάθε εβδομάδας τα δεδομένα του συστήματος.		Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ "CONTAINER"		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9c	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΟΝΟΜΑ/ΡΟΛΟΙ/ΑΡΜΟΔΙΟΤΗΤΕΣ		**ΤΜΗΜΑ / ΤΟΜΕΑΣ**
Προσωπικό Πληροφορικής και Δικτύων		Τμήμα Πληροφορικής
		Τμήμα Δικτύων
Οικονομικό προσωπικό		Οικονομικό Τμήμα
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΠΡΟΜΗΘΕΥΤΕΣ, ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΕΡΓΑΤΕΣ Κ.Τ.Λ.		**ΟΡΓΑΝΙΣΜΟΣ**
		-

Προσδιορισμός των Συνθηκών που λαμβάνονται υπόψη / Σεναρίων Απειλής και Αναγνώριση Κινδύνων

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Οικονομικής και Λογιστικής Διαχείρισης**	
		Τομείς Ενδιαφέροντος	***Πλαστοπροσωπία ταυτότητας χρήστη***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος / εξωτερικός συνεργάτης ή κάποιος που ενεργεί εις βάρος της εταιρείας.	
		(2) Μέσα (Means)	Εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη ή εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ **Τροποποίηση**	❑ Καταστροφή ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς στο σύστημα διαθέτουν πρόσβαση περισσότεροι από τους απαιτούμενους χρήστες. Επίσης ο αριθμός αποδεκτών αποτυχημένων προσπαθειών για την αυθεντικοποίηση των χρηστών σε ένα σταθμό εργασίας είναι πάνω από 10.	
		(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία ❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Στην περίπτωση αλλοίωσης των δεδομένων μπορεί να υπάρξει μικρή οικονομική απώλεια η οποία προέρχεται από το κόστος σε εργατοώρες που θα χρειαστούν για τον έλεγχο και διόρθωση των δεδομένων. Στην περίπτωση αποκάλυψης των δεδομένων επηρεάζεται η καλή εικόνα της εταιρείας. Επίσης, περιλαμβάνονται επιχειρησιακά ευαίσθητα δεδομένα τα οποία δεν πρέπει να είναι διαθέσιμα στο ευρύ κοινό και υπάρχει περίπτωση νομικών κυρώσεων που θα επιφέρουν πρόστιμο για την εταιρεία.		Φήμη - Εμπιστοσύνη πελατών	Μεσαίος	2
			Οικονομικά	Μεσαίος	8
			Παραγωγικότητα	Χαμηλός	2
			Ασφάλεια και υγεία	-	0
			Πρόστιμα και Αγωγές	Μεσαίος	6
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**18**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Σύστημα Οικονομικής & Λογιστικής Διαχείρισης	• Δικαιώματα για δημιουργία, τροποποίηση και διαγραφή της βάσης δεν απαιτούνται σε περιβάλλον παραγωγής και πρέπει να περιοριστούν.		
Σταθμοί Εργασίας	• Καταγραφή της ώρας εισόδου / εξόδου του σταθμού εργασίας. • Μείωση του χρόνου που απαιτείται για το αυτόματο κλείδωμα της οθόνης και ενημέρωση των χρηστών για το χειροκίνητο κλείδωμα σε περίπτωση απουσίας τους από το χώρο. • Μείωση των επιτρεπόμενων αποτυχημένων προσπαθειών εισόδου στους σταθμούς εργασίας. Συνιστάται ο κωδικός του χρήστη να κλειδώνει έπειτα από 3 αποτυχημένες προσπάθειες.		
Όλο το εμπλεκόμενο προσωπικό	• Κατάλληλη εκπαίδευση νέων χρηστών.		

Allegro - Worksheet 10			ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Οικονομικής και Λογιστικής Διαχείρισης**		
		Τομείς Ενδιαφέροντος	***Εισαγωγή Κακόβουλου Κώδικα***		
		(1) Δράστης (Actor)	Οποιοσδήποτε που θα είχε ως στόχο να βλάψει την εταιρεία.		
		(2) Μέσα (Means)	Με την αποστολή κάποιου "email" ή δίνοντας κάποιο αποσπώμενο δίσκο σε υπάλληλο της εταιρείας.		
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.		
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εισαγωγή κακόβουλου κώδικα.		
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία**	❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Μπορεί να επιφέρει οικονομική απώλεια στην εταιρεία, που προκύπτει από το κόστος αποκατάστασης του συστήματος και από τις εργατοώρες που θα χρειαστούν για τον έλεγχο ορθότητας των δεδομένων. Σε περίπτωση αποκάλυψης του συμβάντος επηρεάζεται η φήμη της εταιρείας.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός	3
			Οικονομικά	Υψηλός	8
			Παραγωγικότητα	Μεσαίος	4
			Ασφάλεια και υγεία	-	0
			Πρόστιμα και Αγωγές	-	0
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**15**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Λήψη μέτρων έτσι ώστε να μην υπάρχει δυνατότητα χρήσης αποσπώμενων συσκευών, εκτός από εξαιρετικές περιπτώσεις, και ύστερα από άδεια του Υπεύθυνου Ασφάλειας. • Δημιουργία πολιτικής Αναφοράς και διαχείρισης περιστατικών Ασφάλειας.		
Όλο το εμπλεκόμενο προσωπικό	• Αποδοχή πολιτικής .		

<table>
<tr><td colspan="3">Allegro - Worksheet 10</td><td colspan="4">ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ</td></tr>
<tr><td rowspan="11">Κίνδυνοι Περιουσιακών Στοιχείων</td><td rowspan="9">Απειλή</td><td>Περιουσιακό Στοιχείο</td><td colspan="4">Σύστημα Οικονομικής και Λογιστικής Διαχείρισης</td></tr>
<tr><td>Τομείς Ενδιαφέροντος</td><td colspan="4">Φωτιά</td></tr>
<tr><td>(1) Δράστης (Actor)</td><td colspan="4">Δυσαρεστημένος υπάλληλος που έχει πρόσβαση σε χώρους κοντινούς του computer room.
Ανυπαρξία έλεγχου / συντήρησης.</td></tr>
<tr><td>(2) Μέσα (Means)</td><td colspan="4">Πετώντας κάποιο εύφλεκτο υλικό.</td></tr>
<tr><td>(3) Κίνητρο (Motive)</td><td colspan="4">Ηθική ικανοποίηση.</td></tr>
<tr><td>(4) Αποτέλεσμα
(Outcome)</td><td colspan="2">❑ Αποκάλυψη
❑ Τροποποίηση</td><td colspan="2">✓ Καταστροφή
❑ Διακοπή</td></tr>
<tr><td>(5) Απαιτήσεις Ασφάλειας
(Security Requirements)</td><td colspan="4">Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εκδήλωση φωτιάς καθώς υπάρχει πιθανότητα καταστροφής του computer room Η εταιρεία διαθέτει σύστημα πυρανίχνευσης, αλλά δεν γίνεται ο προκαθορισμένος έλεγχος αυτού και επιπλέον δεν διαθέτει αυτόματο σύστημα πυρόσβεσης.</td></tr>
<tr><td>(6) Πιθανότητα
(Probability)</td><td>❑ Υψηλή</td><td>✓ Μεσαία</td><td>❑ Χαμηλή</td><td></td></tr>
<tr><td colspan="2" rowspan="2">(7) Συνέπειες
(Consequences)</td><td colspan="4">(8) Βαρύτητα (Severity)</td></tr>
<tr><td>Περιοχή Επίπτωσης</td><td>Βαθμός Κινδύνου (Value)</td><td>Βαθμός Αποτίμησης (Score)</td></tr>
<tr><td colspan="2" rowspan="6">Η ολική καταστροφή μπορεί να προκαλέσει οικονομική απώλεια και αδυναμία τήρησης των νομικών και κανονιστικών απαιτήσεων, διότι είναι αδύνατη η αποπληρωμή δανείων και επιταγών προς τρίτους και επιπλέον μπορούν να υπάρξουν μηνύσεις εις βάρος της εταιρείας. Το οικονομικό κόστος προκύπτει από τις ώρες - εργατοώρες που απαιτούνται για την αποκατάσταση της σωστής λειτουργίας του συστήματος. Εάν η καταστροφή του συστήματος γίνει γνωστή στο κοινό αμαυρώνεται η φήμη της εταιρείας.</td><td>Φήμη - Εμπιστοσύνη πελατών</td><td>Υψηλός-</td><td>3</td></tr>
<tr><td>Οικονομικά</td><td>Υψηλός-</td><td>12</td></tr>
<tr><td>Παραγωγικότητα</td><td>Υψηλός-</td><td>6</td></tr>
<tr><td>Ασφάλεια και Υγεία</td><td>-</td><td>0</td></tr>
<tr><td>Πρόστιμα και Αγωγές</td><td>Υψηλός-</td><td>9</td></tr>
<tr><td>Ορίζονται από τον χρήστη</td><td>-</td><td>0</td></tr>
<tr><td colspan="5">Συνολικός Βαθμός Κινδύνου</td><td>30</td></tr>
</table>

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Computer Room, λοιποί χώροι	• Να γίνει εγκατάσταση αυτόματου συστήματος πυρόσβεσης . • Να γίνεται ο προκαθορισμένος έλεγχος του συστήματος πυρανίχνευσης.		
Όλο το προσωπικό	• Απαγόρευση καπνίσματος σε κλειστούς χώρους. • Εκπαίδευση προσωπικού σε περιπτώσεις πυρκαγιάς.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Οικονομικής και Λογιστικής Διαχείρισης**	
		Τομείς Ενδιαφέροντος	***Διακοπή Ηλεκτροδότησης***	
		(1) Δράστης (Actor)	-	
		(2) Μέσα (Means)	-	
		(3) Κίνητρο (Motive)	-	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς χωρίς ρεύμα, υπάρχει διακοπή της λειτουργίας του συστήματος. Το σύστημα διαθέτει μονάδες αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS) και γεννήτρια πετρελαίου.	
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία** ❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Μπορεί να μειώσει την παραγωγικότητα για όσο διάστημα δεν ηλεκτροδοτείται το σύστημα. Σε περίπτωση μη λειτουργίας των UPS ή της γεννήτριας μπορεί να υπάρξει βλάβη σε κάποιο συστατικό του συστήματος επιφέροντας οικονομικό κόστος που προκύπτει από την αντικατάστασή του.		Φήμη - Εμπιστοσύνη πελατών	- / 0
			Οικονομικά	Χαμηλός / 4
			Παραγωγικότητα	Μεσαίος / 4
			Ασφάλεια και Υγεία	- / 0
			Πρόστιμα και Αγωγές	- / 0
			Ορίζονται από τον χρήστη	- / 0
				Συνολικός Βαθμός Κινδύνου / **8**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	✓ **Αναβολή**	❑ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Υπεύθυνος Συντήρησης Εξοπλισμού	• Τακτικός έλεγχος της σωστής λειτουργίας των UPS και της γεννήτριας.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Οικονομικής και Λογιστικής Διαχείρισης**	
		Τομείς Ενδιαφέροντος	***Κλοπή Υλικού / Εξοπλισμού / Δεδομένων***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος, επισκέπτης.	
		(2) Μέσα (Means)	Θα μπορούσε οποιοσδήποτε υπάλληλος ή επισκέπτης έχοντας πρόσβαση στις εγκαταστάσεις να κλέψει αποσπώμενες συσκευές η κασέτες αποθήκευσης εφεδρικών αντιγράφων που περιέχουν δεδομένα του συγκεκριμένου συστήματος. Επίσης αποκτώντας πρόσβαση σε κάποιο σταθμό εργασίας ή στο δίκτυο (κατά τη μεταφορά αρχείων) μπορεί να κλαπούν ηλεκτρονικά αρχεία του συγκεκριμένου συστήματος.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση. Οικονομικό όφελος.	
		(4) Αποτέλεσμα (Outcome)	✓ **Αποκάλυψη** ❑ Τροποποίηση	❑ Καταστροφή ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς η πρόσβαση στους χώρους δεν ελέγχεται και οι χρήστες δεν κλειδώνουν τα γραφεία και τους σταθμούς εργασίας τους πριν την αποχώρηση τους από το χώρο. Δεν γίνεται χρήση ασφαλούς πρωτοκόλλου κατά τη μεταφορά αρχείων. Παρόλο που η είσοδος στο computer room επιτρέπεται μόνο με χρήση μαγνητικών καρτών, η πόρτα ανοίγει τραβώντας τη με δύναμη χωρίς να ενεργοποιείται κάποιος συναγερμός.	
		(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία	❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Η αποκάλυψη δεδομένων θα μπορούσε να οδηγήσει σε απώλεια καλής φήμης για την εταιρεία. Επίσης, στο σύστημα περιλαμβάνονται επιχειρησιακά ευαίσθητα δεδομένα και προσωπικά δεδομένα προμηθευτών, τα οποία δεν πρέπει να είναι διαθέσιμα στο ευρύ κοινό και κατά συνέπεια μπορεί να υπάρξουν νομικές κυρώσεις.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός	3
			Οικονομικά	Υψηλός	12
			Παραγωγικότητα	-	0
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	Μεσαίος	6
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**21**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Δημιουργία πολιτικής Φυσικής Ασφάλειας και Φυσικής Πρόσβασης. • Ανακοίνωση της πολιτικής και αποδοχή της. • Να γίνεται έλεγχος της απογραφής τουλάχιστον μία φορά κάθε 6 μήνες. • Αντικατάσταση του πρωτοκόλλου ftp με πιο ασφαλές πρωτόκολλο (π.χ. sftp).		
Όλο το προσωπικό	• Κάθε εργαζόμενος λύνοντας τη σχέση εργασίας του με την εταιρεία να υποχρεούται να υπογράψει μια δήλωση που να αναφέρει ότι έχει επιστρέψει όλα τα περιουσιακά στοιχεία που ανήκουν στην εταιρεία		
Computer Room	• Να ελεγχθεί η σωστή λειτουργία του συστήματος καρτών για την πρόσβαση στο computer room και να εγκατασταθεί μηχανισμός συναγερμού σε περίπτωση βίαιης εισόδου στο χώρο.		
Φύλακες	• Να γίνεται έλεγχος σε τσάντες / σάκους κ.τ.λ. κατά την είσοδο και έξοδο από το χώρο έτσι ώστε να αποφευχθεί η κλοπή υλικού. • Να επιτρέπεται η είσοδος ακολουθώντας την πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης.		

3.1.3 Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου

Καθορισμός Κριτηρίων Μέτρησης Κινδύνου

Allegro Worksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΦΗΜΗ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Φήμη ***(Προσωπικό)***	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια για την αποκατάσταση της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται μεγάλη προσπάθεια για να αποκατασταθεί.
Φήμη ***(Πελάτες, Προμηθευτές, Εξωτερικοί Συνεργάτες, Ευρύ κοινό)***	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια για την αποκατάσταση της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια ή δαπάνη, για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται αρκετά. Και απαιτείται μεγάλη προσπάθεια η δαπάνη για να αποκατασταθεί

Allegro Worksheet 2	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΙΚΟΝΟΜΙΚΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Λειτουργικά Έξοδα	Αύξηση μικρότερη του 1% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση μεταξύ 1% και 3% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση περισσότερο από 3% σε ετήσιες λειτουργικές δαπά-
Απώλεια Εσόδων	Ετήσια οικονομική απώλεια μικρότερη των 2.000€.	Ετήσια οικονομική απώλεια μεταξύ 2.000€ και 5.000€.	Ετήσια οικονομική απώλεια μεγαλύτερη των 5.000€.

Allegro Worksheet 3	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ώρες Εργασίας Προσωπικού	Οι ώρες εργασίας του προσωπικού δεν αυξάνονται περισσότερο από 3%.	Οι ώρες εργασίας του προσωπικού αυξάνονται μεταξύ 3% και 10%.	Οι ώρες εργασίας του προσωπικού αυξάνονται περισσότερο από 10%.
Ώρες Εργασίας Εξειδικευμένου Προσωπικού (Τεχνικοί, Προγραμματιστές, Προνομιούχοι Χρή-	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται ελάχιστα.	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται μεταξύ 1% και 5%.	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται περισσότερο από 5%.

Allegro Worksheet 4	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ασφάλειας και Υγείας	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 5	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Πρόστιμα - Αγωγές	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 6	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ – ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ορίζονται από τον χρήστη	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 7	ΠΡΟΤΕΡΑΙΟΠΟΙΗΣΗ ΤΩΝ ΠΕΡΙΟΧΩΝ ΕΠΙΠΤΩΣΕΩΝ
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**ΠΕΡΙΟΧΕΣ ΕΠΙΠΤΩΣΕΩΝ**
1	**ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
2	**ΟΙΚΟΝΟΜΙΚΑ**
3	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
-	**ΥΓΕΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ**
-	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ**
-	**ΟΡΙΖΕΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ**

1 χαμηλός βαθμός επίπτωσης
4 μέγιστος βαθμός επίπτωσης

Ανάπτυξη του Προφίλ των Περιουσιακών Στοιχείων

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΟΥ ΠΕΡΙΟΥΣΙΑΚΟΥ ΣΤΟΙΧΕΙΟΥ	
(1) Κρίσιμο Περιουσιακό Στοιχείο	**(2) Αιτιολογία Επιλογής**	**(3) Περιγραφή**
Σύστημα Διαχείρισης Εγγράφων & Πρωτοκόλλου	Η εφαρμογή του συστήματος διαχείρισης εγγράφων και πρωτοκόλλου δημιουργήθηκε κυρίως για την υποστήριξη των λειτουργικών απαιτήσεων της γραμματείας του Μηχανογραφικού Κέντρου της εταιρείας αλλά γίνεται χρήση αυτού και από τις υπόλοιπες γραμματείες	Μέσω του συστήματος γίνεται πρωτοκόλληση εισερχόμενων και εξερχόμενων εγγράφων έτσι ώστε να εξασφαλίζεται η ορθή απόδοση μοναδιαίου αριθμού πρωτοκόλλου στα έγγραφα. Επιπλέον, γίνεται έλεγχος για διπλές αριθμήσεις και διπλές καταχωρήσεις εγγράφων.
(4)Ιδιοκτήτης/ες		
Ευστάθιος Βασιλείου		
(5) Απαιτήσεις Ασφάλειας		
❑ **Εμπιστευτικότητα**	Μόνο το εξουσιοδοτημένο προσωπικό και σε εξαιρετικές περιπτώσεις άτομα από τα ανώτερα στελέχη μπορούν να δουν αυτές τις πληροφορίες.	
❑ **Ακεραιότητα**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει αυτές τις πληροφορίες.	
❑ **Διαθεσιμότητα**	Αυτό το περιουσιακό στοιχείο πρέπει να είναι διαθέσιμο για το προσωπικό για τον έλεγχο και πρωτοκόλληση των εγγράφων.	
❑ **Άλλο**	Αυτό το αγαθό δεν έχει ιδιαίτερες απαιτήσεις κανονιστικής συμμόρφωσης.	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας		
❑ Εμπιστευτικότητα	❑ Ακεραιότητα	✓ **Διαθεσιμότητα** ❑ Άλλο

Προσδιορισμός "Container" Περιουσιακών Στοιχείων

Allegro Worksheet 9a	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΤΕΧΝΙΚΑ)
ΕΣΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Το Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου αποτελείται από έναν εξυπηρετητή εφαρμογών (Application Servers) DELL poweredge 2950 Redhat Enterprise Linux 4.6 64 bit, όπου βρίσκεται και η βάση δεδομένων του συστήματος.	Τμήμα Πληροφορικής
Εσωτερικό δίκτυο εταιρείας: Όλες οι συναλλαγές που αφορούν το σύστημα γίνονται εντός του κλειστού εσωτερικού δικτύου (intranet)	Τμήμα Πληροφορικής Τμήμα Δικτύων
Σταθμοί εργασίας.	Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΦΥΣΙΚΑ)
ΕΣΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Ταινίες και δίσκοι αντιγράφων ασφαλείας στα οποία αποθηκεύονται στο τέλος κάθε ημέρας και στο τέλος κάθε εβδομάδας τα δεδομένα του συστήματος.	Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9c	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ/ΡΟΛΟΙ/ΑΡΜΟΔΙΟΤΗΤΕΣ	**ΤΜΗΜΑ / ΤΟΜΕΑΣ**
Προσωπικό πληροφορικής	Τμήμα Πληροφορικής
Οικονομικό προσωπικό / Γραμματεία	Οικονομικό Τμήμα / Γραμματεία
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΠΡΟΜΗΘΕΥΤΕΣ, ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΕΡΓΑΤΕΣ Κ.Τ.Λ.	**ΟΡΓΑΝΙΣΜΟΣ**

Προσδιορισμός των Συνθηκών που λαμβάνονται υπόψη / Σεναρίων Απειλής και Αναγνώριση Κινδύνων

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου**	
		Τομείς Ενδιαφέροντος	***Πλαστοπροσωπία ταυτότητας χρήστη***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος ή υπάλληλος που ενεργεί με σκοπό την αποκόμιση οικονομικού οφέλους	
		(2) Μέσα (Means)	Εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη ή εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου.	
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ **Τροποποίηση**	❑ Καταστροφή ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν υποκλέπτοντας την ταυτότητα κάποιου εξουσιοδοτημένου χρήστη.	
		(6) Πιθανότητα (Probability	✓ **Υψηλή**	❑ **Μεσαία** ❑ **Χαμηλή**
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Αύξηση της παραγωγικότητας από τη στιγμή που θα πρέπει όλα τα ηλεκτρονικά πρωτοκολλημένα έγγραφα να ελεγχθούν με βάση τα χειρόγραφα που έχουν κρατηθεί. Η οικονομική απώλεια προκύπτει από το κόστος σε εργατοώρες που θα απατηθούν για τον έλεγχο ορθότητας των εγγράφων. Σε περίπτωση αποκάλυψης στοιχείων θα υπάρξει απώλεια φήμης της εταιρείας.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός / 3
			Οικονομικά	Μεσαίος / 4
			Παραγωγικότητα	Υψηλός / 9
			Ασφάλεια και Υγεία	- / 0
			Πρόστιμα και Αγωγές	- / 0
			Ορίζονται από τον χρήστη	- / 0
			Συνολικός Βαθμός Κινδύνου	**16**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Σύστημα Διαχείρισης Εγγράφων & Πρωτοκόλλου	• Καταγραφή αρχείων που έχουν προσπελαστεί. • Χρήση πολυπλοκότητας κατά τη δημιουργία κωδικών. • Κρυπτογράφηση των κωδικών πρόσβασης. • Μηχανισμός κλειδώματος έπειτα από 3 αποτυχημένες προσπάθειες.		
Εσωτερικό Δίκτυο	• Μηχανισμός ασφάλειας που μπορεί να δείξει ποιος έχει αιτηθεί πρόσβαση σε κάποιο αρχείο. • Έλεγχος δραστηριοτήτων χρηστών. • Ανασκόπηση αποτυχημένων προσπαθειών πρόσβασης.		
Όλο το εμπλεκόμενο προσωπικό	• Ενημέρωση χρηστών σε θέματα ασφάλειας και ειδικότερα στη δημιουργία ισχυρών κωδικών.		

Allegro - Worksheet 10			ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου**		
		Τομείς Ενδιαφέροντος	***Εισαγωγή Κακόβουλου Κώδικα***		
		(1) Δράστης (Actor)	Οποιοσδήποτε που θα είχε ως στόχο να βλάψει την εταιρεία.		
		(2) Μέσα (Means)	Με την αποστολή κάποιου "email" ή δίνοντας κάποιο αποσπώμενο δίσκο σε υπάλληλο της εταιρείας.		
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.		
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εισαγωγή κακόβουλου κώδικα.		
		(6) Πιθανότητα (Probability)	❑ Υψηλή	❑ Μεσαία	✓ **Χαμηλή**
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Μπορεί να επιφέρει οικονομική απώλεια στην εταιρεία, που προκύπτει από το κόστος αποκατάστασης του συστήματος και από τις εργατοώρες που θα χρειαστούν για τον έλεγχο ορθότητας των δεδομένων. Επιπλέον αυξάνει αρκετά την παραγωγικότητα καθώς όλα τα έγγραφα θα πρωτοκολλούνται και θα μεταφέρονται χειρόγραφα.		Φήμη - Εμπιστοσύνη πελατών	Μεσαίος	2
			Οικονομικά	Μεσαίος	4
			Παραγωγικότητα	Υψηλός	9
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	-	0
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**15**

(9) Μείωση Κινδύνου			
✓ **Αποδοχή**	❑ Αναβολή	❑ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής	• Λήψη μέτρων έτσι ώστε να μην υπάρχει δυνατότητα χρήσης αποσπώμενων συσκευών, εκτός από εξαιρετικές περιπτώσεις και ύστερα από άδεια του Υπεύθυνου Ασφάλειας.		
Όλο το εμπλεκόμενο προσωπικό	• Ανακοίνωση και αποδοχή των πολιτικών. • Ευαισθητοποίηση σε θέματα που αφορούν το κακόβουλο λογισμικό.		

Allegro - Worksheet 10	ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Περιουσιακό Στοιχείο	***Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου***	
	Τομείς Ενδιαφέροντος	***Φωτιά***	
Απειλή	**(1) Δράστης** (Actor)	Δυσαρεστημένος υπάλληλος που έχει πρόσβαση σε χώρους κοντινούς του computer room. Ανυπαρξία ελέγχου / συντήρησης	
	(2) Μέσα (Means)	Πετώντας κάποιο εύφλεκτο υλικό.	
	(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.	
	(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	✓ **Καταστροφή** ❑ Διακοπή
	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εκδήλωση φωτιάς καθώς υπάρχει πιθανότητα καταστροφής του computer room. Η εταιρεία διαθέτει σύστημα πυρανίχνευσης αλλά δεν γίνεται ο προκαθορισμένος έλεγχος αυτού και επιπλέον δεν διαθέτει αυτόματο σύστημα πυρόσβεσης.	
	(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία** ❑ Χαμηλή

(7) Συνέπειες (Consequences)	**(8) Βαρύτητα** (Severity)		
	Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
Σε περίπτωση καταστροφής του συστήματος, θα πρέπει να δημιουργηθεί εκ νέου σε κάποια άλλη τοποθεσία. Εάν η καταστροφή του συστήματος γίνει γνωστή στο κοινό, αμαυρώνεται η φήμη της εταιρείας.	Φήμη - Εμπιστοσύνη πελατών	Υψηλός	3
	Οικονομικά	Χαμηλός	2
	Παραγωγικότητα	Υψηλός	9
	Ασφάλεια και Υγεία	-	0
	Πρόστιμα και Αγωγές	-	0
	Ορίζονται από τον χρήστη	-	0
		Συνολικός Βαθμός Κινδύνου	**14**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Computer Room, λοιποί χώροι	• Να γίνει εγκατάσταση αυτόματου συστήματος πυρόσβεσης • Να γίνεται ο προκαθορισμένος έλεγχος του συστήματος πυρανίχνευσης.		
Όλο το προσωπικό	• Απαγόρευση καπνίσματος σε κλειστούς χώρους • Εκπαίδευση προσωπικού σε περιπτώσεις πυρκαγιάς.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Οικονομικής και Λογιστικής Διαχείρισης**	
		Τομείς Ενδιαφέροντος	***Διακοπή Ηλεκτροδότησης***	
		(1) Δράστης (Actor)	-	
		(2) Μέσα (Means)	-	
		(3) Κίνητρο (Motive)	-	
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓ **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς χωρίς ρεύμα, υπάρχει διακοπή της λειτουργίας του συστήματος. Το σύστημα διαθέτει μονάδες αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS) και γεννήτρια πετρελαίου.	
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία** ❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)	
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)** / **Βαθμός Αποτίμησης (Score)**
	Μπορεί να μειώσει την παραγωγικότητα για όσο διάστημα δεν ηλεκτροδοτείται το σύστημα. Σε περίπτωση μη λειτουργίας των UPS ή της γεννήτριας μπορεί να υπάρξει βλάβη σε κάποιο συστατικό του συστήματος επιφέροντας οικονομικό κόστος που προκύπτει από την αντικατάσταση του.		Φήμη - Εμπιστοσύνη πελατών	- / 0
			Οικονομικά	Χαμηλός / 2
			Παραγωγικότητα	Μεσαίος / 9
			Ασφάλεια και Υγεία	- / 0
			Πρόστιμα και Αγωγές	- / 0
			Ορίζονται από τον χρήστη	- / 0
				Συνολικός Βαθμός Κινδύνου / **11**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	✓ **Αναβολή**	❑ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Υπεύθυνος Συντήρησης Εξοπλισμού	• Τακτικός έλεγχος της σωστής λειτουργίας των UPS και της γεννήτριας.		

Allegro - Worksheet 10		ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου**	
		Τομείς Ενδιαφέροντος	***Κλοπή Υλικού / Εξοπλισμού / Δεδομένων***	
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος, επισκέπτης.	
		(2) Μέσα (Means)	Θα μπορούσε οποιοσδήποτε υπάλληλος ή επισκέπτης έχοντας πρόσβαση στις εγκαταστάσεις να κλέψει αποσπώμενες συσκευές η κασέτες αποθήκευσης εφεδρικών αντιγράφων που περιέχουν δεδομένα του συγκεκριμένου συστήματος. Επίσης, αποκτώντας πρόσβαση σε κάποιο σταθμό εργασίας ή στο δίκτυο (κατά τη μεταφορά αρχείων) μπορεί να κλαπούν ηλεκτρονικά αρχεία του συγκεκριμένου συστήματος.	
		(3) Κίνητρο (Motive)	• Ηθική ικανοποίηση. • Οικονομικό όφελος	
		(4) Αποτέλεσμα (Outcome)	✓ **Αποκάλυψη** ❑ Τροποποίηση	❑ Καταστροφή ❑ Διακοπή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς η πρόσβαση στους χώρους δεν ελέγχεται και οι χρήστες δεν κλειδώνουν τα γραφεία και τους σταθμούς εργασίας τους πριν την αποχώρηση τους από το χώρο. Δεν γίνεται χρήση ασφαλούς πρωτοκόλλου κατά τη μεταφορά αρχείων. Παρόλο που η είσοδος στο computer room επιτρέπεται μόνο με χρήση μαγνητικών καρτών, η πόρτα ανοίγει τραβώντας τη με δύναμη χωρίς να ενεργοποιείται κάποιος συναγερμός.	
		(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία	❑ Χαμηλή

(7) Συνέπειες (Consequences)	**(8) Βαρύτητα** (Severity)		
	Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
Η αποκάλυψη δεδομένων θα μπορούσε να οδηγήσει σε απώλεια καλής φήμης για την εταιρεία και αύξηση της παραγωγικότητας καθώς παραγωγικότητα καθώς όλα τα έγγραφα θα πρωτοκολλούνται και θα μεταφέρονται χειρόγραφα.	Φήμη - Εμπιστοσύνη πελατών	Υψηλός	3
	Οικονομικά	Υψηλός	6
	Παραγωγικότητα	Υψηλός	9
	Ασφάλεια και υγεία	-	0
	Πρόστιμα και Αγωγές	-	0
	Ορίζονται από τον χρήστη	-	0
		Συνολικός Βαθμός Κινδύνου	**18**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Δημιουργία πολιτικής Φυσικής Ασφάλειας και Φυσικής Πρόσβασης • Ανακοίνωση της πολιτικής και αποδοχή της. • Να γίνεται έλεγχος της απογραφής τουλάχιστον μία φορά κάθε 6 μήνες. • Αντικατάσταση ftp με πιο ασφαλές πρωτόκολλο (π.χ. sftp)		
Όλο το προσωπικό	• Κάθε εργαζόμενος λύνοντας τη σχέση εργασίας του με την εταιρεία να υποχρεούται να υπογράψει μια δήλωση που να αναφέρει ότι έχει επιστρέψει όλα τα περιουσιακά στοιχεία που ανήκουν στην εταιρεία		
Computer Room	• Να ελεγχθεί η σωστή λειτουργία του συστήματος καρτών για την πρόσβαση στο computer room και να εγκατασταθεί μηχανισμός συναγερμού σε περίπτωση βίαιης εισόδου στο χώρο.		
Φύλακες	• Να γίνεται έλεγχος σε τσάντες / σάκους κ.τ.λ. κατά την είσοδο και έξοδο από το χώρο έτσι ώστε να αποφευχθεί η κλοπή υλικού. • Να επιτρέπεται η είσοδος ακολουθώντας την πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης.		

3.1.4 Σύστημα Διαχείρισης Προσωπικού

Καθορισμός Κριτηρίων Μέτρησης Κινδύνου

Allegro Worksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΦΗΜΗ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Φήμη (Προσωπικό)	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια για την αποκατάσταση της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται κατά πολύ και απαιτείται μεγάλη προσπάθεια η δαπάνη για να αποκατασταθεί .
Φήμη (Πελάτες, Προμηθευτές, Εξωτερικοί Συνεργάτες, Ευρύ κοινό)	Η φήμη της εταιρείας επηρεάζεται ελάχιστα. Απαιτείται μικρή η καθόλου προσπάθεια για την αποκατάσταση της.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται μικρή προσπάθεια για να αποκατασταθεί.	Η φήμη της εταιρείας επηρεάζεται αρκετά και απαιτείται προσπάθεια μεγάλη ή δαπάνη για να αποκατασταθεί.

Allegro Worksheet 2	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΙΚΟΝΟΜΙΚΑ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Λειτουργικά Έξοδα	Αύξηση μικρότερη του 1% σε ετήσιες λειτουργικές δαπάνες	Αύξηση μεταξύ 1% και 3% σε ετήσιες λειτουργικές δαπάνες	Αύξηση περισσότερο από 3% σε ετήσιες λειτουργικές δαπάνες
Απώλεια Εσόδων	Ετήσια οικονομική απώλεια μικρότερη των 3.000 €	Ετήσια οικονομική απώλεια μεταξύ 3.000€ και 7.000€	Ετήσια οικονομική απώλεια μεγαλύτερη από 7.000€

Allegro Worksheet 3	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΑΡΑΓΩΓΙΚΟΤΗΤΑΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ώρες Εργασίας Προσωπικού	Οι ώρες εργασίας του προσωπικού δεν αυξάνονται περισσότερο από 10%	Οι ώρες εργασίας του προσωπικού αυξάνονται μεταξύ 10% και 20%	Οι ώρες εργασίας του προσωπικού αυξάνονται περισσότερο από 20%
Ώρες Εργασίας Εξειδικευμένου Προσωπικού (Τεχνικοί, Προγραμματιστές, Προνομιούχοι Χρήστες)	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται ελάχιστα ή καθόλου	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται μεταξύ 1% και 5%	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται περισσότερο από 5%
Ώρες Εργασίας Ανώτερων Στελεχών:	Οι ώρες εργασίας των ανωτέρων στελεχών δεν αυξάνονται.	Οι ώρες εργασίας των ανωτέρων στελεχών ενδέχεται να αυξηθούν έως 2%	Οι ώρες εργασίας των ανωτέρων στελεχών αυξάνονται περισσότερο από 2%

Allegro Worksheet 4	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΓΕΙΑΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ασφάλειας και υγείας	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 5	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Πρόστιμα - Αγωγές	Επιβολή προστίμων – αγωγών μικρότερη από 10.000€.	Επιβολή προστίμων – αγωγών μεταξύ 10.000€ και 20.000€ .	Επιβολή προστίμων – αγωγών μεγαλύτερων από μεγαλύτερων από 20.000€.

Allegro Worksheet 6	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ορίζονται από τον χρήστη	Δεν υπάρχουν επιπτώσεις		

Allegro Worksheet 7	ΠΡΟΤΕΡΑΙΟΠΟΙΗΣΗ ΤΩΝ ΠΕΡΙΟΧΩΝ ΕΠΙΠΤΩΣΕΩΝ
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**ΠΕΡΙΟΧΕΣ ΕΠΙΠΤΩΣΕΩΝ**
2	**ΦΗΜΗ / ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
1	**ΟΙΚΟΝΟΜΙΚΑ**
4	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
-	**ΥΓΕΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ**
3	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ**
-	**ΟΡΙΖΕΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ**

1 χαμηλός βαθμός επίπτωσης
4 μέγιστος βαθμός επίπτωσης

Ανάπτυξη του Προφίλ των Περιουσιακών Στοιχείων

Allegro Worksheet 8	ΠΡΟΦΊΛ ΚΡΊΣΙΜΟΥ ΠΕΡΙΟΥΣΙΑΚΟΎ ΣΤΟΙΧΕΊΟΥ	
(1) Κρίσιμο Περιουσιακό Στοιχείο	**(2) Αιτιολογία Επιλογής**	**(3) Περιγραφή**
Σύστημα Διαχείρισης Προσωπικού.	Το σύστημα Διαχείρισης Προσωπικού δημιουργήθηκε για να καλύψει τις ανάγκες της Διεύθυνσης Οικονομικών Υπηρεσιών	Το περιουσιακό στοιχείο περιλαμβάνει τα ακόλουθα: • Μηχανογραφική τήρηση των προσωπικών μητρώων και έκδοση πιστοποιητικών υπηρεσιακών μεταβολών των υπαλλήλων. • Μηχανογραφική τήρηση αρχείων διορισμού, πρόσληψης, μονιμοποίησης, μετακίνησης κ.τ.λ. • Μηχανογραφική τήρηση σύμβασης προσωπικού, κρατήσεις, ταμεία, φορολογικά στοιχεία, προϋπηρεσία, άδειες, συντάξεις • Διαχείριση κατάταξης των υπαλλήλων σε μισθολογική κλίμα και διαχείριση μισθοδοσίας προσωπικού. Εκκαθάριση αποδοχών (τακτικές, επιδόματα, ασθενείας, υπερωρίες, αποζημίωσης, αναδρομικών).
(4) Ιδιοκτήτης/ες		
Παναγιώτης Γεωργίου		
(5) Απαιτήσεις Ασφάλειας		
❑ **Εμπιστευτικότητα**	Μόνο εξουσιοδοτημένο προσωπικό της Οικονομικής Διεύθυνσης μπορεί να δείτε αυτές τις πληροφορίες.	
❑ **Ακεραιότητα**	Μόνο εξουσιοδοτημένο προσωπικό της Οικονομικής Διεύθυνσης μπορεί να τροποποιήσει αυτές τις πληροφορίες.	
❑ **Διαθεσιμότητα**	Το σύστημα θα πρέπει να είναι διαθέσιμο στο προσωπικό για τη μισθοδοσία των υπαλλήλων και για τη διεκπεραίωση των απαιτούμενων εργασιών.	
❑ **Άλλο**	Αυτό το αγαθό δεν έχει ιδιαίτερες απαιτήσεις κανονιστικής συμμόρφωσης-	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας		
✓ **Εμπιστευτικότητα**	❑ Ακεραιότητα	❑ Διαθεσιμότητα ❑ Άλλο

Προσδιορισμός “Container” Περιουσιακών Στοιχείων

Allegro Worksheet 9a	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΤΕΧΝΙΚΑ)	
ΕΣΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ “CONTAINER”		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Το σύστημα Καταγραφής & Διαχείρισης των Δελτίων αποτελείται από έναν εξυπηρετητή εφαρμογών (Application Servers) DELL poweredge 2950 Redhat Enterprise Linux 4.6 64 bit, όπου βρίσκεται και η βάση δεδομένων του συστήματος.		Οικονομικό Τμήμα
Εσωτερικό δίκτυο εταιρείας: Το σύστημα βρίσκεται εντός του κλειστού εσωτερικού δικτύου (intranet) της εταιρείας.		Τμήμα Πληροφορικής
		Τμήμα Δικτύων
Σταθμοί εργασίας		Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ “CONTAINER”		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΦΥΣΙΚΑ)	
ΕΣΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ “CONTAINER”		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Ταινίες και δίσκοι αντιγράφων ασφαλείας στα οποία αποθηκεύονται στο τέλος κάθε ημέρας και στο τέλος κάθε εβδομάδας τα δεδομένα του συστήματος.		Τμήμα Πληροφορικής
ΕΞΩΤΕΡΙΚΑ		
ΠΕΡΙΓΡΑΦΗ “CONTAINER”		**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

Allegro Worksheet 9c	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΟΝΟΜΑ/ΡΟΛΟΙ/ΑΡΜΟΔΙΟΤΗΤΕΣ		**ΤΜΗΜΑ / ΤΟΜΕΑΣ**
Προσωπικό πληροφορικής και δικτύων		Τμήμα Πληροφορικής
		Τμήμα Δικτύων
Οικονομικό προσωπικό		Οικονομικό Τμήμα
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΠΡΟΜΗΘΕΥΤΕΣ, ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΕΡΓΑΤΕΣ Κ.Τ.Λ.		**ΟΡΓΑΝΙΣΜΟΣ**

Προσδιορισμός των Συνθηκών που λαμβάνονται υπόψη / Σεναρίων Απειλής & Αναγνώριση Κινδύνων

Allegro - Worksheet 10	ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων — Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Προσωπικού**	
	Τομείς Ενδιαφέροντος	***Πλαστοπροσωπία ταυτότητας χρήστη***	
	(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος ή υπάλληλος που ενεργεί με σκοπό την αποκόμιση οικονομικού οφέλους	
	(2) Μέσα (Means)	Εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη ή εκμεταλλεύόμενος αδυναμία στην ασφάλεια του δικτύου.	
	(3) Κίνητρο (Motive)	Αποκόμιση οικονομικού οφέλους, ηθική ικανοποίηση.	
	(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ Τροποποίηση	❑ Καταστροφή ❑ Διακοπή
	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν υποκλέπτοντας την ταυτότητα κάποιου εξουσιοδοτημένου χρήστη. Ο λογαριασμός του χρήστη δεν κλειδώνει έπειτα από έναν αριθμό αποτυχημένων προσπαθειών και οι κωδικοί δεν αποθηκεύονται σε κρυπτογραφημένη μορφή	
	(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία ❑ Χαμηλή
	(7) Συνέπειες (Consequences)	**(8) Βαρύτητα** (Severity)	
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Εκτιμάται ότι θα υπάρξει οικονομική απώλεια για την εταιρεία λαμβάνοντας υπόψη περιπτώσεις λαθών σε μισθούς, συντάξεις κ.τ.λ. Αύξηση της παραγωγικότητας από τη στιγμή που θα πρέπει να γίνει έλεγχος των χειρόγραφων δεδομένων για την ορθότητα των στοιχείων.	Φήμη - Εμπιστοσύνη πελατών	Υψηλός	6
		Οικονομικά	Υψηλός	3
		Παραγωγικότητα	Μεσαία-	8
		Ασφάλεια και υγεία	-	0
		Πρόστιμα και Αγωγές	-	0
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**17**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Σύστημα Καταγραφής & Διαχείρισης Δελτίων	• Καταγραφή αρχείων που έχουν προσπελαστεί • Χρήση πολυπλοκότητας κατά τη δημιουργία κωδικών • Κρυπτογράφηση των κωδικών πρόσβασης • Μηχανισμός κλειδώματος έπειτα από 3 αποτυχημένες προσπάθειες		
Εσωτερικό Δίκτυο	• Μηχανισμός ασφάλειας που μπορεί να δείξει ποιος έχει αιτηθεί πρόσβαση σε κάποιο αρχείο • Έλεγχος δραστηριοτήτων χρηστών • Ανασκόπηση αποτυχημένων προσπαθειών πρόσβασης		
Όλο το εμπλεκόμενο προσωπικό	• Ενημέρωση του προσωπικού ότι η κίνησή τους καταγράφεται • Ενημέρωση χρηστών σε θέματα ασφάλειας		

<table>
<tr><td colspan="3">Allegro - Worksheet 10</td><td colspan="4">ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ</td></tr>
<tr><td rowspan="10">Κίνδυνοι Περιουσιακών Στοιχείων</td><td rowspan="7">Απειλή</td><td>Περιουσιακό Στοιχείο</td><td colspan="4">Σύστημα Διαχείρισης Προσωπικού</td></tr>
<tr><td>Τομείς Ενδιαφέροντος</td><td colspan="4">Εισαγωγή Κακόβουλου Κώδικα</td></tr>
<tr><td>(1) Δράστης (Actor)</td><td colspan="4">“Hacker”</td></tr>
<tr><td>(2) Μέσα (Means)</td><td colspan="4">Με την αποστολή κάποιου email ή δίνοντας κάποιο αποσπώμενο δίσκο σε υπάλληλο της εταιρείας.</td></tr>
<tr><td>(3) Κίνητρο (Motive)</td><td colspan="4">Ηθική ικανοποίηση.</td></tr>
<tr><td>(4) Αποτέλεσμα (Outcome)</td><td colspan="2">❑ Αποκάλυψη
❑ Τροποποίηση</td><td colspan="2">❑ Καταστροφή
✓ Διακοπή</td></tr>
<tr><td>(5) Απαιτήσεις Ασφάλειας (Security Requirements)</td><td colspan="4">Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εισαγωγή κακόβουλου κώδικα.</td></tr>
<tr><td>(6) Πιθανότητα (Probability)</td><td>❑ Υψηλή</td><td>✓ Μεσαία</td><td colspan="2">❑ Χαμηλή</td></tr>
<tr><td colspan="2" rowspan="2">(7) Συνέπειες (Consequences)</td><td colspan="4">(8) Βαρύτητα (Severity)</td></tr>
<tr><td>Περιοχή Επίπτωσης</td><td>Βαθμός Κινδύνου (Value)</td><td colspan="2">Βαθμός Αποτίμησης (Score)</td></tr>
<tr><td colspan="2" rowspan="7">Θα έχει ως αποτέλεσμα οικονομική απώλεια που προκύπτει από το κόστος επιπλέον εργατοωρών που θα απαιτηθούν για τη συνέχιση της λειτουργίας με χειρόγραφο τρόπο και από το κόστος αποκατάστασης του συστήματος.</td><td>Φήμη - Εμπιστοσύνη πελατών</td><td>Υψηλός</td><td colspan="2">3</td></tr>
<tr><td>Οικονομικά</td><td>Υψηλός</td><td colspan="2">3</td></tr>
<tr><td>Παραγωγικότητα</td><td>Υψηλός</td><td colspan="2">12</td></tr>
<tr><td>Ασφάλεια και Υγεία</td><td>-</td><td colspan="2">0</td></tr>
<tr><td>Πρόστιμα και Αγωγές</td><td>-</td><td colspan="2">0</td></tr>
<tr><td>Ορίζονται από τον χρήστη</td><td>-</td><td colspan="2">0</td></tr>
<tr><td colspan="5">Συνολικός Βαθμός Κινδύνου</td><td>18</td></tr>
</table>

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό Πληροφορικής και Δικτύων	• Λήψη μέτρων έτσι ώστε να μην υπάρχει δυνατότητα χρήσης αποσπώμενων συσκευών, εκτός από εξαιρετικές περιπτώσεις, και ύστερα από άδεια του Υπεύθυνου Ασφάλειας. • Δημιουργία πολιτικής Αναφοράς και διαχείρισης περιστατικών Ασφάλειας		
Όλο το εμπλεκόμενο προσωπικό	• Ανακοίνωση και αποδοχή των πολιτικών • Ευαισθητοποίηση σε θέματα που αφορούν το κακόβουλο λογισμικό.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή		

Allegro - Worksheet 10			ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Προσωπικού**		
		Τομείς Ενδιαφέροντος	***Φωτιά***		
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος που έχει πρόσβαση σε χώρους κοντινούς του computer room. Ανυπαρξία ελέγχου / συντήρησης		
		(2) Μέσα (Means)	Πετώντας κάποιο εύφλεκτο υλικό.		
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση.		
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	✓ **Καταστροφή** ❑ Διακοπή	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν με την εκδήλωση φωτιάς καθώς υπάρχει πιθανότητα καταστροφής του computer room. Η εταιρεία διαθέτει σύστημα πυρανίχνευσης αλλά δεν γίνεται ο προκαθορισμένος έλεγχος αυτού και επιπλέον δεν διαθέτει αυτόματο σύστημα πυρόσβεσης.		
		(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ **Μεσαία**	❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Μπορεί να επιφέρει οικονομική απώλεια στην εταιρεία, που προκύπτει από το κόστος αποκατάστασης του συστήματος και από τις εργατοώρες που θα χρειαστούν για την επανεισαγωγή των δεδομένων. Εάν η καταστροφή γίνει γνωστή στο κοινό, επηρεάζεται η φήμη της εταιρείας και επιπλέον θα υπάρξουν νομικές κυρώσεις.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός	6
			Οικονομικά	Υψηλός	3
			Παραγωγικότητα	Μεσαίος	8
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	Υψηλός	9
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**26**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Computer Room, ***Λοιποί χώροι***	• Να γίνει εγκατάσταση αυτόματου συστήματος πυρόσβεσης • Να γίνεται ο προκαθορισμένος έλεγχος του συστήματος πυρανίχνευσης		
Όλο το προσωπικό	• Απαγόρευση καπνίσματος σε κλειστούς χώρους • Εκπαίδευση προσωπικού σε περιπτώσεις πυρκαγιάς.		
Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων	• Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή		

Allegro - Worksheet 10			ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Προσωπικού**		
		Τομείς Ενδιαφέροντος	***Διακοπή Ηλεκτροδότησης***		
		(1) Δράστης (Actor)	-		
		(2) Μέσα (Means)	-		
		(3) Κίνητρο (Motive)	-.		
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ❑ Τροποποίηση	❑ Καταστροφή ✓**Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς χωρίς ρεύμα, υπάρχει διακοπή της λειτουργίας του συστήματος. Το σύστημα διαθέτει μονάδες αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS) και γεννήτρια πετρελαίου.		
		(6) Πιθανότητα (Probability)	❑ Υψηλή	❑ Μεσαία	✓ **Χαμηλή**
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Μπορεί να μειώσει την παραγωγικότητα για όσο διάστημα δεν ηλεκτροδοτείται το σύστημα.		Φήμη - Εμπιστοσύνη πελατών	-	0
			Οικονομικά	Χαμηλός	2
			Παραγωγικότητα	Υψηλός	12
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	-	0
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**14**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	✓ **Αναβολή**	❑ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Υπεύθυνος Συντήρησης Εξοπλισμού	• Τακτικός έλεγχος της σωστής λειτουργίας των UPS και της γεννήτριας.		

Allegro - Worksheet 10			ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ		
Κίνδυνοι Περιουσιακών Στοιχείων	Απειλή	Περιουσιακό Στοιχείο	**Σύστημα Διαχείρισης Προσωπικού**		
		Τομείς Ενδιαφέροντος	***Κλοπή Υλικού / Εξοπλισμού / Δεδομένων***		
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος, επισκέπτης.		
		(2) Μέσα (Means)	Θα μπορούσε οποιοσδήποτε υπάλληλος ή επισκέπτης έχοντας πρόσβαση στις εγκαταστάσεις να κλέψει αποσπώμενες συσκευές η κασέτες αποθήκευσης εφεδρικών αντιγράφων που περιέχουν δεδομένα του συγκεκριμένου συστήματος. Επίσης έχοντας πρόσβαση σε κάποιο σταθμό εργασίας μπορεί να κλέψει ηλεκτρονικά αρχεία του συγκεκριμένου συστήματος.		
		(3) Κίνητρο (Motive)	Ηθική ικανοποίηση. Οικονομικό όφελος		
		(4) Αποτέλεσμα (Outcome)	✓ **Αποκάλυψη** ❑ **Τροποποίηση**	❑ **Καταστροφή** ❑ **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν καθώς η πρόσβαση στους χώρους δεν ελέγχεται και οι χρήστες δεν κλειδώνουν τα γραφεία και τους σταθμούς εργασίας τους πριν την αποχώρηση τους από το χώρο. Δεν γίνεται χρήση ασφαλούς πρωτοκόλλου κατά τη μεταφορά αρχείων. Παρόλο που η είσοδος στο computer room επιτρέπεται μόνο με χρήση μαγνητικών καρτών, η πόρτα ανοίγει τραβώντας τη με δύναμη χωρίς να ενεργοποιείται κάποιος συναγερμός.		
		(6) Πιθανότητα (Probability)	✓ **Υψηλή**	❑ Μεσαία	❑ Χαμηλή
	(7) Συνέπειες (Consequences)		**(8) Βαρύτητα** (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου (Value)**	**Βαθμός Αποτίμησης (Score)**
	Η κλοπή θα έχει ελάχιστο κόστος για την εταιρεία αλλά θα μπορούσε να οδηγήσει σε αποκάλυψη δεδομένων και κατά συνέπεια σε απώλεια καλής φήμης για την εταιρεία και επιβολή προστίμων.		Φήμη - Εμπιστοσύνη πελατών	Υψηλός-	6
			Οικονομικά	Μεσαίος	2
			Παραγωγικότητα	-	0
			Ασφάλεια και Υγεία	-	0
			Πρόστιμα και Αγωγές	Υψηλός	9
			Ορίζονται από τον χρήστη	-	0
				Συνολικός Βαθμός Κινδύνου	**17**

(9) Μείωση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να μειωθούν πρέπει να γίνουν τα ακόλουθα:			
Προσωπικό πληροφορικής και δικτύων	• Δημιουργία πολιτικής Φυσικής Ασφάλειας και Φυσικής Πρόσβασης • Ανακοίνωση της πολιτικής και αποδοχή της. • Να γίνεται έλεγχος της απογραφής τουλάχιστον μία φορά κάθε 6 μήνες. • Αντικατάσταση ftp με πιο ασφαλές πρωτόκολλο (π.χ. sftp)		
Όλο το προσωπικό	• Κάθε εργαζόμενος λύνοντας τη σχέση εργασίας του με την εταιρεία να υποχρεούται να υπογράψει μια δήλωση που να αναφέρει ότι έχει επιστρέψει όλα τα περιουσιακά στοιχεία που ανήκουν στην εταιρεία		
Computer Room	• Να ελεγχθεί η σωστή λειτουργία του συστήματος καρτών για την πρόσβαση στο computer room και να εγκατασταθεί μηχανισμός συναγερμού σε περίπτωση βίαιης εισόδου στο χώρο.		
Φύλακες	• Να γίνεται έλεγχος σε τσάντες / σάκους κ.τ.λ. κατά την είσοδο και έξοδο από το χώρο έτσι ώστε να αποφευχθεί η κλοπή υλικού. • Να επιτρέπεται η είσοδος ακολουθώντας την πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης.		

Κεφάλαιο 4

Σχέδιο Ασφάλειας

4.1 Πολιτική Ασφάλειας

Εισαγωγή

Η Πολιτική Ασφαλείας (Security Policy) είναι ένα έγγραφο που περιλαμβάνει τους στόχους που έχει θέσει η εταιρεία αναφορικά με την ασφάλεια πληροφοριακών συστημάτων, τους ρόλους, τις υπευθυνότητες και τις αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται. Η πολιτική ασφάλειας αποτελεί δέσμευση της Διοίκησης για την παροχή όλων των απαραίτητων πόρων για την εφαρμογή της. Επιπλέον, πρέπει να επανεξετάζεται σε περιπτώσεις σημαντικών αλλαγών της πληροφοριακής υποδομής ή σε περιπτώσεις εμφάνισης νέων κινδύνων - απειλών. Στην περίπτωση της εταιρείας που μελετήθηκε έχει ήδη συνταχθεί μία Γενική Πολιτική Ασφάλειας, η οποία παραπέμπει σε επιμέρους πολιτικές και διαδικασίες αλλά με βάση τα παραπάνω αποτελέσματα ανάλυσης επικινδυνότητας καθίσταται αναγκαίος ο εμπλουτισμός της.

Πεδίο Εφαρμογής μιας Πολιτικής

Οι πολιτικές Ασφάλειας πρέπει να εφαρμόζονται από όλα τα μέλη του προσωπικού της εταιρείας που εμπλέκονται άμεσα ή έμμεσα στην εκτέλεση των υπηρεσιών και λειτουργιών, καθώς επίσης και στη χρήση της υποδομής και του εξοπλισμού που χρησιμοποιεί η εταιρεία στα πλαίσια εκτέλεσης των λειτουργικών της απαιτήσεων.

Σκοπός

Η εταιρεία επιδιώκει την παροχή των υπηρεσιών σύμφωνα με το ισχύον νομικό και κανονιστικό πλαίσιο και τις λοιπές συμβατικές υποχρεώσεις της, με τρόπο που να προστατεύεται η πληροφορία από εκούσια ή ακούσια κλοπή, καταστροφή, ή χρήση κατά παράβαση των νόμων και των κανονιστικών διατάξεων.

Ο σκοπός της ασφάλειας της πληροφορίας είναι να διασφαλίσει την επιχειρησιακή συνέχεια της εταιρείας και να ελαχιστοποιήσει τους κινδύνους που απειλούν την πληροφορία, αποφεύγοντας περιστατικά ασφαλείας και μειώνοντας τις επιπτώσεις που μπορεί να έχουν τα περιστατικά αυτά.

Πολιτική

Στόχος της πολιτικής είναι να προστατέψει τα πληροφοριακά αγαθά της εταιρείας και των πελατών της από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές.

Οι επιμέρους στόχοι της εταιρείας σχετικά με την ασφάλεια της πληροφορίας είναι:

- Η προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση
- Η διασφάλιση της εμπιστευτικότητας της πληροφορίας
- Η διατήρηση της ακεραιότητας της πληροφορίας
- Η διατήρηση της διαθεσιμότητας της πληροφορίας
- Η τήρηση των Νομικών και Κανονιστικών απαιτήσεων
- Η ανάπτυξη, διατήρηση και ο έλεγχος των Σχεδίων Επιχειρησιακής Συνέχειας
- Η παροχή εκπαίδευσης στο προσωπικό σε θέματα ασφάλειας
- Η αναφορά και διερεύνηση όλων των περιστατικών ασφάλειας

Για την επίτευξη των παραπάνω στόχων έχουν αναπτυχθεί και εφαρμόζονται επιμέρους πολιτικές ασφαλείας και διαδικασίες, όπου περιγράφονται όλες οι σχετικές αρμοδιότητες του προσωπικού. Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται) είναι υποχρεωμένοι να εφαρμόζουν τις πολιτικές ασφαλείας που εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Πολιτικές Ασφάλειας της εταιρείας

Οι πολιτικές ασφάλειας που έχει αναπτύξει η εταιρεία είναι οι ακόλουθες:

- Πολιτική Αρμοδιοτήτων για την Ασφάλεια Πληροφοριών
- Πολιτική Κατηγοριοποίησης και Διαχείρισης Πληροφοριακών περιουσιακών Στοιχείων
- Πολιτική Διαχείρισης Προσωπικού και Δικαιωμάτων Πρόσβασης
- Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης
- Πολιτική Ελέγχων Τεχνικής Συμμόρφωσης
- Πολιτική Χρήσης Αποσπώμενων Συσκευών
- Πολιτική Απόρριψης Υλικού
- Πολιτική Ασφάλειας Καλωδιώσεων
- Πολιτική Αντιγράφων Ασφάλειας
- Πολιτικής Διαχείρισης Ηλεκτρονικής Αλληλογραφίας

Αλλαγές – Προσθήκες στις Πολιτικές Ασφάλειας

Οι αλλαγές στην ήδη υπάρχουσα κατάσταση πρέπει να γίνουν με βάση των όσων περιγράφονται στη συνέχεια.

Αρχικά η εταιρεία θα πρέπει να διασφαλίσει ότι η Γενική Πολιτική ασφάλειας καθώς και οι επιμέρους πολιτικές και διαδικασίες που υπάρχουν και αυτές που πρόκειται να υλοποιηθούν, θα εφαρμόζονται από όλα τα εμπλεκόμενα μέλη του προσωπικού.

Επιπλέον Πολιτικές

Για τη διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων πρέπει τεκμηριωθούν οι ακόλουθες πολιτικές:

- Πολιτική Επικοινωνίας με Αρχές και Ενδιαφερόμενες Ομάδες
- Πολιτική Διαχείρισης Ασφάλειας για Συμφωνίες με Τρίτους
- Πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης
- Πολιτική Αντιμετώπισης Περιστατικών Έκτακτης Ανάγκης
- Πολιτική Εγκατάστασης Υλικού και Λογισμικού
- Πολιτική Ανάπτυξης και Αναβάθμισης Λογισμικού
- Πολιτική Διαχείρισης Κύκλου Ζωής Συμβάντων και Επιθεωρήσεων
- Πολιτική Διαχείρισης Απομακρυσμένης Πρόσβασης (mobile computing και τηλεργασία)
- Πολιτική Συντήρησης Εξοπλισμού
- Πολιτική Αναφοράς και Διαχείρισης Περιστατικών Ασφάλειας

Εκπαίδευση του Προσωπικού

Η εταιρεία πρέπει να μεριμνήσει για τη επαρκή εκπαίδευση του προσωπικού σε θέματα Ασφάλειας Πληροφοριακών Συστημάτων και προστασίας προσωπικών δεδομένων και να τους παρέχει τις απαραίτητες οδηγίες για τη σωστή επιτέλεση των εργασιών τους. Επίσης θα πρέπει να γίνουν εκπαιδεύσεις του προσωπικού σε περιπτώσεις εκτάκτων αναγκών όπως φωτιά, πλημμύρα κ.τ.λ.

Για τα άτομα του προσωπικού που είναι αρμόδια για τη διαχείριση της ασφάλειας θα πρέπει να παρέχεται επιπλέον εξειδικευμένη εκπαίδευση σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

Έλεγχος πρόσβασης

Η εκχώρηση δικαιωμάτων πρόσβασης σε πόρους και δεδομένα γίνεται σύμφωνα με την Πολιτική Διαχείρισης Προσωπικού και Δικαιωμάτων Πρόσβασης και σύμφωνα με συγκεκριμένες διαδικασίες. Θα πρέπει όμως να υπάρξει μέριμνα και για τα ακόλουθα:

- Υλοποίηση μηχανισμού ελέγχου πρόσβασης που να μπορεί να δείξει ποιος έχει αιτηθεί πρόσβαση σε κάποιο αρχείο
- Υλοποίηση μηχανισμού ελέγχου πρόσβασης που να υποδεικνύει σε ποια αρχεία μπορεί να έχει πρόσβαση ο κάθε χρήστης
- Τακτικός έλεγχος δικαιωμάτων και έγκαιρη ανάκληση αυτών όταν απαιτείται
- Να ανακοινώνονται γραπτώς τα δικαιώματα πρόσβασης των χρηστών και οι χρήστες να υπογράφουν δήλωση που θα βεβαιώνει ότι κατανοούν και αποδέχονται τα δικαιώματά τους.

Κτηριακές Εγκαταστάσεις

Υπάρχει κανονισμός για την είσοδο στις Κτηριακές εγκαταστάσεις αλλά θα πρέπει να τεκμηριωθεί μια Πολιτική Φυσικής Ασφάλειας και Φυσικής Πρόσβασης και να ανακοινωθεί σε όλα τα εμπλεκόμενα άτομα. Επιπλέον, θα πρέπει να διενεργούνται οι προκαθορισμένες περιπολίες στους χώρους και στα γραφεία της εταιρείας τις μη εργάσιμες ημέρες και ώρες.

Εξοπλισμός

Για τον εξοπλισμό θα πρέπει να τεκμηριωθεί Πολιτική Συντήρησης Εξοπλισμού. Επιπλέον, πρέπει να υπάρξει μέριμνα για την ασφαλή φύλαξή του, να διενεργούνται συχνότεροι έλεγχοι απογραφής εξοπλισμού και ο κάθε εργαζόμενος να υποχρεούται να επιστρέψει στην εταιρεία κατά την αποχώρηση - λήξη σύμβασής του, οποιοδήποτε είδος εξοπλισμού που θεωρείται περιουσία της εταιρείας.

Περιστατικά Ασφάλειας

Πρέπει να υπάρχουν μηχανισμοί που θα ανιχνεύουν παραβιάσεις ασφάλειας, μέσω των οποίων θα ενημερώνονται οι υπεύθυνοι. Εν συνεχεία, πρέπει να τεκμηριωθεί Πολιτική Αναφοράς και Διαχείρισης Αδυναμιών και Περιστατικών Ασφάλειας, καθώς και διαδικασίες έγκαιρης αντιμετώπισης περιστατικών που ενδέχεται να απειλήσουν την ασφάλεια του Π.Σ..

Διαβάθμιση της Πληροφορίας

Αναφορικά με την Πολιτική Κατηγοριοποίησης και Διαχείρισης Πληροφοριακών Περιουσιακών Στοιχείων, θα πρέπει να γίνει επικαιροποίησή της, συμπεριλαμβάνοντας τη διαβάθμιση για όλα τα νέα πληροφοριακά περιουσιακά στοιχεία της εταιρείας. Επίσης, πρέπει να καθοριστούν συγκεκριμένες διαδικασίες διαχείρισής τους με βάση αυτή την κατηγοριοποίηση.

Αποσπώμενες συσκευές

Εκτός από την Πολιτική Χρήσης Αποσπώμενων Συσκευών που υπάρχει σαν έγγραφο και σε γενικές γραμμές ακολουθείται, θα πρέπει να παρθούν κάποια μέτρα, έτσι ώστε οι σταθμοί εργασίας που χρησιμοποιούνται από τους χρήστες να μην διαθέτουν δυνατότητα εξαγωγής δεδομένων με χρήση αποσπώμενων μέσων, εκτός από περιπτώσεις που κάτι τέτοιο κρίνεται αναγκαίο για τη διεκπεραίωση εργασιών και μόνο έπειτα από έγκριση του Υπεύθυνου Ασφάλειας.

4.2 Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)

Ο σκοπός ενός ολοκληρωμένου Σχεδίου Επιχειρησιακής Συνέχειας (Business Continuity Plan) είναι να παρουσιάσει το πλαίσιο ενεργειών με στόχο την εξασφάλιση της Επιχειρησιακής Συνέχειας των κρίσιμων λειτουργιών της εταιρείας. Στο συγκεκριμένο Σχέδιο θα πρέπει να περιγράφονται όλες οι ενέργειες και τα βήματα που πρέπει να ακολουθηθούν προκειμένου να συνεχιστεί η ομαλή λειτουργία των κρίσιμων επιχειρησιακών λειτουργιών και πληροφοριακών υποδομών της εταιρείας σε περίπτωση φυσικής ή άλλης καταστροφής.

Ένα αποτελεσματικό Σχέδιο Επιχειρηματικής Συνέχειας (Business Continuity Plan) πρέπει να καταγράφει τις απαραίτητες ενέργειες και τις διαδικασίες που θα πρέπει να ακολουθούνται πριν, κατά τη διάρκεια και μετά από μία κρίση καθώς και τους απαιτούμενους πόρους. Ως

εκ τούτου, η ανάπτυξη ενός Σχεδίου Επιχειρηματικής Συνέχειας θα μπορούσε να έχει τα ακόλουθα αποτελέσματα:

- Υψηλά επίπεδα ετοιμότητας των εργαζομένων για τη διασφάλιση της ασφάλειας του προσωπικού και μιας οργανωμένης ανταπόκρισης στην κρίση.
- Συμμόρφωση με τις ισχύουσες ρυθμιστικές απαιτήσεις για την αποφυγή δυνητικών κυρώσεων.
- Ανάκτηση, με σειρά προτεραιότητας, των επιχειρηματικών λειτουργιών και διαδικασιών, ώστε να επιτευχθεί η βέλτιστη κατανομή των πόρων με έμφαση στην προστασία των εσόδων και τον περιορισμό των εξόδων.
- Εξατομικευμένες στρατηγικές ανταπόκρισης με έμφαση στα πιο πιθανά σενάρια για τη διασφάλιση της πιο αποτελεσματικής και αποδοτικής κατανομής του προϋπολογισμού του Πλάνου.
- Οργανωμένο πλαίσιο επικοινωνίας για την ανταπόκριση σε περιστατικά, σχεδιασμένο να καλύπτει εσωτερικές και εξωτερικές απαιτήσεις.
- Βελτιωμένη ενημέρωση σχετικά με τα Σχέδια Επιχειρηματικής Συνέχειας των προμηθευτών / συνεργατών της εταιρείας για τη διασφάλιση της αδιάλειπτης λειτουργίας.

Έπειτα από την Ανάλυση και Διαχείριση Επικινδυνότητας, όπου έχουν αναγνωριστεί και αξιολογηθεί οι κίνδυνοι που απειλούν τις επιχειρησιακές λειτουργίες και έχουν εκτιμηθεί οι επιπτώσεις (οικονομικές, λειτουργικές κλπ.) που μπορεί να έχουν αυτοί οι κίνδυνοι για την εταιρεία θα πρέπει να καθοριστούν τα ακόλουθα:

- Οι προτεραιότητες ανάκτησης των κρίσιμων επιχειρησιακών λειτουργιών και πληροφοριακών συστημάτων της εταιρείας.
- Τα χρονικά περιθώρια ανάκτησης (Recovery Time Objectives, RTO) των επιχειρησιακών λειτουργιών και συστημάτων πληροφορικής της εταιρείας.
- Τα επιθυμητά σημεία ανάκτησης (Recovery Point Objectives, RPO) των επιχειρησιακών λειτουργιών και συστημάτων πληροφορικής της εταιρείας.

- Οι απαιτούμενοι πόροι πληροφορικής (π.χ. υλικό και λογισμικό, υλικό τεκμηρίωσης των συστημάτων κ.λπ.) που είναι απαραίτητοι για την ανάκτηση των επιχειρησιακών λειτουργιών και των συστημάτων της εταιρείας.
- Οι απαιτούμενοι ανθρώπινοι πόροι και οι δεξιότητες που θα πρέπει αυτοί να διαθέτουν για την ανάκτηση των επιχειρησιακών λειτουργιών και των συστημάτων της εταιρείας.

Προσδιορισμός στρατηγικής της ανάκτησης

Για τον προσδιορισμό της βέλτιστης στρατηγικής ανάκτησης των πληροφοριακών συστημάτων της εταιρείας πραγματοποιούνται τα ακόλουθα:

- Ανάπτυξη σεναρίων καταστροφής
- Καθορισμός εναλλακτικών στρατηγικών ανάκτησης των συστημάτων και των μεθόδων επίτευξής τους, η κάθε μια από τις οποίες αντιστοιχεί σε διαφορετικό κόστος και αποτελεσματικότητα
- Πραγματοποίηση ανάλυσης κόστους-οφέλους κάθε εναλλακτικής στρατηγικής ανάκτησης για την επιλογή της βέλτιστης στρατηγικής.

Σχέδιο Επιχειρησιακής Συνέχειας

Στο πλαίσιο της ανάπτυξης ενός αποτελεσματικού και ολοκληρωμένου Σχεδίου Επιχειρησιακής Συνέχειας, αναπτύσσονται τα ακόλουθα επιμέρους σχέδια:

- Σχέδιο Αντιμετώπισης Εκτάκτων Γεγονότων,
- Σχέδιο Διαχείρισης Κρίσεων (Crisis Management Plan) – Για την αποτελεσματική διαχείριση και αντιμετώπιση έκτακτων περιστατικών / κρίσεων.
- Σχέδιο Ανάκτησης Επιχειρησιακών Μονάδων / Λειτουργιών (Business Unit Recovery Plan) που διασφαλίζει την απρόσκοπτη λειτουργία της εταιρείας σε επίπεδο επιχειρησιακών μονάδων / λειτουργιών. Η ανάπτυξη του σχεδίου αυτού βασίζεται στα αποτελέσματα της εκτίμησης των κινδύνων και της ανάλυσης των επιχειρησιακών επιπτώσεων, που προσδιορίζουν τις κρίσιμες επιχειρησιακές μονάδες / λειτουργίες, τις επιπτώσεις από τη διακοπή της λειτουργίας τους και τους απαιτούμενους χρόνους ανάκτησής τους.

- Σχέδιο Ανάκτησης Πληροφοριακών Συστημάτων από Καταστροφή (Disaster Recovery Plan), το οποίο περιλαμβάνει όλες τις απαραίτητες διαδικασίες για την ανάκτηση των πληροφοριακών συστημάτων και των δεδομένων της εταιρείας σε περίπτωση φυσικής ή άλλης καταστροφής.
- Σχέδιο Διαχείρισης Θεμάτων Επικοινωνίας και ΜΜΕ

Ενδεικτικά τα Σχέδια Συνέχειας Εργασιών που θα αναπτυχθούν θα πρέπει να περιλαμβάνουν:

- Γενικά στοιχεία: στόχοι, παραδοχές, εύρος σχεδίου.
- Καθορισμό επιμέρους ομάδων, καθώς επίσης και των σχετικών ρόλων και αρμοδιοτήτων τους.
- Τις διαδικασίες αντιμετώπισης εκτάκτων περιστατικών (Emergency Response).
- Διαδικασίες προειδοποίησης, ενεργοποίησης του πλάνου και κλιμάκωσης των ενεργειών.
- Τις διαδικασίες ανάκαμψης και συνέχειας των κρίσιμων εργασιών σε επιχειρησιακό επίπεδο (Business Level).
- Τις διαδικασίες ενημέρωσης εμπλεκομένων στελεχών και της ενεργοποίησης του σχεδίου.
- Καθορισμό του κέντρου συντονισμού και ελέγχου των διαδικασιών επιχειρησιακής συνέχειας.
- Στοιχεία επικοινωνίας των μελών των ομάδων, με τρίτους φορείς / οργανισμούς.

Απαιτήσεις λεπτομερών σχεδίων δοκιμών

Αναπτύσσονται λεπτομερή σχέδια των δοκιμών, πριν εκτελεστεί οποιαδήποτε δοκιμή των σχεδίων συνέχειας. Τα σχέδια δοκιμών περιγράφουν σαφώς το πεδίο εφαρμογής, τους στόχους, όπως και το χρόνο διεξαγωγής των δοκιμών. Τα στοιχεία αυτά είναι τεκμηριωμένα και συγκρίνονται αργότερα με τα αποτελέσματα των δοκιμών για να ελεγχθεί ο βαθμός επίτευ-ξης των προδιαγεγραμμένων στόχων.

Τεκμηρίωση των αποτελεσμάτων των δοκιμών και ελλείψεων των σχεδίων

Τα αποτελέσματα των δοκιμών και οι παρατηρούμενες ελλείψεις των σχεδίων τεκμηριώνονται κατά τη διάρκεια και μετά το πέρας της δοκιμής τους, έτσι ώστε να διασφαλίζεται ότι τα σχέδια είναι σύγχρονα και ανταποκρίνονται στις τρέχουσες ανάγκες.

Συχνότητα των δοκιμών

Δοκιμές πραγματοποιούνται ανά τακτά χρονικά διαστήματα (π.χ. δύο φορές ετησίως). Αυτές οι δοκιμές μπορεί να είναι δοκιμές ολόκληρων των σχεδίων ή τμημάτων αυτών.

Εφαρμογή σε ένα εύρος πιθανών διακοπών λειτουργίας

Το πεδίο εφαρμογής των δοκιμών πρέπει να περιλαμβάνει ένα εύρος πιθανών διακοπών λειτουργίας, κατά τη διάρκεια ωρών αιχμής ή μη, έτσι ώστε να εξοικειωθεί το προσωπικό με όλα τα πιθανά σενάρια καταστροφής.

Ανάγκες δοκιμών έπειτα από σημαντικές αλλαγές

Δοκιμές του Σχεδίου Επιχειρησιακής Συνέχειας εκτελούνται έπειτα από κάθε μεγάλη αλλαγή στο επιχειρησιακό περιβάλλον της εταιρείας.

Κεφάλαιο 5

Σύγκριση CRAMM – OCTAVE Allegro

Για το Πληροφοριακό Σύστημα που μελετήθηκε πρέπει να επιλεγεί η καταλληλότερη μέθοδος μεταξύ της μεθόδου CRAMM και Octave Allegro. Κατά καιρούς έχουν δημοσιευτεί διάφορα κείμενα [11], [12], [13], [14] τα οποία περιέχουν συγκρίσεις μεθόδων ανάλυσης επικινδυνότητας ή και μειονεκτήματα και πλεονεκτήματα διαφόρων μεθόδων. Από τα κείμενα αυτά μπορεί κανείς να πάρει ιδέες για την προσέγγιση που θα ακολουθήσει αναφορικά με τις επιλεγείσες περιοχές σύγκρισης.

Η παρούσα σύγκριση έχει βασιστεί στα όσα προέκυψαν από την παραπάνω ανάλυση του Π.Σ και η επιλογή της πιο κατάλληλης μεθόδου, θα γίνει λαμβάνοντας υπόψη όσα αναφέρονται στον πίνακα 16 που ακολουθεί.

Όταν μία περιοχή καλύπτεται πλήρως από τη μέθοδο, θεωρείται πλεονέκτημα της μεθόδου και σημειώνεται ο βαθμός «1», όταν θεωρείται μειονέκτημα της μεθόδου σημειώνεται ο βαθμός «-1» και ότι δεν μπορεί να θεωρηθεί πλεονέκτημα ή μειονέκτημα σημειώνεται ο βαθμός «0».

Περιοχές Σύγκρισης	**Μέθοδοι**	
Μέγεθος / Πολυπλοκότητα Π.Σ.	**CRAMM (+1)**	**OCTAVE (-1)**
	Μπορεί να χρησιμοποιηθεί σε πολύπλοκα και ανεξαρτήτου μεγέθους Π.Σ.	Ενδείκνυται για μικρά Π.Σ. χωρίς ιδιαίτερη πολυπλοκότητα. Δυσκολία υλοποίησης στο συγκεκριμένο Π.Σ. λόγω του μεγάλου όγκου των φύλλων εργασίας.
Περιοχές Κάλυψης	**CRAMM (+1)**	**OCTAVE (0)**
	Καλύπτει όλες τις συνιστώσες ασφάλειας (θέματα προσωπικού, θέματα διαδικασιών, τεχνικά θέματα, φυσική και περιβαλλοντική ασφάλεια κ.τ.λ.)	Η κάλυψη των συνιστωσών ασφάλειας εξαρτάται από την εμπειρία του αναλυτή και ενδέχεται να μην ληφθούν υπόψη κρίσιμες περιοχές.

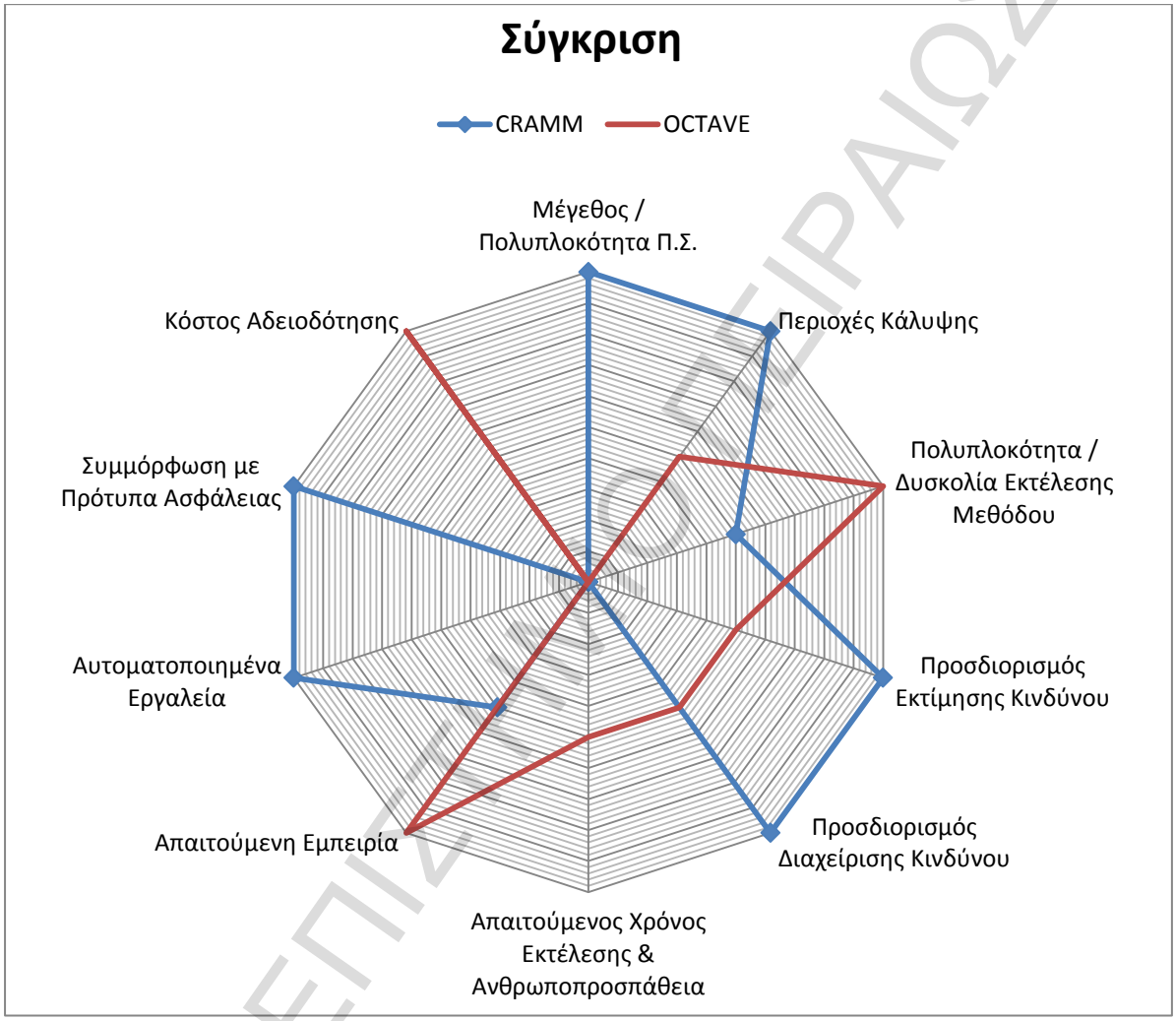
Πολυπλοκότητα Μεθόδου	**CRAMM (0)**	**OCTAVE (+1)**
	Υψηλή πολυπλοκότητα που προκύπτει από τα ακόλουθα: Γίνεται διαχωρισμός του περιουσιακού στοιχείου σε δεδομένα, λογισμικό και υλικό καθώς καθένα από αυτά μπορεί να χρήζουν διαφορετικού επίπεδου ασφάλειας. Τα δεδομένα διαχωρίζονται σε επιμέρους κατηγορίες (π.χ. οικονομικά, επιχειρησιακά ευαίσθητα κ.τ.λ.). Καθορίζεται η αξία των φυσικών αγαθών, βάσει της αξίας αντικατάστασης τους.	Χαμηλή πολυπλοκότητα που προκύπτει από τα ακόλουθα: Για τον προσδιορισμό του περιουσιακού στοιχείου δεν απαιτείται διαχωρισμός σε δεδομένα, υλικό και λογισμικό αλλά περιγράφονται ως επιμέρους συστατικά του. Παρακάμπτει το ζήτημα του υπολογισμού συγκεκριμένων χρηματικών ποσών για την αξία των αγαθών.
Προσδιορισμός Εκτίμησης Κινδύνου	**CRAMM (+1)**	**OCTAVE (0)**
	Για την εκτίμηση του κινδύνου λαμβάνει υπόψη την κατηγορία που έχει μεγαλύτερη προκληθείσα συνέπεια για την εταιρεία. Για την αποτίμηση σε περιπτώσεις όπως απώλεια δεδομένων γίνεται υπολογισμός της επίπτωσης λαμβάνοντας υπόψη το χρονικό διάστημα. (π.χ για το σύστημα πελατών η απώλεια των δεδομένων για χρονικό διάστημα 1 ημέρας δεν έχει σημαντική οικονομική απώλεια ενώ για χρονικό διάστημα μεγαλύτερο της μίας εβδομάδας έχει πολύ μεγάλη οικονομική απώλεια και δημιουργεί πρόβλημα ρευστότητας για την εταιρεία).	Για την εκτίμηση του κινδύνου λαμβάνει υπόψη όλες τις περιοχές (π.χ. οικονομικά, φήμη κ.τ.λ.) που μπορεί να έχει επίπτωση ο κάθε κίνδυνος και προσθέτοντάς τες γίνεται ο υπολογισμός του συνολικού κινδύνου. Δεν λαμβάνει υπόψη την απώλεια των δεδομένων ή του συστήματος για συγκεκριμένο χρονικό διάστημα, κάτι το οποίο σε πολλές περιπτώσεις είναι σημαντικό για τον καθορισμό του χρόνου ανάκτησης / αποκατάστασης του συστήματος, καθώς διαφορετική επίπτωση έχει η απώλεια για μία εβδομάδα από ότι η απώλεια για ένα μήνα.

	CRAMM (+1)	OCTAVE (0)
Προσδιορισμός Διαχείρισης κινδύνου	Για τη διαχείριση του κινδύνου, λαμβάνονται υπόψη όλοι οι πιθανοί κίνδυνοι ανεξαρτήτως επιπέδου επικινδυνότητας. Επιπλέον η επιλογή του τρόπου αντιμετώπισης καθορίζεται από τον αναλυτή, εκτιμώντας την υπάρχουσα κατάσταση (όπως Εγκατεστημένο, Προς υλοποίηση, Έχει ήδη καλυφθεί, Αποδεκτός εναπομένων βαθμός κινδύνου, Μη εφαρμόσιμο).	Για τη διαχείριση του κινδύνου συνυπολογίζεται η πιθανότητα εκδήλωσης μιας απειλής με τον συνολικό βαθμό κινδύνου. Σύμφωνα με τον συνολικό βαθμό κινδύνου οι απειλές ταξινομούνται σε ομάδες. Ανάλογα με την ομάδα (1 - 4) στην οποία ανήκει κάθε απειλή καθορίζεται και ο τρόπος αντιμετώπισής της (Αποδοχή, Αναβολή, Μείωση, Μεταφορά). Με αυτό τον τρόπο υπάρχει η πιθανότητα να μην ληφθούν μέτρα για απειλές που σημειώνουν χαμηλή πιθανότητα εκδήλωσης ενώ αν εκδηλωθούν θα επέφεραν κρίσιμες επιπτώσεις. (π.χ αν για ένα αγαθό η πιθανότητα εκδήλωσης του μεσαία και ο συνολικός βαθμός μικρότερος του 15 τότε θα ενταχθεί στην ομάδα 3 και δεν θα ληφθούν μέτρα για την αντιμετώπισης της απειλής.
	CRAMM (-1)	**OCTAVE (0)**
Απαιτούμενος Χρόνος Εκτέλεσης και Ανθρωποπροσπάθεια	Απαιτεί μεγάλη προσπάθεια και χρόνο, που προκύπτουν από την πολυπλοκότητα των διαφόρων φάσεων της μεθόδου, από τους διάφορους γύρους συνεντεύξεων που πρέπει να γίνουν με τα αρμόδια άτομα της εταιρείας και τις απαντήσεις που πρέπει να δοθούν στα ερωτηματολόγια που παράγει η μέθοδος.	Είναι εύκολα κατανοητή. Όταν πρόκειται για μικρό Π.Σ. απαιτεί ελάχιστο χρόνο και ελάχιστους πόρους για να υλοποιηθεί. Για μεγάλο Π.Σ. δεν είναι ιδανική, καθώς είναι δύσκολο να προσδιοριστεί το κρίσιμο περιουσιακό στοιχείο και να συμπληρωθεί ο μεγάλος όγκος των φύλλων εργασίας.

Απαιτούμενη Εμπειρία / Εξειδίκευση / Τεχνογνωσία / προφίλ αναλυτή	**CRAMM (0)**	**OCTAVE (+1)**
	Λαμβάνοντας υπόψη την πολυπλοκότητα του εργαλείου και τις φάσεις της μεθόδου, απαιτείται εξειδίκευση τόσο στη χρήση του εργαλείου καθώς και εμπειρία στην εκτέλεση παρόμοιων αναλύσεων.	Μπορεί να υλοποιηθεί από μη έμπειρους αναλυτές. Παρέχει κατευθυντήριες οδηγίες, φύλλα εργασίας και παράδειγμα χρήσης της μεθόδου, τα οποία είναι εύκολα κατανοητά και καθοδηγούν το αναλυτή σε όλα τα στάδια της μεθόδου. Συνηθίζεται να εκτελείται ακόμη και από άτομα εσωτερικά της εταιρείας, καθώς το μόνο που πρέπει να γνωρίζουν είναι το περιβάλλον και τις ιδιαιτερότητες του Π.Σ.
Αυτοματοποιημένα Εργαλεία	**CRAMM (+1)**	**OCTAVE (-1)**
	Διαθέτει το αυτοματοποιημένο εργαλείο CRAMM Express / Expert μέσω του οποίου παρέχεται μία λίστα από απειλές βοηθώντας την αντιστοίχιση των απειλών στα περιουσιακά στοιχεία. Επιπλέον διαθέτει μία μεγάλη βιβλιοθήκη αντιμέτρων. Backtrack: επιτρέπει τον προσδιορισμό των παραγόντων που οδήγησαν σε ένα συγκεκριμένο αντίμετρο.	Δεν διαθέτει κάποιο εργαλείο. Βασίζεται σε φύλλα εργασίας και κατευθυντήριες οδηγίες που παρέχονται από τη μέθοδο. Ο αναλυτής επιλέγει μόνος του τις απειλές και τα αντίμετρα χωρίς να του παρέχονται έτοιμες λίστες από τη μέθοδο. Στην περίπτωση όμως που ο αναλυτής δεν είναι έμπειρος υπάρχει ο κίνδυνος να μην ληφθούν υπόψη σημαντικές απειλές.
Συμμόρφωση με Πρότυπα Ασφάλειας	**CRAMM (+1)**	**OCTAVE (-1)**
	Αντιστοίχιση με τα σημεία ελέγχου που προβλέπονται στο πρότυπο ISO 27001.	Δεν υπάρχει αντιστοίχιση με κάποιο πρότυπο Ασφάλειας.
Κόστος (Αδειοδότηση / Άδεια χρήσης μεθόδου)	**CRAMM (-1)**	**OCTAVE (+1)**
	Απαιτείται η αγορά άδειας χρήσης σε ετήσια βάση.	Παρέχεται δωρεάν.

Πίνακας 16: Σύγκριση CRAMM- OCTAVE Allegro

Με βάση τα παραπάνω η μέθοδος CRAMM υπερισχύει έναντι της μεθόδου Octave Allegro, καλύπτοντας το μεγαλύτερο σύνολο των κριτηρίων και έτσι κρίνεται ως καταλληλότερη για το Π.Σ. που μελετήθηκε. Το αποτέλεσμα αυτής της σύγκρισης αναπαρίσταται στην εικόνα 5.



Εικόνα 5: Περιοχές κάλυψης CRAMM - Octave Allegro

Κεφάλαιο 6

Συμπεράσματα - Προτάσεις

Για να μπορέσει να γίνει η επιλογή της πιο κατάλληλης μεθόδου θα πρέπει να υπάρχει γνώση του περιβάλλοντος που πρόκειται να χρησιμοποιηθεί, καθώς και γνώση των συγκρίσιμων μεθόδων. Είναι σημαντικό να γίνει μία ανάλυση με τις μεθόδους που βρίσκονται πλησιέστερα στις απαιτήσεις της εταιρείας, να υπάρχει γνώση της κουλτούρας και του διαθέσιμου προϋπολογισμού καθώς έτσι μπορεί να επιλεγεί η πιο κατάλληλη μέθοδος.

Για το Π.Σ. που μελετήθηκε λαμβάνοντας υπόψη την πολυπλοκότητα και το μεγάλο εύρος των συστημάτων που διαθέτει, ταιριάζει περισσότερο η μεθοδολογία CRAMM. Μέσω της μεθόδου αυτής, ο αναλυτής κερδίζει χρόνο από την αναζήτηση απειλών και αντιμέτρων, καθώς αυτά διατίθενται μέσω του εργαλείου.

Η Octave Allegro θα μπορούσε να υλοποιηθεί εύκολα και γρήγορα, μόνο για ένα πολύ μικρό κομμάτι του Π.Σ. (π.χ. μόνο για το σύστημα Πελατών) και με την προϋπόθεση ότι ο αναλυτής γνωρίζει πολύ καλά το περιβάλλον της εταιρείας.

Η ανάλυση με τη χρήση της Octave Allegro θα πρέπει να γίνει πολύ προσεκτικά ως προς τις περιοχές που πρέπει να καλυφθούν, καθώς δεν έχει κάποιο βοηθητικό εργαλείο που να καλύπτει όλες τις απαραίτητες περιοχές, με αποτέλεσμα να μην ληφθούν υπόψη περιοχές κρίσιμες για την ασφάλεια του Π.Σ. Επιπλέον υπάρχει η ανάγκη για αναζήτηση αντιμέτρων μιας και η Octave Allegro δεν διαθέτει κάποια έτοιμη λίστα.

Λόγω του ότι συνεχώς προστίθενται νέα συστήματα που βρίσκονται σε αλληλεπίδραση με τα ήδη υπάρχοντα, δημιουργείται η ανάγκη μίας συνεχώς επαναλαμβανόμενης μελέτης ανάλυσης επικινδυνότητας. Επιλέγοντας μία συγκεκριμένη μέθοδο, είναι πιο εύκολα συγκρίσιμα τα αποτελέσματα μιας επόμενης μελέτης με μία προηγούμενη, από ότι εάν κάθε φορά χρησιμοποιούνταν μία διαφορετική μέθοδος.

Λαμβάνοντας υπόψη όλα τα προαναφερθέντα πλεονεκτήματα και μειονεκτήματα των μεθόδων CRAMM και OCTAVE Allegro και το γεγονός ότι η ανάλυση επικινδυνότητας είναι απαραίτητο συστατικό για την ορθή διαχείριση της ασφάλειας, θα ήταν αρκετά χρήσιμη για τον αναλυτή η ύπαρξη ενός νέου μεθοδολογικού πλαισίου και του αντίστοιχου υποστηρικτικού εργαλείου. Το εργαλείο αυτό θα μπορούσε να ενσωματώσει θετικά στοιχεία και των δύο μεθό-

δων-εργαλείων, όπως για παράδειγμα να περιέχει λίστα από απειλές, ευπάθειες και αντίμετρα και να προσφέρει τη δυνατότητα εύκολης παραμετροποίησης και ανανέωσης αυτών.

Όπως αναφέρθηκε και προηγουμένως η Octave Allegro παρόλη την ευκολία υλοποίησης της, ενδείκνυται κυρίως για μικρά Π.Σ., θα ήταν λοιπόν χρήσιμο η νέα μέθοδος να μπορεί να εφαρμόζεται σε ανεξαρτήτως μεγέθους Π.Σ., όπως και η CRAMM, αλλά να προσφέρει αντίστοιχο βαθμό ευχρηστίας. Πολύ σημαντικό κομμάτι είναι και η ενσωμάτωση νέων περιοχών ασφάλειας (π.χ. Mobile Device Managment). Θα πρέπει επίσης το νέο εργαλείο να λαμβάνει υπόψη τις τεχνολογικές εξελίξεις και να ενσωματώνει νέα αντίμετρα όπως ανανέωση παρωχημένων πρωτοκόλλων, λειτουργικών συστημάτων κ.τ.λ., ούτως ώστε να παρέχεται ένα καλύτερο επίπεδο διαχείρισης του κινδύνου.

Λαμβάνοντας ως δεδομένο ότι πολλές εταιρείες ακολουθούν τις απαιτήσεις κάποιου προτύπου π.χ. ISO 27001, θα ήταν χρήσιμο το νέο εργαλείο να είναι συμβατό με διάφορα πρότυπα / πλαίσια ασφάλειας όπως ISO 27001:2013, NIST, COBIT, ITIL κ.τ.λ. και να παρέχεται στον αναλυτή η δυνατότητα επιλογής.

Τέλος, θα ήταν πολύ σημαντικό το εργαλείο να έχει δυνατότητα εξαγωγής αναφορών και εκθέσεων σε format που διευκολύνουν τη διαλειτουργικότητα, π.χ. xml, αλλά και να παρέχονται δυνατότητες visualization, έτσι ώστε να είναι πιο εύκολο για τον αναλυτή να κατανοήσει και να παρουσιάσει τα δεδομένα.

Βιβλιογραφία

[1] «http://www.dpa.gr/portal/page?_pageid=33,132277&_dad=portal&_schema=PORTAL,» [Ηλεκτρονικό].

[2] Σ. Κάτσικας, Δ. Γρίτζαλης και Σ. Γρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων,» Αθήνα, Εκδόσεις Νέων Τεχνολογιών, 2004.

[3] Filipe Neto Rodeia Macedo , «Models for Assessing Information Security Risk,» 2009.

[4] Douglas J. Landoll, «The Security Risk Assessment Handbook,» 2011.

[5] «http://rm-inv.enisa.europa.eu/methods/m_cramm.html,» [Ηλεκτρονικό].

[6] Zeki Yazar, «SANS Institute Infosec Reading Room,» 2011. [Ηλεκτρονικό]. Available: http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83?show=qualitative-risk-analysis-management-tool-cramm-83&cat=auditing.

[7] *CRAMM User Guide,* 2005.

[8] Μελετητική Ομάδα Ασφάλειας Πανεπιστημίου Αιγαίου, *Αποτίμηση Αγαθών των Πληροφοριακών Συστημάτων.*

[9] Σ. Κάτσικας, «Ασφάλεια Υπολογιστών,» Πάτρα, 2011.

[10] Richard A. Caralli , James F. Stevens, Lisa R. Young και William R. Wilson, «The OCTAVE Allegro Guidebook,» May 2007.

[11] E. Wheeler, Security Risk Managment, Waltham, USA: Elsevier, 2011.

[12] F. Macedo και Mira da Silva, «Comparative Study of Information Security Risk Assessment Models,» Lisboa, Portuga.

[13] «Enisa,» [Ηλεκτρονικό]. Available: http://rm-inv.enisa.europa.eu/methods/compare_frames.html?m1=http://rm-inv.enisa.europa.eu/methods/m_cramm.html&m2=m_octave.html.

[14] Ε. Ρεκλείτης , «Πρακτικός οδηγός του εργαλείου ασφάλειας CRAMM,» Πανεπιστήμιο Πειραιώς, Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων.

Παράρτημα Α

Κλίμακες αποτίμησης Δεδομένων [14]

Διεθνείς σχέσεις

ΑΠΩΛΕΙΑ	ΤΙΜΗ
Δεν ορίζεται	1
Δεν ορίζεται	2
Μικρή επίπτωση στις διπλωματικές σχέσεις – "Περιορισμένης Χρήσης"	3
Δεν ορίζεται	4
Δεν ορίζεται	5
Δεν ορίζεται	6
Σημαντική επίπτωση στις διπλωματικές σχέσεις – "Εμπιστευτικό"	7
Δεν ορίζεται	8
Ένταση στις διεθνείς σχέσεις ή δυσμενής επίπτωση στις σχέσεις με φιλικό κράτος – "Απόρρητο"	9
Πολύ σημαντική επίπτωση στις σχέσεις με φιλικά κράτη ή απειλή της σταθερότητας στην περιοχή – "Άκρως Απόρρητο"	10

Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας

ΑΠΩΛΕΙΑ	ΤΙΜΗ
<1.000 Ευρώ	1
1.001-10.000 Ευρώ	2
10.001-30.000 Ευρώ	3
30.001-100.000 Ευρώ	4
100.001-300.000 Ευρώ	5
300.001-1.000.000 Ευρώ	6
>1.000.001 Ευρώ (έμμεση απώλεια)	7
>1.000.001 Ευρώ (άμεση απώλεια)	8
Δεν ορίζεται	9
Δεν ορίζεται	10

Αποκάλυψη προσωπικών πληροφοριών

ΣΥΝΕΠΕΙΑ	ΤΙΜΗ
Μικρή ενόχληση ενός ατόμου	1
Μεγάλη ενόχληση ενός ατόμου	2
Παραβίαση νομοθεσίας και μικρή ενόχληση	3
Παραβίαση νομοθεσίας και μεγάλη ενόχληση	4
Παραβίαση νομοθεσίας και σοβαρή ενόχληση	5
Παραβίαση νομοθεσίας και σοβαρή ενόχληση πολλών ατόμων	6

Εφαρμογή πολιτικής και λειτουργία δημόσιου οργανισμού

ΣΥΝΕΠΕΙΑ	ΤΙΜΗ
Ανεπαρκής λειτουργία μέρους του οργανισμού	1
Υπονόμευση της σωστής διαχείρισης ή/και λειτουργίας ενός δημόσιου οργανισμού	3
Παρεμπόδιση της αποτελεσματικής ανάπτυξης και εφαρμογής των κυβερνητικών πολιτικών	5
Υποβάθμιση της διαπραγματευτικής και συναλλακτικής δυνατότητας της κυβέρνησης	6
Σοβαρή παρεμπόδιση ή διακοπή της ανάπτυξης και εφαρμογής κυβερνητικών πολιτικών	7

Απώλεια καλής φήμης

ΣΥΝΕΠΕΙΑ	ΤΙΜΗ
Απώλεια περιορίζεται στον οργανισμό	2
Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Έντονη αποδοκιμασία κοινού σε εθνική κλίμακα	7

Παρεμπόδιση δικαιοσύνης

ΣΥΝΕΠΕΙΑ	ΤΙΜΗ
Διευκόλυνση πραγματοποίησης εγκλήματος ή παρεμπόδιση των ερευνών	3
Διακοπή των ερευνών ή διακοπή της δίκης	4
Διευκόλυνση της πραγματοποίησης σοβαρού εγκλήματος ή παρεμπόδιση των ερευνών	7
Διακοπή των ερευνών ή διακοπή της δίκης ενός σοβαρού εγκλήματος	8

Εθνική ασφάλεια

ΣΥΝΕΠΕΙΑ	ΤΙΜΗ
Υποβάθμιση της αποτελεσματικότητας επιχειρήσεων εθνικής ή δημόσιας ασφάλειας ή αποκάλυψη εμπιστευτικών (confidential) πληροφοριών	7
Σοβαρή ζημιά στην εθνική ή τη δημόσια ασφάλεια ή αποκάλυψη Απόρρητων (secret) πληροφοριών	9
Πολύ σοβαρή ζημιά στην εθνική ασφάλεια ή αποκάλυψη Άκρως Απόρρητων (top secret) πληροφοριών	10

Εμπορικά και οικονομικά συμφέροντα

ΑΠΩΛΕΙΑ	ΤΙΜΗ
Μη οικονομική ωφέλεια ανταγωνιστή	1
Ωφέλεια ανταγωνιστή μέχρι 10.000 Ευρώ	2
Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 100.000 Ευρώ	3
Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 1.000.000 Ευρώ	4
Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 10.000.000 Ευρώ	5
Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή περισσότερο των 10.000.000 Ευρώ	6
Πρόκληση οικονομικής ζημιάς σε εθνικό επίπεδο	7
Σημαντική ζημιά στην εθνική οικονομία με βραχυπρόθεσμες συνέπειες	9
Σημαντική ζημιά στην εθνική οικονομία με μακροπρόθεσμες συνέπειες	10

Παραβίαση νομοθεσίας

ΑΠΩΛΕΙΑ	ΤΙΜΗ
Αποζημίωση ή πρόστιμο < 2.000 Ευρώ	3
Αποζημίωση ή πρόστιμο < 10.000 Ευρώ	4
Αποζημίωση ή πρόστιμο < 50.000 Ευρώ ή φυλάκιση μέχρι 2 έτη	5
Πολλαπλές μηνύσεις < 250.000 Ευρώ ή ποινική δίωξη που επιφέρει ποινή φυλάκισης μέχρι 10 έτη	6
Πολλαπλές μηνύσεις, απεριόριστη ζημία ή περισσότερα από 10 έτη φυλάκιση	7