ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΛΥΣΗ ΤΟΥ ΕΡΓΑΛΕΙΟΥ CRAMM

Δημοσχάκης Λουλούδης

Εισηγητής: Κ. Λαμπρινουδάκης – Επίκουρος καθηγητής

2010

Περίληψη

Αντιμετωπίζοντας τις νέες προκλήσεις της εποχής του Διαδικτύου, τα διευθυντικά στελέχη και οι επαγγελματίες πληροφοριών ασφάλειας, των επιχειρήσεων και των κυβερνήσεων, θα πρέπει να διαχειρίζονται συγκεκριμένους κινδύνους για τις επιχειρήσεις και οργανισμούς τους, προκειμένου να εξασφαλίσουν την αποτελεσματική λειτουργία τους.

Η παρούσα διπλωματική εξηγεί τις βασικές συνιστώσες της ανάλυσης κινδύνου και των διαδικασιών διαχείρισης επικινδυνότητας ενός πληροφοριακού συστήματος και αναφέρει διαφορετικές μεθοδολογίες και προσεγγίσεις. Στη συνέχεια περιγράφει και αναλύει τη μέθοδο CRAMM, ως ένα αυτοματοποιημένο εργαλείο ανάλυσης επικινδυνότητας και καταγράφει τα αποτελέσματα της πραγματοποίησης μιας ανάλυσης ρίσκου για ένα πρακτικό σενάριο υλοποίησης εταιρικού δικτύου, μέσω του συγκεκριμένου εργαλείου.

Το Πληροφοριακό Σύστημα της Εταιρίας NEC Unified Solutions αποτελεί το μοντέλο πάνω στο οποίο θα στηριχθεί όλη η μελέτη.

Abstract

Facing the emerging challenges of the Internet era, managers and information security professionals inbusiness and government should manage specific risks to their organizations to ensure efficient operations.

This paper explains basic components of risk analysis and management processes and mentions different methodologies and approaches. It then describes and discusses CRAMM, as an automated tool based on qualitativerisk assessment methodology, by going through the stages of a CRAMM review. At last, a risk analysis for a practical implementation scenario in a corporate network, is carried out, using CRAMM tool.

The Information System of NEC Unified Solutions Company is the model on which i build the whole study.

Περιεχόμενα

Περιεχόμενα πινάκων

Ευχαριστίες

Φτάνοντας στο σημείο να έχω τελειώσει τη διπλωματική μου εργασία, θα ήθελα να ευχαριστήσω τον εισηγητή και επιβλέπων καθηγητή της εργασίας κ. Λαμπρινουδάκη Κώστα, Επίκουρο καθηγητή του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά. Οι γνώσεις του πάνω στο αντικείμενο της παρούσας μελέτης, οι συμβουλές και η στήριξη που μου προσέφερε, βοηθήσανε στο να περατωθεί αυτή η εργασία, εντός του χρονικού ορίου που είχαμε θέσει εξ' αρχής και εντός των στόχων της.

Οφείλω βέβαια να ευχαριστήσω, κυρίως τους γονείς μου, που με στηρίξανε σε κάθε μου βήμα από τη πρώτη στιγμή, προκειμένου να ολοκληρώσω επιτυχώς τις μεταπτυχιακές σπουδές μου.

Πειραιάς, Νοέμβριος 2010
Δημοσχάκης Λουλούδης

Θέμα

“Ανάλυση του εργαλείου CRAMM”

Στη διπλωματική αυτή εργασία θα γίνει μια αναλυτική μελέτη του λογισμικού CRAMM, το οποίο είναι ένα εργαλείο εκτίμησης και αξιολόγησης ρίσκου για επιχειρήσεις και οργανισμούς. Πιο συγκεκριμένα, θα γίνει μια εκτενής μελέτη στις μεθοδολογίες εκτίμησης ρίσκου της CRAMM, καθώς και στα αποτελέσματα που παράγει. Τέλος θα πραγματοποιηθεί μια ανάλυση ρίσκου για ένα πρακτικό σενάριο υλοποίησης εταιρικού δικτύου.

1 Εισαγωγή

1.1 Λίγα λόγια για την εταιρία NEC Unified Solutions

Η NEC Unified Solutions (NEC) διαθέτει πάνω από 50 χρόνια εμπειρία στην παροχή επικοινωνιακών συστημάτων, εφαρμογών, δικτύων και υπηρεσιών σε πελάτες σε ολόκληρο τον κόσμο..

Ειδικεύεται στην παροχή επικοινωνιακών λύσεων σε μικρές, μεσαίες και μεγάλες επιχειρήσεις, τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα. Αυτές οι λύσεις ενσωματώνουν την πιο πρόσφατη τεχνολογία φωνής, δεδομένων και βίντεο, χρησιμοποιώντας επιτραπέζιους και φορητούς σταθμούς εργασίας, και επιτρέπουν συνεργασία σε πραγματικό χρόνο, αυξημένη παραγωγικότητα και σημαντικά βελτιωμένη εξυπηρέτηση πελατών.

1.2 Σκοπός της παρούσας μελέτης

Ο σκοπός της παρούσας μελέτης είναι η καταγραφή του πληροφοριακού συστήματος της εταιρίας NEC και η αποτίμηση του βαθμού επικινδυνότητάς του, μέσω της ανάλυσης επικινδυνότητας που προσφέρει η μέθοδος CRAMM.

2 Ανάλυση και διαχείριση επικινδυνότητας Πληροφοριακού Συστήματος (ΠΣ)

2.1 Γενικά

Τα ζητήματα που αφορούν την ασφάλεια πληροφοριακών συστημάτων αποτελούν ένα από τα προσφιλέστερα θέματα των μέσων μαζικής ενημέρωσης, αλλά και ένα από τα κεντρικά ζητήματα προβληματισμού για τους επαγγελματίες και τους ερευνητές της πληροφορικής. Το ενδιαφέρον αυτό έχει οδηγήσει την έρευνα στην περιοχή της ασφάλειας ΠΣ σε σημαντική ανάπτυξη, με ιδιαίτερη έμφαση στην ανάπτυξη τεχνικών και μέσων προστασίας (κρυπτογραφικές τεχνικές, τεχνικές ανίχνευσης παρεισφρήσεων κ.ά.). Πολλά από τα αποτελέσματα των ερευνητών του χώρου ενσωματώνονται σε προϊόντα που προσφέρονται στην αγορά από πλήθος ειδικευμένων εταιρειών.

Η ένταξη, όμως, των συστημάτων ασφάλειας στο πλαίσιο λειτουργίας ενός οργανισμού δεν θα πρέπει να θεωρηθεί εύκολη υπόθεση, γεγονός που εξηγεί σε μεγάλο βαθμό και το χαμηλό επίπεδο ασφάλειας που παρουσιάζουν τα ΠΣ των σύγχρονων επιχειρήσεων και οργανισμών. Ορισμένες από τις σημαντικότερες δυσκολίες, που αντιμετωπίζουν οι επαγγελματίες του χώρου στην προσπάθειά τους να αναπτύξουν την ασφάλεια ΠΣ σε επιχειρήσεις και οργανισμούς, είναι:

- Η δυσκολία να αιτιολογηθεί το κόστος των μέτρων ασφάλειας.
- Η δυσκολία επικοινωνίας ανάμεσα στους επαγγελματίες της πληροφορικής και τα διοικητικά στελέχη των επιχειρήσεων και οργανισμών.
- Η δυσκολία εξασφάλισης της ενεργητικής συμμετοχής των χρηστών στην προσπάθεια προστασίας του ΠΣ και της διαρκούς υποστήριξης της ανώτερης διοίκησης.
- Η διαδεδομένη αντίληψη ότι η ασφάλεια ΠΣ αποτελεί αποκλειστικά τεχνικό ζήτημα.
- Η δυσκολία ανάπτυξης ενός ολοκληρωμένου, αποδοτικού και αποτελεσματικού σχεδίου ασφάλειας ΠΣ.
- Ο προσδιορισμός και η αποτίμηση των οργανωσιακών επιπτώσεων από την εφαρμογή ενός σχεδίου ασφάλειας ΠΣ.

Η δυσκολία να αιτιολογηθεί το κόστος των μέτρων ασφάλειας και ιδιαίτερα εκείνων που είναι διοικητικού και διαδικαστικού χαρακτήρα, πηγάζει από την ίδια τη φύση της ασφάλειας. Η ανάγκη για ένα μέτρο προστασίας μπορεί να αποδειχθεί μόνο "μετά την καταστροφή", ενώ δεν υπάρχει τρόπος να αποδειχθεί ότι τα ήδη εγκατεστημένα μέτρα αρκούν να αντιμετωπίσουν μία ενδεχόμενη νέα απειλή.

Η αδυναμία αιτιολόγησης των μέτρων ασφάλειας με χρηματοοικονομικούς όρους αποτελεί έναν από τους βασικούς παράγοντες που δυσχεραίνουν την επικοινωνία των ειδικών της πληροφορικής με τα διοικητικά στελέχη, με άμεση συνέπεια την αδυναμία εξασφάλισης της διαρκούς υποστήριξης της ανώτερης διοίκησης. Το εγχείρημα γίνεται ακόμη δυσκολότερο όταν προτείνονται μέτρα προστασίας με διοικητικό και οργανωτικό χαρακτήρα. Η διοίκηση, αλλά και οι χρήστες, ανησυχούν για τις επιπτώσεις αυτών των μέτρων, ειδικά όταν αμφισβητείται η διαδεδομένη αντίληψη ότι το ζήτημα της ασφάλειας είναι αποκλειστικά ένα 'τεχνικό ζήτημα'.

Επιπλέον, η προστασία ενός πληροφοριακού συστήματος απαιτεί μία ολοκληρωμένη μελέτη που θα απαντά σε ερωτήματα όπως:

- ✓ Ποια στοιχεία του ΠΣ θέλουμε να προστατέψουμε; Ποια από αυτά είναι πιο σημαντικά;
- ✓ Ποιες απειλές αντιμετωπίζει το ΠΣ;
- ✓ Ποια είναι τα αδύνατα σημεία του;
- ✓ Ποια μέτρα προστασίας θα πρέπει να ληφθούν;
- ✓ Αν δοθεί απάντηση σε αυτά τα ερωτήματα, τότε θα έχουμε αποκτήσει μία άποψη για την τρέχουσα κατάσταση του ΠΣ.

Καθώς, όμως, τα ΠΣ και οι απειλές που αντιμετωπίζουν είναι δυναμικά, απαιτείται επιπλέον η συνεχής παρακολούθηση και διαχείριση της ασφάλειας του ΠΣ.

Η πλέον διαδεδομένη μεθοδολογία, η οποία στοχεύει στην αντιμετώπιση των παραπάνω ζητημάτων, είναι η μεθοδολογία της *ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ*. Η μεθοδολογία αυτή υιοθετεί την έννοια της επικινδυνότητας (risk), η οποία προέρχεται από το χώρο της χρηματοοικονομικής διοίκησης, υποκαθιστώντας το στόχο της επίτευξης της ασφάλειας με τον εφικτό και μετρήσιμο στόχο του περιορισμού της επικινδυνότητας, που ενέχεται στη λειτουργία ενός ΠΣ, εντός αποδεκτών ορίων.

2.2 Πλεονεκτήματα και μειονεκτήματα ανάλυσης και διαχείρισης επικινδυνότητας

Στα πλεονεκτήματα της ανάλυσης και διαχείρισης επικινδυνότητας περιλαμβάνονται τα παρακάτω:

- Δίνει τη δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων.
- Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των ΠΣ και τη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως «επένδυση» που αποτιμάται με όρους κόστους/οφέλους.
- Είναι αρκετά ευέλικτη, ώστε να μπορεί να ενταχθεί σε διάφορα επιστημολογικά πλαίσια και να εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες.
- Καλύπτει τις απαιτήσεις της ευρωπαϊκής και ελληνικής νομοθεσίας, που απαιτούν από τα ΠΣ, τα οποία επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε «να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων» (Νόμος 2472/1997, άρθρο 10, παρ. 3).
- Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος. Αποτελεί, δηλαδή, ένα μέσο καταγραφής και ανάλυσης του πληροφοριακού συστήματος.
- Αποτελεί την πλέον διαδεδομένη μεθοδολογία σχεδιασμού και διαχείρισης της ασφάλειας ΠΣ και έχει εφαρμοστεί με επιτυχία σε ένα μεγάλο πλήθος περιπτώσεων.

Παράλληλα όμως, η μεθοδολογία αυτή παρουσιάζει σημαντικά μειονεκτήματα, όπως τα παρακάτω:

- Στηρίζεται σε ένα απλοϊκό μοντέλο του ΠΣ και αγνοεί τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις του οργανισμού στον οποίο ανήκει το ΠΣ.
- Εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών (assets), όσο και στην αποτίμηση απειλών (threats) και ευπάθειας (vulnerability). Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων στα οποία στηρίζεται, τη συστηματικότητα των περισσότερων μεθόδων ανάλυσης επικινδυνότητας και την ‘αντικειμενικότητα’ των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.

- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής. Η εγκυρότητα της εφαρμογής των μεθόδων αυτών στον τομέα της ασφάλειας πληροφοριακών συστημάτων έχει αμφισβητηθεί από πολλούς ερευνητές.

2.3 Εννοιολογικό πλαίσιο της παρούσας μελέτης

Η εργασία στηρίζεται σ' ένα εννοιολογικό πλαίσιο που αφορά στην ασφάλεια των πληροφοριακών συστημάτων. Παρατίθεται πίνακας (*Πίνακας 1*) με τις βασικότερες έννοιες που εμφανίζονται στο παραδοτέο.

ΕΝΝΟΙΑ	ΟΡΙΣΜΟΣ
Πληροφοριακό Σύστημα (Information System, IS)	Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.
Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.
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.
Απειλή (Threat)	Μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος.
Σημείο Ευπάθειας - Αδυναμία (Vulnerability)	Σημείο ενός Πληροφοριακού Συστήματος που μπορεί να επιτρέψει να συμβεί μία παραβίαση.
Επικινδυνότητα (Risk)	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.

Πίνακας 1: Πίνακας εννοιών

3 Μεθοδολογίες διαχείρισης επικινδυνότητας

3.1 Γενικά

Σήμερα υπάρχουν διαθέσιμες πολλές μεθοδολογίες διαχείρισης κινδύνων. Οι περισσότερες απ' αυτές διατίθενται και σε αυτοματοποιημένη μορφή, δηλαδή επιτρέπουν τη χρήση υπολογιστή. Η επιλογή της πιο κατάλληλης μεθόδου για το συγκεκριμένο περιβάλλον και τις ανάγκες μιας επιχείρησης ή οργανισμού είναι πολύ σημαντική αλλά και καθόλου εύκολη. Οι παράγοντες που δυσκολεύουν μια τέτοια επιλογή είναι οι εξής:

- Δεν υπάρχει διαθέσιμος πλήρης κατάλογος όλων των διαθέσιμων μεθοδολογιών, με τα ιδιαίτερα χαρακτηριστικά τους.
- Δεν υπάρχει κοινά αποδεκτό σύνολο κριτηρίων αξιολόγησης για τις μεθοδολογίες.
- Κάποιες μεθοδολογίες καλύπτουν τμήματα μόνο της όλης διαδικασίας διαχείρισης κινδύνων. Για παράδειγμα, μερικές μεθοδολογίες αναφέρονται μόνο στον υπολογισμό του βαθμού κινδύνου και καθόλου στην επιλογή των κατάλληλων μέτρων προστασίας. Άλλες επικεντρώνονται σε κάποιο μόνο μικρό τμήμα της όλης διαδικασίας, όπως, π.χ., στο σχεδιασμό διαδικασιών ανάκαμψης μετά από καταστροφή. Κάποιες μέθοδοι ασχολούνται μόνο με τον έλεγχο των μέτρων προστασίας και όχι με τον υπολογισμό του βαθμού ευπάθειας κ.ο.κ.
- Οι μεθοδολογίες διαφέρουν πολύ στο επίπεδο ανάλυσης που χρησιμοποιούν. Κάποιες χρησιμοποιούν υψηλού επιπέδου περιγραφές του πληροφοριακού συστήματος που μελετούν, ενώ κάποιες άλλες απαιτούν λεπτομερειακές περιγραφές.
- Κάποιες μέθοδοι δε διατίθενται στην ελεύθερη αγορά, γεγονός που κάνει την αξιολόγησή τους πολύ δύσκολη, αν όχι αδύνατη.

Μία μεθοδολογία δίνει το πλαίσιο εντός του οποίου αναπτύσσονται και εφαρμόζονται μία ή περισσότερες μέθοδοι. Με άλλα λόγια, μέθοδος είναι ένας κανονικός και συστηματικός τρόπος για να εκτελεστεί ένα έργο. Έτσι, ένα μεγάλο πλήθος, περισσότερες από εκατό, μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ έχουν αναπτυχθεί, πολλές από τις οποίες υποστηρίζονται από εργαλεία λογισμικού (software tools). Στις παραγράφους που ακολουθούν περιγράφονται οι περισσότερες, εκ των υπαρχόντων, μέθοδοι και αναλύονται εκτενέστερα οι δημοφιλέστερες.

3.2 EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Η EBIOS αναπτύχθηκε το 1995 από την DCSSI (Direction Centrale de la Sécurité des Systèmes d' Information) της Γαλλικής κυβέρνησης. Η συγκεκριμένη μέθοδος λαμβάνει υπόψη τόσο τεχνικές όσο και μη τεχνικές οντότητες. Επιτρέπει σε όλο το προσωπικό που χρησιμοποιεί το ΠΣ να εμπλακεί στα θέματα ασφάλειας και προσφέρει μια δυναμική προσέγγιση που ενθαρρύνει τη διάδραση ανάμεσα στις διάφορες λειτουργίες του οργανισμού, εξετάζοντας το συνολικό κύκλο ζωής του συστήματος.

Αποτελείται από πέντε φάσεις. Η φάση 1 καθορίζει το περιεχόμενο, με όρους εξάρτησης της ολικής επιχειρησιακής διαδικασίας από το ΠΣ. Στις φάσεις 2 και 3 πραγματοποιούνται η ανάλυση απαιτήσεων ασφάλειας και η ανάλυση απειλών. Οι φάσεις 4 και 5 παράγουν αντικειμενικές διαγνώσεις της επικινδυνότητας. Στη συνέχεια, διατυπώνονται οι αναγκαίοι και ικανοί στόχοι ασφάλειας, παρέχεται η απόδειξη κάλυψής τους και εκφράζονται ρητά οι απομένουσες επικινδυνότητες.

- Η EBIOS υποστηρίζεται από ένα εργαλείο software, που έχει αναπτυχθεί από την Γαλλική *Central Information Systems Security Division.*
- Η EBIOS είναι συμβατή *με τα πρότυπα* ISO/IEC 27001, ISO/IEC 13335 (GMITS), ISO/IEC 15408 (Common Criteria), ISO/IEC 17799 και ISO/IEC 21827. *(Κάτσικας Σ., [6])*

3.3 IT-Grundschutz

Είναι μέθοδος με την οποία μια επιχείρηση μπορεί να καθιερώσει ένα σύστημα διαχείρισης ασφάλειας (ISMS). Ανακοινώθηκε το 1994. Περιέχει και γενικές συστάσεις για την δημιουργία μιας εφαρμόσιμης διαδικασίας ασφάλειας και λεπτομερείς τεχνικές οδηγίες για την επίτευξη του απαραίτητου επιπέδου ασφάλειας σε συγκεκριμένα πεδία. Η διαδικασία ασφάλειας που προβλέπει η IT-Grundschutz αποτελείται από τα εξής βήματα: αρχικοποίηση της διαδικασίας, καθορισμός στόχων ασφάλειας και επιχειρησιακού περιβάλλοντος, καθιέρωση οργανωτικής δομής για την ασφάλεια, παροχή των απαραίτητων πόρων, δημιουργία της έννοιας της ασφάλειας, ανάλυση της πληροφοριακής υποδομής, αποτίμηση απαιτήσεων προστασίας, μοντελοποίηση, έλεγχος ασφάλειας, συμπληρωματική ανάλυση ασφάλειας, σχεδιασμός υλοποίησης και υλοποίηση, συντήρηση, παρακολούθηση και βελτίωση της διαδικασίας και πιστοποίηση (προαιρετικά). Η IT-Grundschutz υποστηρίζεται από το εργαλείο *Gstool* που αναπτύχθηκε από το *Federal Office for Information Security (BSI).* Τέλος είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001. *(Κάτσικας Σ., [6])*

3.4 MARION

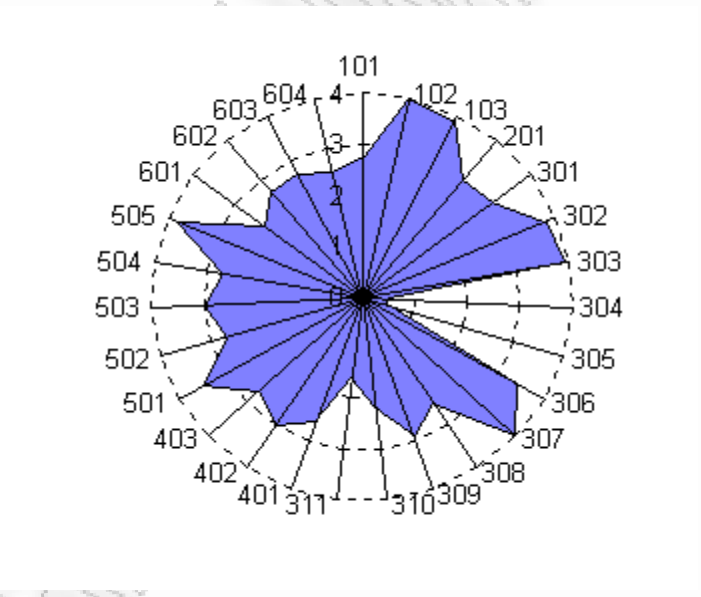
Η μέθοδος MARION αναπτύχθηκε στη Γαλλία από τον οργανισμό CLUSIF (Club dela Sécurité des Systèmes d'Information Français) το 1987. Η τελευταία έκδοσή της (1998) περιλαμβάνει τέσσερις φάσεις.

3.4.1 Φάση 0: Προετοιμασία

Σε αυτήν τη φάση καθορίζονται οι στόχοι και οριοθετείται η ανάλυση. Επίσης, διαμορφώνονται οι ομάδες εργασίας και γίνεται ο προγραμματισμός των εργασιών.

3.4.2 Φάση 1: Επιθεώρηση των αδυναμιών του συστήματος

Με τη βοήθεια ερωτηματολογίων εντοπίζονται και αξιολογούνται τα σημεία ευπάθειας (αδυναμίες) του συστήματος. Τα αποτελέσματα της ανάλυσης απεικονίζονται σε μία "ροζέτα" όπως αυτή του Σχήματος 2. Η ροζέτα παρουσιάζει 27 δείκτες ευπάθειας σε έναν κύκλο και απεικονίζει το βαθμό ευπάθειας για κάθε ένα δείκτη. Το διάγραμμα αυτό βοηθά, ώστε να έχουμε μία συνοπτική και περιεκτική εικόνα της κατάστασης του συστήματος, εντοπίζοντας άμεσα τους τομείς που απαιτούν μεγαλύτερη προστασία.



Εικόνα 1: Η «ροζέτα» της MARION

3.4.3 Φάση 2: Ανάλυση κινδύνων

Σε αυτή τη φάση γίνεται επεξεργασία των δεδομένων που προέκυψαν από τις προηγούμενες φάσεις και κατηγοριοποιούνται οι κίνδυνοι σε Μείζονες Κινδύνους (Major Risks) και Απλούς Κινδύνους (Simple Risks). Έπειτα, το πληροφοριακό σύστημα χωρίζεται σε τομείς λειτουργικότητας και ο κάθε τομέας αναλύεται χωριστά. Στην ανάλυση λαμβάνονται υπόψη 17 διαφορετικοί τύποι απειλών, όπως ατυχήματα, σφάλματα υλικού και λογισμικού, κακόβουλες ενέργειες κ.λπ.

3.4.4 Φάση 3: Σχέδιο δράσης

Στην τελευταία φάση επιλέγονται τα μέτρα προστασίας με βάση την αποτελεσματικότητα και το κόστος τους. Υποστηρίζονται διάφοροι τύποι μέτρων προστασίας, όπως:

- Προληπτικά μέτρα, που έχουν στόχο τη μείωση της πιθανότητας εμφάνισης μίας απειλής.
- Περιοριστικά μέτρα, που έχουν στόχο τη μείωση των επιπτώσεων.
- Μέτρα ανίχνευσης, που έχουν στόχο την έγκαιρη ανίχνευση και αντιμετώπιση μίας απειλής.
- Μέτρα ανάκαμψης, που αφορούν στην αποκατάσταση της λειτουργίας του συστήματος, μετά την πραγματοποίηση μιας απειλής.

3.4.5 Πλεονεκτήματα και μειονεκτήματα

Για τη MARION μπορούμε να παρατηρήσουμε ότι:

- Παρά το μεγάλο χρονικό διάστημα από την τελευταία ανανέωσή της, εξακολουθεί να είναι ιδιαίτερα αποτελεσματική.
- Είναι εύκολη στην εφαρμογή, καθώς το μεγαλύτερο μέρος της ανάλυσης βασίζεται σε ερωτηματολόγια που προσφέρονται μαζί με τη μέθοδο.
- Αντιμετωπίζει με την ίδια βαρύτητα τα οργανωτικά και τεχνικά ζητήματα.
- Η ροζέτα αποτελεί μία ιδιαίτερα πετυχημένη τεχνική παρουσίασης των αποτελεσμάτων της ανάλυσης.
- Απουσιάζει μία βιβλιοθήκη μέτρων προστασίας και η αυστηρή μέθοδος επιλογής τους. *(Κοκολάκης Σ., [9])*

3.5 MEHARI (Méthode Harmonisée d' Analyse de Risques Informatiques)

Σχεδιάστηκε από ειδικούς ασφάλειας του *CLUSIF (Club de la Sécurité Informatique Français)* και αντικατέστησε τις προηγούμενες μεθόδους MARION και MELISA. Ανακοινώθηκε το 1996. Παρέχει ένα μοντέλο αποτίμησης επικινδυνότητας και αρθρωτά συστατικά και διαδικασίες. Περιέχει τύπους που διευκολύνουν την αναγνώριση και χαρακτηρισμό των απειλών και τη βέλτιστη επιλογή διορθωτικών μέτρων. Έχει λίστα σημείων ευπαθειών που πρέπει να ελεγχθούν. Είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 13335. *(Κάτσικας Σ., [6])*

3.6 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Η επιχειρησιακή ανάλυση κρίσιμων απειλών, πόρων και ευπαθειών, (The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM - OCTAVE®) είναι μία τεχνική που επιτρέπει στους οργανισμούς να εφαρμόζουν μία αυτοαξιολόγηση των συστημάτων και των αλλαγών που επέρχονται σε αυτά στην πάροδο του χρόνου. Η μέθοδος αυτή που προσαρμόζεται στις ανάγκες του κάθε οργανισμού, λαμβάνει υπόψη της τους πόρους, τις απειλές και τις ευπάθειες (οργανωσιακής αλλά και τεχνολογικής φύσεως) ώστε ο οργανισμός να αποκτήσει μία σαφή εικόνα της ασφάλειας των συστημάτων του. Με τη βοήθεια μίας παραλλαγής της μεθόδου OCTAVE, της OCTAVE-S μπορεί η ίδια τεχνική να εφαρμοστεί σε οργανισμούς μικρότερου μεγέθους. Η OCTAVE-S είναι μια παραλλαγή της μεθόδου για μικρούς (λιγότερα από 100 άτομα) οργανισμούς. Το *Octave Automated Tool* αναπτύχθηκε από το *Advanced Technology Institute (ATI)* προκειμένου να υποστηρίζει τους χρήστες της *OCTAVE*.

Στα πλαίσια της εφαρμογής τεχνικών που αφορούν σε συστήματα διακυβέρνησης γίνεται προσπάθεια να ενθαρρυνθούν οι οργανισμοί να κατακτήσουν ένα κατάλληλο επίπεδο ασφάλειας.

Ανακοινώθηκε το 1999, από το Software Engineering Institute του Carnegie-Mellon University. Η OCTAVE είναι αυτοκατευθυνόμενη, με την έννοια ότι μια μικρή ομάδα ατόμων από τις επιχειρησιακές μονάδες και τη Δ/νση Πληροφορικής εργάζονται μαζί για να ικανοποιήσουν τις ανάγκες ασφάλειας του οργανισμού. *(Κάτσικας Σ., [6])*

3.7 Callio Secura

Προϊόν της Callio Technologies που ανακοινώθηκε το 2001. Είναι multiuser Web application που στηρίζεται σε database και επιτρέπει στους χρήστες να υλοποιήσουν και να πιστοποιήσουν ένα ISMS και οδηγεί τους χρήστες στα βήματα που οδηγούν σε συμμόρφωση με το πρότυπο ISO 27001 / 17799 και πιστοποίηση κατά BS 7799-2.Επιτρέπει επίσης την εκτέλεση ελέγχων για άλλα πρότυπα, όπως τα COBIT, HIPAA και Sarbanes-Oxley.Το Callio Secura είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001. *(Κάτσικας Σ., [6])*

3.8 COBRA

Το COBRA (Consultative, Objective & Bi-functional Risk Analysis) είναι ένα εργαλείο με το οποίο μπορεί να διεξαχθεί εξολοκλήρου η ανάλυση επικινδυνότητας σε ένα πληροφοριακό σύστημα και να ελεγχθεί το επίπεδο συμβατότητας του συστήματος με το ISO/IEC 17799. Το λογισμικό, δημιουργήθηκε από την εταιρία C & A Security Systems Ltd. Είναι ένα ευέλικτο εργαλείο που είναι σχεδιασμένο για να καλύπτει ένα μεγάλο αριθμό αρχιτεκτονικών πληροφοριακών συστημάτων. Είναι Windows PC εργαλείο, βασισμένο σε ερωτηματολόγια, που χρησιμοποιεί αρχές των έμπειρων συστημάτων και ένα σύνολο βάσεων γνώσης. Περιλαμβάνει επιπλέον και τη λεγόμενη “What if” ανάλυση, κατά την οποία ελέγχονται υποθετικά σενάρια, ώστε να διαπιστωθεί δυναμικά η επίδραση που θα έχουν συγκεκριμένα αντίμετρα στους βαθμούς κινδύνου. Μπορεί να χρησιμοποιηθεί για την αναγνώριση απειλών και ευπαθειών. Μετρά το βαθμό επικινδυνότητας για κάθε περιοχή ενός συστήματος και τον συνδέει με τη πιθανή επιχειρησιακή επίπτωση. Μπορεί να προσφέρει λεπτομερείς λύσεις και συστάσεις μείωσης της επικινδυνότητας.

3.8.1 Αρχιτεκτονική του COBRA

Το COBRA, χρησιμοποιεί ως engine, την Visual FoxPro, που είναι ουσιαστικά ένα πακέτο επεξεργασίας των βάσεων γνώσης (knowledge bases). Οι βάσεις αυτές είναι ένα σύνολο από ερωτηματολόγια (questionnaire modules) και συστάσεις για τη βελτίωση της ασφάλειας του συστήματος, το καθένα από τα οποία έχει ένα συγκεκριμένο θέμα, που πιθανώς (ανάλογα με το σύστημα), αντιστοιχεί σε ένα τμήμα του πληροφοριακού συστήματος. Οι βάσεις γνώσης είναι πέντε στο σύνολό τους:

i. ISO 17799
ii. E-Structure
iii. IT Security
iv. Operational Risk

v. High Level Risk

Η πρώτη βάση περιέχει τις συστάσεις του προτύπου ISO 17799 και χρησιμεύει στον έλεγχο της συμβατότητας του συστήματος με το πρότυπο. Οι επόμενες τρεις, περιλαμβάνουν ερωτηματολόγια για τη διεξαγωγή μιας λεπτομερούς ανάλυσης επικινδυνότητας σε ένα πληροφοριακό σύστημα, οι οποίες έχουν και κοινά σημεία, αλλά και αλληλοσυμπληρώνονται. Οι αναφορές που παράγει το COBRA μπορούν να αποθηκευθούν σε όλους τους γνωστούς τύπους αρχείων κειμένου. Μάλιστα υπάρχει η δυνατότητα αναφορών που αναφέρονται είτε σε τεχνικό προσωπικό (άρα με γνώσεις σε τεχνικούς όρους) είστε στη διοίκηση του οργανισμού. *(Πολέμη Δ., [3])*

3.9 CounterMeasures

Προϊόν της Allion για διαχείριση επικινδυνότητας βασισμένο στις σειρές αμερικανικών προτύπων US-NIST 800 και OMB Circular A-130. Ο χρήστης προτυποποιεί τα κριτήρια αξιολόγησης και, χρησιμοποιώντας μια "tailor-made" λίστα ελέγχου αποτίμησης, το software παρέχει αντικειμενικά κριτήρια αξιολόγησης για να αποφασίσει για το βαθμό ασφάλειας και συμμόρφωσης με τα πρότυπα. *(Κάτσικας Σ., [6])*

3.10 Proteus

Είναι σύνολο προϊόντων της Infogov, που ανακοινώθηκε το 1999. Επιτρέπει τη διεξαγωγή ανάλυσης κενών στη συμμόρφωση με πρότυπα όπως το ISO 17799 ή τη δημιουργία και διαχείριση ενός ISMS σύμφωνα με το πρότυπο ISO 27001 (BS 7799-2). Το *Proteus Enterprise* είναι πλήρως ολοκληρωμένη Web-based εφαρμογή για διαχείριση επικινδυνότητας για μεγάλες επιχειρήσεις. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001. *(Κάτσικας Σ., [6])*

3.11 RA2 art of risk

Είναι το νέο εργαλείο της AEXIS, που αντικατέστησε το RA Software Tool και ανακοινώθηκε το 2000. Είναι σχεδιασμένο για να βοηθήσει τις επιχειρήσεις να αναπτύξουν ένα ISMS συμβατό με το πρότυπο ISO/IEC 27001:2005 (προηγουμένως BS 7799 Part 2:2002) και τον κώδικα πρακτικής ISO/IEC 27002. Το *RA2 Information Collection Device,* ένα συστατικό που διανέμεται μαζί με το εργαλείο, μπορεί να εγκατασταθεί οπουδήποτε στον οργανισμό υπάρχει ανάγκη για συλλογή πληροφορίας προς χρήση από τη διαδικασία αποτίμησης επικινδυνότητας. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001. *(Κάτσικας Σ., [6])*

3.12 RiskWatch for Information Systems & ISO 17799

Προϊόν της RiskWatch. Άλλα προϊόντα της σειράς είναι τα RiskWatch for Financial Institutions, RiskWatch for HIPAA Security, RiskWatch for Physical & Homeland Security, RiskWatch for University and School Security, και RiskWatch for NERC (Electrical North American Reliability Council) and C-TPAT-Supply Chain. Το εργαλείο διεξάγει αυτοματοποιημένη ανάλυση επικινδυνότητας και αποτίμηση ευπαθειών ΠΣ. Το εργαλείο είναι συμβατό με τα πρότυπα ISO 17799 και USNIST 800-26. *(Κάτσικας Σ., [6])*

3.13 Security by Analysis (SBA)

Η SBA (Security By Analysis) αναπτύχθηκε στη Σουηδία στις αρχές της δεκαετίας του '80. Αν και είναι ελάχιστα γνωστή εκτός της Σκανδιναβικής χερσονήσου, αποτελεί την πλέον δημοφιλή και ευρέως εφαρμοζόμενη μέθοδο ανάλυσης επικινδυνότητας στη Σουηδία. Η SBA θα πρέπει να θεωρείται λιγότερο ως αυστηρή μέθοδος και περισσότερο ως μία ανθρωποκεντρική οπτική απέναντι στο ζήτημα της ανάλυσης επικινδυνότητας.

Η SBA βασίζεται στη διαπίστωση ότι οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία του συστήματος, ανεξάρτητα από το ρόλο και τη θέση στην ιεραρχία, είναι αυτοί που έχουν τις περισσότερες πιθανότητες να εντοπίσουν τα προβλήματα ασφάλειας και να προτείνουν λύσεις. Τα είκοσι έτη επιτυχημένης εφαρμογής της μεθόδου ενισχύουν την παραπάνω θέση και καταδεικνύουν ότι η ανθρωποκεντρική ανάλυση επικινδυνότητας αποτελεί μία ρεαλιστική και αποτελεσματική προσέγγιση.

Η SBA αποτελείται στην πραγματικότητα από ένα σύνολο μεθόδων, που ακολουθούν την ίδια φιλοσοφία και λειτουργούν συμπληρωματικά. Οι κυριότερες από αυτές είναι η *SBA Check* και η *SBA Scenario*. Και οι δύο μέθοδοι υποστηρίζονται από ειδικό λογισμικό, που διευκολύνει σημαντικά την εφαρμογή τους.

3.13.1 SBA Check

Η SBA Check χρησιμοποιείται για την ταχεία αποτίμηση του επιπέδου ασφάλειας ενός πληροφοριακού συστήματος. Αποτελείται κατά βάση από μία σειρά ερωτηματολογίων, που εστιάζουν, κυρίως, στη διαχείριση της ασφάλειας του

συστήματος, έχοντας ως σημείο αναφοράς το πρότυπο ISO/IEC 17799 και ακολουθώντας το κλασικό μοντέλο του καταλόγου (checklist model). Σύμφωνα με το μοντέλο του καταλόγου η ασφάλεια ενός συστήματος ελέγχεται με βάση έναν

κατάλογο από ενδεικνυόμενες ενέργειες και μέτρα προστασίας (checklist), που βρίσκουν εφαρμογή σε ένα μεγάλο εύρος διαφορετικών συστημάτων. Η SBA Check είναι ιδιαίτερα εύκολη στην εφαρμογή και υποστηρίζεται από εξειδικευμένο λογισμικό.

3.13.2 SBA Scenario

Η SBA Scenario αποτελεί τον πυρήνα της SBA και χρησιμοποιείται για την ποσοτική (quantitative) ανάλυση της επικινδυνότητας ενός πληροφοριακού συστήματος. Η εφαρμογή της υποστηρίζεται από ειδικό λογισμικό, το οποίο καλύπτει όλα τα στάδια της μεθόδου, εκτός από τη δημιουργική φάση της επινόησης πιθανών σεναρίων παραβίασης της ασφάλειας του ΠΣ. Ανάλογα με το μέγεθος του πληροφοριακού συστήματος παρέχονται οι εξής τρεις επιλογές:

- *Main analysis*: Πλήρης ανάλυση με στόχο τον προσδιορισμό της πιθανότητας πραγματοποίησης ενός επεισοδίου ασφάλειας και την εκτίμηση του κόστους με αναλυτικές αριθμητικές μεθόδους.

- *Ten analysis*: Ταχεία ανάλυση με την πιθανότητα και το κόστος να προσδιορίζονται στην κλίμακα 1-10.

- *Risk window*: Συνοπτική ανάλυση βασισμένη σε μία ποιοτική κλίμακα τεσσάρων βαθμίδων.

Η SBA Scenario περιλαμβάνει τα εξής τέσσερα στάδια:

i. Προετοιμασία (Preparation).
ii. Σενάρια (Scenarios).
iii. Σύνοψη (Overview).
iv. Σχέδιο Δράσης (Action Plan).

3.13.2.1 Προετοιμασία (Στάδιο 1ο)

Στο στάδιο της προετοιμασίας συγκροτούνται οι ομάδες ανάλυσης και διδάσκεται η SBA. Βασικό στοιχείο της φιλοσοφίας της μεθόδου είναι η συμμετοχή εργαζομένων από διάφορες θέσεις και βαθμίδες. Οι ίδιοι οι εργαζόμενοι στο σύστημα είναι υπεύθυνοι για την επιτυχία του έργου της ανάλυσης επικινδυνότητας, ενώ ο ρόλος του ειδικού της ασφάλειας περιορίζεται στη διδασκαλία της μεθόδου και στο συντονισμό των εργασιών της ομάδας. Με στόχο την επίτευξη μεγαλύτερης αποτελεσματικότητας συνήθως συγκροτούνται περισσότερες από μία ομάδες.

Επίσης, ιδιαίτερη έμφαση αποδίδεται στην οργάνωση του τρόπου εργασίας της κάθε ομάδας. Σε αυτό το στάδιο ρυθμίζονται ζητήματα, όπως το χρονοδιάγραμμα του έργου, ο προσδιορισμός του αντικειμένου της ανάλυσης (σύστημα, υποσύστημα κ.λπ.), ο καθορισμός της έκτασης (οριοθέτηση) της ανάλυσης, ο καθορισμός του ρόλου που θα αναλάβει το κάθε μέλος της ομάδας, η διαμόρφωση κοινής αντίληψης για το σκοπό του έργου κ.λπ.

3.13.2.2 Σενάριο (Στάδιο 2ο)

Στο δεύτερο στάδιο εντοπίζονται, καταγράφονται και αναλύονται τα πιθανά σενάρια επεισοδίων ασφάλειας (events). Πρόκειται για τη δημιουργική φάση της μεθόδου, όπου το κάθε μέλος της ομάδας εργασίας θα πρέπει να αναλάβει πρωτοβουλία και να προτείνει σενάρια, τα οποία θα αξιολογηθούν και θα αναλυθούν με τη βοήθεια των υπολοίπων μελών της ομάδας. Ακολούθως, για κάθε ένα σενάριο διεξάγεται ανάλυση επικινδυνότητας και διαχείριση επικινδυνότητας.

Ανάλυση επικινδυνότητας

Αρχικά, το κάθε σενάριο περιγράφεται αναλυτικά και καταγράφονται όλα τα διαθέσιμα στοιχεία που αφορούν το σενάριο, όπως τα γεγονότα που δύναται να οδηγήσουν στην πραγματοποίηση του σεναρίου κ.λπ. Επίσης, εκτιμάται η πιθανότητα το σενάριο να γίνει πραγματικότητα.

Ακολούθως οι πιθανές συνέπειες από την πραγματοποίηση του σεναρίου προσδιορίζονται και αναλύονται, ώστε να εκτιμηθεί η σοβαρότητά τους και να προσδιοριστεί ποσοτικά το κόστος που αναμένεται να προκύψει.

Διαχείριση επικινδυνότητας

Η διαχείριση της επικινδυνότητας γίνεται σε δύο φάσεις. Αρχικά, προσδιορίζονται οι αδυναμίες του συστήματος που συνδέονται με το σενάριο και δύναται να επιτρέψουν την πραγματοποίησή του. Στη δεύτερη φάση επιλέγονται συγκεκριμένα μέτρα προστασίας. Η αποτελεσματικότητα του κάθε μέτρου αξιολογείται και αντιπαραβάλλεται με το κόστος υλοποίησης.

3.13.2.3 Σύνοψη (Στάδιο 3ο)

Στόχος αυτού του σταδίου είναι ο προσδιορισμός των προτεραιοτήτων υλοποίησης των μέτρων προστασίας. Οι προτεραιότητες καθορίζονται με βάση του εξής δύο παράγοντες:

- το κόστος που ενδέχεται να προκύψει από τη ζημία που θα προκληθεί, εάν δεν υλοποιηθεί το προτεινόμενο μέτρο προστασίας και συμβούν τα γεγονότα που προβλέπει το σχετικό σενάριο και
- τη μείωση της επικινδυνότητας που επιτυγχάνεται με την υλοποίηση του μέτρου προστασίας.

3.13.2.4 Σχέδιο δράσης (Στάδιο 4ο)

Στο τελευταίο στάδιο καταρτίζεται ένα συνολικό σχέδιο δράσης για την ασφάλεια του πληροφοριακού συστήματος και καθορίζονται οι υπεύθυνοι για την υλοποίηση των μέτρων προστασίας.

3.13.2.5 Πλεονεκτήματα και μειονεκτήματα

Η SBA διακρίνεται για τον ανθρωποκεντρικό και συμμετοχικό της χαρακτήρα. Δίνει ιδιαίτερη βαρύτητα στη συμμετοχή των ανθρώπων που η εργασία τους σχετίζεται με το πληροφοριακό σύστημα και ενθαρρύνει τη δημιουργικότητα και τη φαντασία τους.

Τα βασικότερα πλεονεκτήματα της μεθόδου είναι τα εξής:

- Υιοθετεί μία ολιστική προσέγγιση του ζητήματος της ασφάλειας, εξετάζοντας το πληροφοριακό σύστημα ως ενιαίο σύνολο και μελετώντας το από όλες τις πλευρές.
- Η ανάλυση γίνεται από τους ίδιους τους ανθρώπους που χρησιμοποιούν καθημερινά το σύστημα, γεγονός που ενισχύει την αποτελεσματικότητα της μεθόδου και κυρίως εξασφαλίζει σε μεγάλο βαθμό την αποδοχή και εφαρμογή του σχεδίου ασφάλειας που προκύπτει ως αποτέλεσμα της εφαρμογής της μεθόδου.
- Είναι αρκετά απλή, κατανοητή και από μη-ειδικούς και μπορεί να υλοποιηθεί με μικρό, σχετικά, κόστος.
- Υποστηρίζεται από ειδικό λογισμικό, το οποίο είναι απλό και εύχρηστο.

Τα κυριότερα μειονεκτήματα της μεθόδου είναι τα εξής:

- Στηρίζεται σε μεγάλο βαθμό στις ικανότητες, τη φαντασία και τη διάθεση για συνεισφορά των εργαζομένων.
- Προϋποθέτει την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας. Αυτός είναι, ίσως, ο κυριότερος λόγος που η εφαρμογή της μεθόδου δεν έχει επεκταθεί ιδιαίτερα εκτός των Σκανδιναβικών χωρών.

- Δεν συνοδεύεται από βιβλιοθήκες μέτρων προστασίας. Η επινόηση και ο σχεδιασμός των μέτρων προστασίας επαφίεται στις ομάδες εργασίας. *(Κοκολάκης Σ., [9])*

3.14 Information Security Forum's (ISF) Standard of Good Practice

Παρέχει ένα σύνολο αρχών και στόχων ασφάλειας υψηλού επιπέδου και συσχετιζόμενες οδηγίες καλής πρακτικής. Χωρίζεται σε πέντε τμήματα, καθένα από τα οποία καλύπτει έναν τύπο περιβαλλόντων: Διαχείριση ασφάλειας, κρίσιμες επιχειρησιακές εφαρμογές, υπολογιστικές εγκαταστάσεις, δίκτυα, ανάπτυξη συστημάτων.

Η **FIRM** (Fundamental Information Risk Management) είναι μια λεπτομερής μέθοδος για την παρακολούθηση και τον έλεγχο της επικινδυνότητας στο επίπεδο της επιχείρησης. Η **Information Risk Scorecard** είναι τμήμα της FIRM. Η Scorecard είναι μια φόρμα συλλογής σημαντικών λεπτομερειών για ένα πληροφοριακό πόρο. Η ISF's Information Security Status Survey είναι ένα εργαλείο διαχείρισης επικινδυνότητας που αξιολογεί αντίμετρα. Η SARA (Simple to Apply Risk Analysis) είναι μέθοδος ανάλυσης επικινδυνότητας για κρίσιμα ΠΣ. Η SPRINT (Simplified Process for Risk Identification) είναι μια σχετικά γρήγορη και εύχρηστη μέθοδος αποτίμησης επιχειρηματικών επιπτώσεων και ανάλυσης επικινδυνότητας για σημαντικά αλλά όχι κρίσιμα ΠΣ. Είναι συμβατή με το πρότυπο ISO/IEC 17799. *(Κάτσικας Σ., [6])*

4 Η μέθοδος CRAMM

4.1 Γενικά

Για την Ανάλυση Επικινδυνότητας του ΟΠΣ χρησιμοποιήθηκε η πρότυπη *(standard)* μέθοδος CRAMM *(CCTA Risk Analysis and Management Methodology)*. Η CRAMM αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών *(Central Computer and Telecommunications Agency)* του Ηνωμένου Βασιλείου το 1987 και αποτελεί πρότυπο για τους οργανισμούς του ευρύτερου δημόσιου τομέα στη χώρα αυτή. Συγκεκριμένα, χρησιμοποιήθηκε το εργαλείο λογισμικού CRAMM v. 5.1.

Η Μέθοδος CRAMM επιλέχθηκε για τους εξής λόγους:

- Αποτελεί πρότυπη μεθοδολογία και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε πλήθος περιπτώσεων, συνεπώς είναι ώριμη μεθοδολογία.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια της εφαρμογής της, καθώς και την επιλογή αντιμέτρων.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

Το λογισμικό υποστήριξης της CRAMM υποστηρίζει το σύνολο της μεθόδου και αποτελεί αναπόσπαστο τμήμα της. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή, βήμα-προς-βήμα, εφαρμογή της μεθόδου, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της μεθόδου. Επίσης, το λογισμικό CRAMM υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας, ενώ ενσωματώνει τη βάση των αντιμέτρων και τους μηχανισμούς επιλογής των κατάλληλων αντιμέτρων.

4.2 Αναλυτική περιγραφή της CRAMM

Η μέθοδος CRAMM περιλαμβάνει τρία βασικά στάδια, όπως παρουσιάζει ο *Πίνακας 2*

- Προσδιορισμός και αξιολόγηση των αγαθών *(identification and valuation of assets)*
- Ανάλυση επικινδυνότητας *(risk analysis)*
- Διαχείριση επικινδυνότητας *(risk management)*

Στάδιο	*Βήματα σταδίου*
1. Προσδιορισμός και αξιολόγηση αγαθών	*Βήμα 1.1*: Περιγραφή Πληροφοριακών Συστημάτων και εγκαταστάσεων *Βήμα 1.2*: Αποτίμηση αγαθών Πληροφοριακού Συστήματος *Βήμα 1.3*: Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας	*Βήμα 2.1*: Προσδιορισμός απειλών που αφορούν κάθε Αγαθό *Βήμα 2.2*: Εκτίμηση απειλών και αδυναμιών *Βήμα 2.3*: Υπολογισμός επικινδυνότητας συνδυασμών *Αγαθό-Απειλή-Αδυναμία* *Βήμα 2.4*: Αποτίμηση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας	*Βήμα 3.1*: Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 3.2:* Σχέδιο Ασφάλειας Πληροφοριακού Συστήματος

Πίνακας 2: Στάδια και βήματα της μεθόδου CRAMM

4.2.1 Στάδιο 1: Προσδιορισμός και αξιολόγηση των Αγαθών

Το πρώτο στάδιο αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων του Πληροφοριακού Συστήματος που χρήζουν προστασίας. Αποτελείται από τα εξής βήματα:

- ✓ Βήμα 1.1. Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων.
- ✓ Βήμα 1.2. Αποτίμηση αγαθών πληροφοριακών συστημάτων.
- ✓ Βήμα 1.3. Επιβεβαίωση και επικύρωση της αποτίμησης.

Αναλυτικά, το κάθε επιμέρους βήμα περιλαμβάνει:

4.2.1.1 Βήμα 1.1: Περιγραφή Πληροφοριακών Συστημάτων και εγκαταστάσεων

Αναφέρεται στον προσδιορισμό των στοιχείων του Πληροφοριακού Συστήματος που απαιτούν προστασία. Τα στοιχεία αυτά είναι, κυρίως, τα δεδομένα που χειρίζεται το Πληροφοριακό Σύστημα, όπως επίσης το λογισμικό και το υλικό του Πληροφοριακού Συστήματος. 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 που αποθηκεύει και επεξεργάζεται τα δεδομένα. Επιπλέον, αναγκαία είναι και η προστασία των επικοινωνιακών μέσων που χρησιμοποιούνται για τη μεταφορά των δεδομένων. Για το λόγο αυτό, στα πλαίσια της μεθοδολογίας δημιουργείται ένα μοντέλο του συστήματος, που παρουσιάζει τις συσχετίσεις μεταξύ των στοιχείων του Πληροφοριακού Συστήματος.

4.2.1.2 Βήμα 1.2: Αποτίμηση αγαθών Πληροφοριακού Συστήματος

Κατά την αποτίμηση των στοιχείων του Πληροφοριακού Συστήματος ιδιαίτερη έμφαση δίδεται στην αποτίμηση των δεδομένων που διαχειρίζεται το Πληροφοριακό Σύστημα. Ο στόχος είναι να προσδιοριστεί η σπουδαιότητα 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)*. Ειδικότερα, εξετάζονται οι εξής περιπτώσεις:

- *Μη-διαθεσιμότητα* [Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο].
- *Καταστροφή* [Απώλεια των δεδομένων μετά τη λήψη του τελευταίου αντιγράφου ασφαλείας, Απώλεια όλων των δεδομένων μαζί με το τηρούμενο αντίγραφο].
- *Αποκάλυψη* [Αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού, Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού, Αποκάλυψη των δεδομένων σε παρόχους υπηρεσιών].
- *Μη-εξουσιοδοτημένη μεταβολή* [Μικρής έκτασης λάθη, Μεγάλης έκτασης λάθη].
- *Εκούσια μεταβολή των δεδομένων*.
- *Λάθη μετάδοσης δεδομένων* [Παρεμβολή λανθασμένων μηνυμάτων, Άρνηση αποστολής μηνύματος (*non-repudiation of origin*), Άρνηση παραλαβής μηνύματος (*non-repudiation of receipt*), Αποτυχία αποστολής μηνύματος, Επανάληψη μηνύματος (*replay*), Λανθασμένη δρομολόγηση (*misrouting*), Παρακολούθηση κίνησης (*traffic monitoring*), Απώλεια ακολουθίας μηνυμάτων (*out of sequence*)].

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. Η CRAMM παρέχει οδηγίες (*guidelines*) για την αποτίμηση των Επιπτώσεων που ανήκουν στις παρακάτω κατηγορίες:

- Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων
- Επιπτώσεις από την αποκάλυψη προσωπικών ή και ευαίσθητων προσωπικών δεδομένων
- Νομικές επιπτώσεις
- Παρεμπόδιση εφαρμογής της δικαιοσύνης και της εξιχνίασης παρανομιών

- Οικονομικές απώλειες
- Διατάραξη της δημόσιας τάξης
- Διεθνείς σχέσεις
- Άμυνα και εθνική ασφάλεια
- Εφαρμογή της πολιτικής του οργανισμού
- Απώλεια της εμπιστοσύνης του κοινού στον οργανισμό.

Ακολούθως η CRAMM μέσω του αυτοματοποιημένου εργαλείου υπολογίζει την έμμεση αξία (*implied value*) των στοιχείων των πληροφοριακών συστημάτων.

Η αποτίμηση των πληροφοριακών συστημάτων βασίζεται σε συνεντεύξεις που γίνονται με στελέχη που εμπλέκονται στην αξιοποίηση του ΟΠΣ. Στην περίπτωση της παρούσας μελέτης ασφάλειας διεξήχθησαν συνεντεύξεις με τους αναδόχους υλοποίησης του κυρίως έργου ως εκπρόσωποι των μελλοντικών χρηστών των ΟΠΣ, καθώς τελικοί χρήστες των υπηρεσιών των πληροφοριακών συστημάτων δεν υπάρχουν μέχρι τη λειτουργία του.

Το λογισμικό της CRAMM αποθηκεύει και επεξεργάζεται τα δεδομένα που συλλέγονται και πραγματοποιεί το συσχετισμό της αποτίμησης των επιμέρους στοιχείων του συστήματος με το μοντέλο του συστήματος. Έτσι, υπολογίζεται η έμμεση αξία των στοιχείων του συστήματος, υπολογισμός που δε θα μπορούσε να διεξαχθεί με εμπειρικές μεθόδους.

4.2.1.3 Βήμα 1.3: Επιβεβαίωση και επικύρωση της αποτίμησης

Η αποτίμηση των στοιχείων του Πληροφοριακού Συστήματος αποτελεί κρίσιμο παράγοντα για τη διεξαγωγή της Ανάλυσης Επικινδυνότητας. Για αυτόν το λόγο, σε αυτό το σημείο θα πρέπει η αποτίμηση να επιβεβαιωθεί από τον οργανισμό. Η ομάδα εργασίας παρουσιάζει με τη μορφή έκθεσης τα αποτελέσματα του πρώτου σταδίου σε αρμόδια στελέχη του φορέα. Τα αποτελέσματα εξετάζονται από κοινού και επικυρώνονται.

4.2.2 Στάδιο 2: Ανάλυση Επικινδυνότητας

Τα βήματα που ακολουθεί το δεύτερο στάδιο είναι:

- Βήμα 2.1. Προσδιορισμός των Απειλών που αφορούν το κάθε Αγαθό.
- Βήμα 2.2. Εκτίμηση των Απειλών και Αδυναμιών.

- Βήμα 2.3. Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία.
- Βήμα 2.4. Επιβεβαίωση και επικύρωση του Βαθμού Επικινδυνότητας.

Αναλυτικά το κάθε επιμέρους βήμα περιλαμβάνει:

4.2.2.1 Βήμα 2.1: Προσδιορισμός των απειλών που αφορούν κάθε αγαθό

Η μέθοδος δεν περιορίζεται στον προσδιορισμό των πιθανών Απειλών που καλείται να αντιμετωπίσει ένα Πληροφοριακό Σύστημα γενικά, αλλά επικεντρώνεται στον προσδιορισμό συγκεκριμένων Απειλών για κάθε Αγαθό του Πληροφοριακού Συστήματος. Η CRAMM παρέχει έναν ενδεικτικό κατάλογο Απειλών, καθώς και συστάσεις για το ποιες κατηγορίες Αγαθών ενός Πληροφοριακού Συστήματος απειλούνται συνήθως από τη συγκεκριμένη Απειλή. Το λογισμικό, έχοντας ένα πλήρες μοντέλο του Πληροφοριακού Συστήματος, έχει τη δυνατότητα να συνυπολογίσει πως όταν ένα από τα Αγαθά του Πληροφοριακού Συστήματος αντιμετωπίζει μία Απειλή, τότε και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια Απειλή. Για παράδειγμα, όταν ένας υπολογιστής αντιμετωπίζει την Απειλή της κλοπής, τότε και τα δεδομένα που αυτός έχει αποθηκευμένα θα κλαπούν μαζί του. Έτσι ο αναλυτής δε χρειάζεται να υπολογίζει ο ίδιος όλες τις συσχετίσεις και αλληλεπιδράσεις.

Το λογισμικό της CRAMM ζητά από τους αναλυτές να συσχετίσουν τα Αγαθά με κατηγορίες Απειλών από την παραπάνω κατάσταση. Το λογισμικό οδηγείται σε συμπεράσματα με βάση το μοντέλο του συστήματος. Έτσι, αν μία Απειλή (π.χ. πυρκαγιά) συσχετιστεί από τον αναλυτή με μία τοποθεσία (π.χ. υπολογιστικό κέντρο), τότε το λογισμικό συμπεραίνει ότι η Απειλή αυτή αφορά και όλο το υλικό που βρίσκεται στη συγκεκριμένη τοποθεσία (π.χ. υπολογιστικές συσκευές, περιφερειακά, δικτυακό εξοπλισμό).

4.2.2.2 Βήμα 2.2: Εκτίμηση Απειλών και Αδυναμιών

Για κάθε συνδυασμό Απειλής-Αγαθού γίνεται εκτίμηση του μεγέθους της Απειλής και της σοβαρότητας των Αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίησή της. Η εκτίμηση αυτή γίνεται με δομημένα ερωτηματολόγια. Η εκτίμηση της Απειλής γίνεται στην κλίμακα 1-5 (very low, low, medium, high, very high) αυτόματα από το εργαλείο, με βάση τις απαντήσεις που δόθηκαν στα ερωτηματολόγια. Αντίστοιχα για τις Αδυναμίες συμπληρώνονται τα ερωτηματολόγια των Αδυναμιών και υπολογίζεται η σοβαρότητα της Αδυναμίας στην κλίμακα 1-3 (low, medium, high). Οι απαντήσεις που θα δοθούν στα ερωτη-

ματολόγια 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.

4.2.2.3 Βήμα 2.3: Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία

Η CRAMM υπολογίζει το Βαθμό Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής-Αδυναμίας. Δεν έχουμε, δηλαδή, απλώς ένα Βαθμό Επικινδυνότητας για το Πληροφοριακό Σύστημα στο σύνολό του, αλλά έχουμε συγκεκριμένη αποτίμηση της επικινδυνότητας για κάθε επιμέρους συνδυασμό Αγαθού-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 Αγαθών του Πληροφοριακού Συστήματος. Ουσιαστικά ο Βαθμός Επικινδυνότητας απεικονίζει τις απαιτήσεις ασφάλειας για κάθε Αγαθό του Πληροφοριακού Συστήματος, καθώς μεγαλύτερη επικινδυνότητα συνεπάγεται και υψηλότερη απαίτηση για ασφάλεια. Ο υπολογισμός του Βαθμού Επικινδυνότητας ακολουθεί την κλίμακα 1-7. Ο Βαθμός Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής υπολογίζεται από το εργαλείο. 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 αλληλο-συσχέτισης των Αγαθών στα πλαίσια ενός Πληροφοριακού Συστήματος, κάνουν πρακτικά αδύνατο τον εμπειρικό και χειρογραφικό υπολογισμό της επικινδυνότητας.

4.2.2.4 Βήμα 2.4: Αποτίμηση βαθμού επικινδυνότητας

Ο Βαθμός Επικινδυνότητας θα χρησιμοποιηθεί στο επόμενο στάδιο για την επιλογή των Αντιμέτρων. Συνεπώς, η ορθότητα των εκτιμήσεων που έγιναν κατά τη διάρκεια του δεύτερου σταδίου θα πρέπει να ελεγχθεί πριν το επόμενο στάδιο της μεθοδο-λογίας.

4.2.3 Στάδιο 3: Διαχείριση Επικινδυνότητας

Με βάση τα αποτελέσματα της Ανάλυσης Επικινδυνότητας (Στάδιο 2), η CRAMM παράγει ένα προτεινόμενο Σχέδιο Ασφάλειας *(security plan)*. Αυτό αποτελείται από μία σειρά Αντιμέτρων - Μέτρων Ασφάλειας, τα οποία θεωρούνται απαραίτητα για

τη Διαχείριση της Επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν στο Πληροφοριακό Σύστημα.

Τα βήματα του τρίτου σταδίου περιλαμβάνουν:

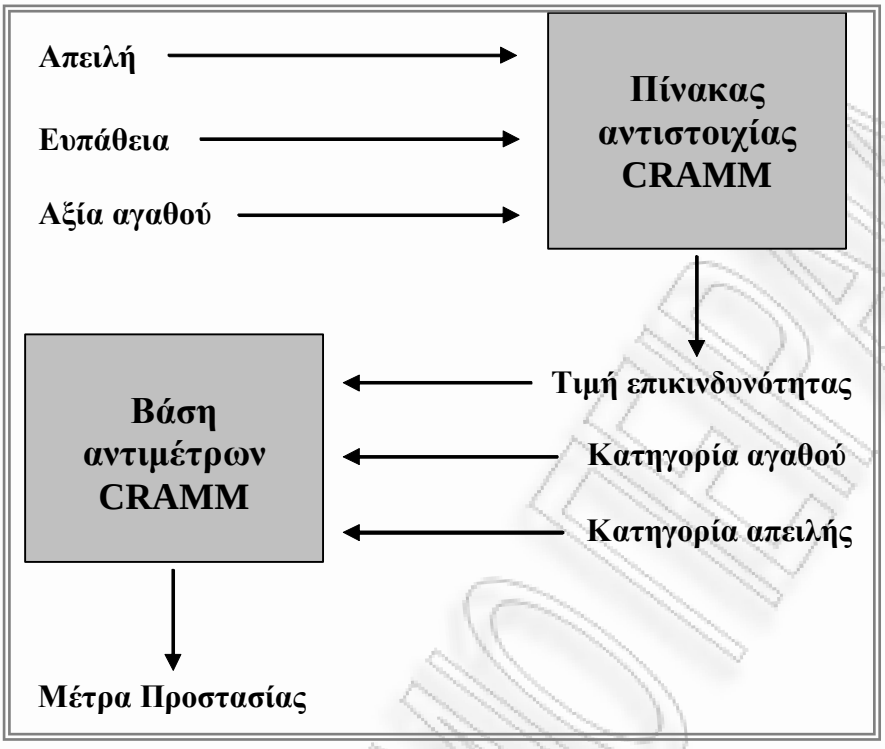
- Βήμα 3.1. Προσδιορισμός προτεινόμενων Αντιμέτρων.
- Βήμα 3.2. Σχέδιο Ασφάλειας Πληροφοριακών Συστημάτων.

Αναλυτικά το κάθε επιμέρους βήμα περιλαμβάνει:

4.2.3.1 Βήμα 3.1: Προσδιορισμός προτεινόμενων αντιμέτρων

Το λογισμικό της CRAMM διαθέτει μία βάση αντιμέτρων. Τα αντίμετρα αυτά είναι τεχνικά, διοικητικά και οργανωτικά. Το λογισμικό επιλέγει αυτόματα έναν κατάλογο προτεινόμενων αντιμέτρων, με βάση τα αποτελέσματα της Ανάλυσης Επικινδυνότητας. Τα αντίμετρα αυτά χωρίζονται σε ομάδες ανάλογα με το είδος των Απειλών που καλούνται να αντιμετωπίσουν και το είδος των Αγαθών που καλούνται να προστατέψουν. Από τον προτεινόμενο κατάλογο θα πρέπει να γίνουν συγκεκριμένες επιλογές. Η βιβλιοθήκη Αντιμέτρων περιλαμβάνει περίπου 2.500 αντίμετρα, χωρισμένα σε ομάδες και ιεραρχημένα ανάλογα με το επίπεδο ασφάλειας που προσφέρουν. Το λογισμικό επιλέγει αυτόματα τα αντίμετρα σύμφωνα με τα αποτελέσματα της Ανάλυσης Επικινδυνότητας.

Η παρακάτω εικόνα παρουσιάζει τη μέθοδο με την οποία το εργαλείο λογισμικού της CRAMM παράγει τον κατάλογο με τα προτεινόμενα μέτρα προστασίας.



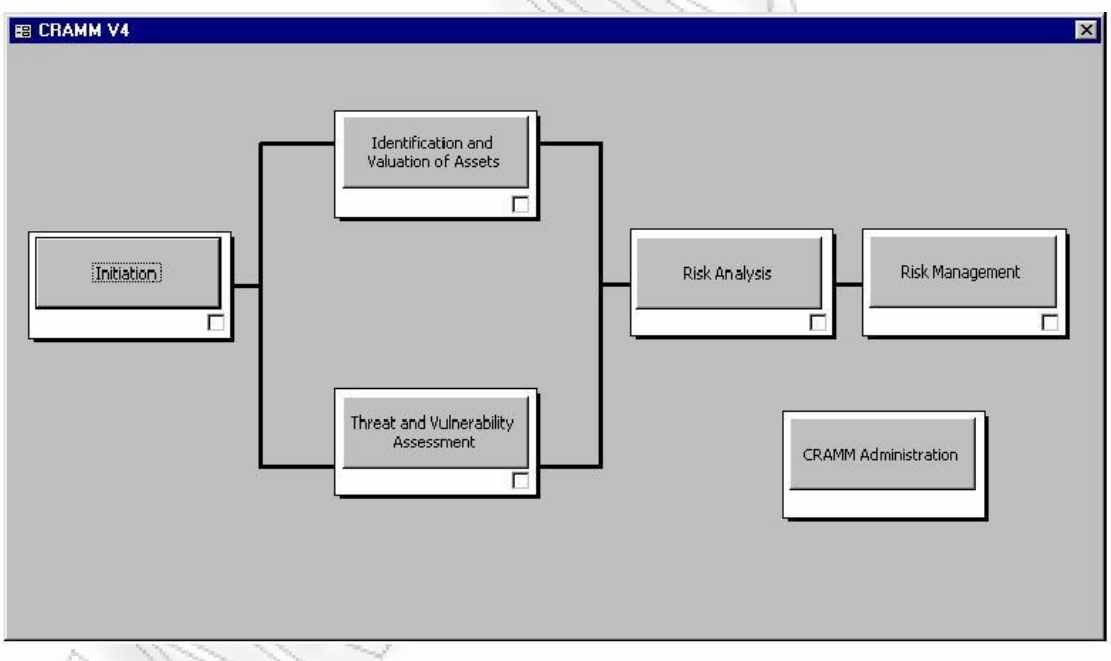
Εικόνα 2: Μέθοδος παραγωγής μέτρων προστασίας

4.2.3.2 Βήμα 3.2: Σχέδιο Ασφάλειας Πληροφοριακού Συστήματος

Κατά τη διάρκεια του συγκεκριμένου βήματος συγγράφεται το Σχέδιο Ασφάλειας που περιλαμβάνει:

- Σχέδιο Πολιτικής Ασφάλειας
- Μέτρα Ασφάλειας
- Στρατηγική για την εφαρμογή του Σχεδίου Ασφάλειας.

Σημειώνεται ότι η Πολιτική Ασφάλειας χαρακτηρίζεται ως "σχέδιο", δεδομένου ότι η υιοθέτησή της προϋποθέτει την ενδεχόμενη τελική επεξεργασία και έγκρισή της από τις αρμόδιες υπηρεσίες και ενδεχομένως και τη Διοίκηση του οργανισμού. *(Κοκολάκης Σ., [9])*



Εικόνα 3: Cramm Main screen

5 Το Πληροφοριακό Σύστημα της εταιρίας NEC Unified Solutions

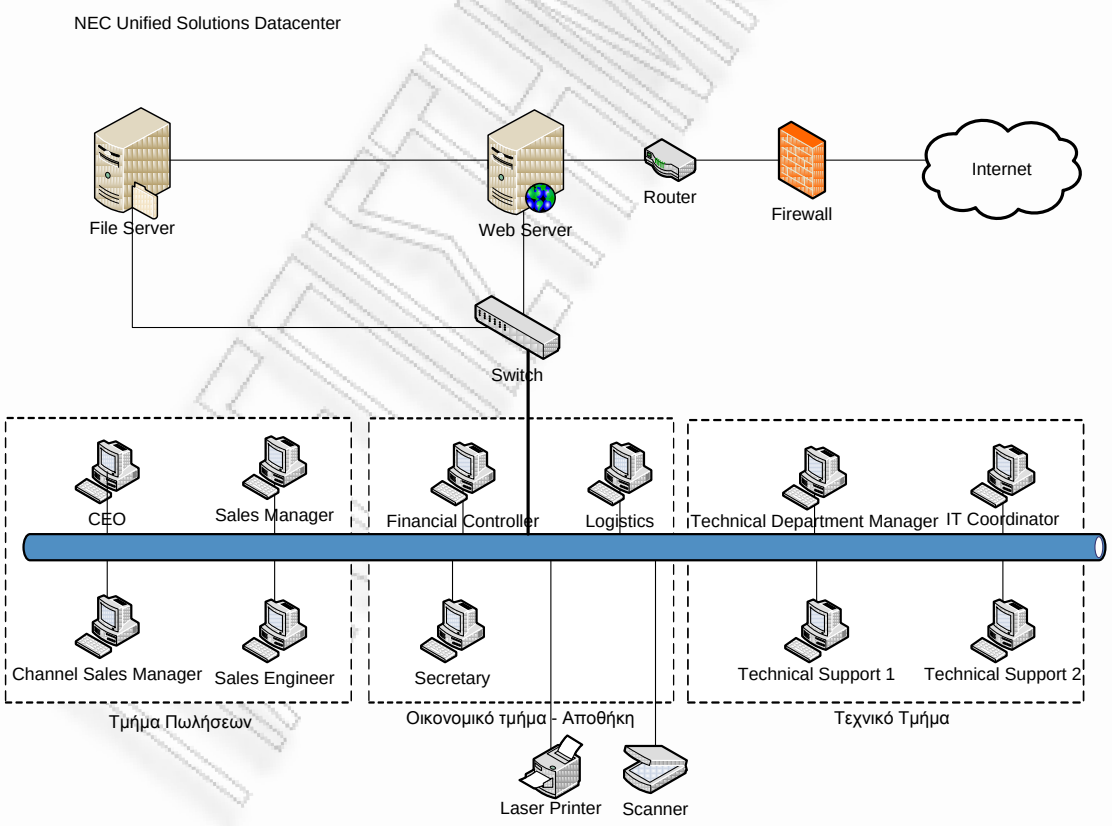
5.1 Εισαγωγή

Το πληροφοριακό σύστημα (ΠΣ) της εταιρίας NEC αποτελείται από ένα σύνολο δεδομένων, τα οποία βρίσκονται αποθηκευμένα στο υλικό (hardware) και διαχειρίζονται από το λογισμικό που είναι εγκατεστημένο. Το σύνολο αυτών των τριών αποτελεί το ΠΣ της εταιρίας και πάνω σ' αυτό θα στηριχθεί όλη η μελέτη.

5.2 Αρχιτεκτονική δικτύου ΠΣ

Η αρχιτεκτονική δικτύου του ΠΣ αφορά το hardware (υλικό), software (λογισμικό), τα δεδομένα και το προσωπικό (users) που απαρτίζουν το σύνολο της εταιρίας.

Ακολουθεί η γραφική απεικόνιση του εταιρικού δικτύου αποτελούμενο από ένα Fileserver, ένα Web Server, τα απαραίτητα switches και routers, τους τερματικούς χρήστες (Clients) καθώς και τις διάφορες περιφερειακές συσκευές.



Εικόνα 4: Nec Unified Solutions Datacenter

Το Hardware του δικτύου περιλαμβάνει τα εξής:

- Ένα File Server στον οποίο αποθηκεύονται τα δεδομένα της εταιρίας όπως επίσης και το καθημερινό backup σε ξεχωριστό σκληρό δίσκο
- Ένα Web Server απαραίτητο για την πρόσβαση του δικτύου στο internet (λειτουργεί στον ίδιο υπολογιστή)
- Router και Switch για τη δικτύωση των επιμέρους μηχανημάτων
- Έντεκα τερματικούς χρήστες (Clients)
- Περιφερειακός εξοπλισμός (Printer, Scanner)

5.3 Δεδομένα ΠΣ

Τα δεδομένα είναι ένα σύνολο αριθμών, λέξεων, συμβόλων, γεγονότων, που περιγράφουν ή αντιπροσωπεύουν ποσότητες, έννοιες, αντικείμενα, καταστάσεις και λειτουργίες. Στην πληροφορική συναντούμε τα δεδομένα στον πληθυντικό αριθμό, σπανιότερα στον ενικό (δεδομένο).

Τα δεδομένα περιγράφουν μόνο μέρος ενός συμβάντος, δεν περιλαμβάνουν καμία ανάλυση, κριτική ή αξιόπιστη βάση για περαιτέρω ενέργεια. Τα δεδομένα δεν αναφέρουν τίποτα για τη σημαντικότητά τους ή τη σχέση τους προς οτιδήποτε. Σε αντίθεση με τα δεδομένα η πληροφορία έχει ορισμένο νόημα και είναι οργανωμένη για συγκεκριμένο σκοπό. Με βάση τις συνέπειες που θα μπορούσαν να προκύψουν από την απώλεια των δεδομένων, εκτιμάται η αξία τους. Η απώλεια των δεδομένων αφορά:

- ✓ Τη διαθεσιμότητά τους
- ✓ Την εμπιστευτικότητα τους
- ✓ Την ακεραιότητά τους

Η κατηγοριοποίηση των δεδομένων με βάση τη νομική τους υπόσταση έχει ως εξής:

- ✓ Μη – προσωπικά δεδομένα
- ✓ Προσωπικά δεδομένα
- ✓ Ευαίσθητα προσωπικά δεδομένα

5.3.1 Δεδομένα εταιρίας

Τα δεδομένα που υπάρχουν στη βάση της εταιρίας NEC ομαδοποιούνται σε κάποιες κύριες κατηγορίες ομάδων που φαίνονται παρακάτω:

Κατηγορία Δεδομένων	Είδος Δεδομένων
Προσωπικά στοιχεία υπαλλήλων	Προσωπικά δεδομένα
Εργασιακά στοιχεία υπαλλήλων	Ευαίσθητα προσωπικά δεδομένα
Έσοδα – Έξοδα	Μη – προσωπικά δεδομένα
Πελάτες	Μη – προσωπικά δεδομένα
Συμβάσεις έργων - Προμηθευτές - Μεταπωλητές	Μη – προσωπικά δεδομένα
Προσωπικά αρχεία υπαλλήλων (live backup)	Προσωπικά δεδομένα
Πρωτόκολλο	Μη – προσωπικά δεδομένα

Πίνακας 3: Δεδομένα εταιρίας

5.3.1.1 *Προσωπικά στοιχεία υπαλλήλων - Προσωπικά δεδομένα*

Στην καρτέλα του κάθε υπαλλήλου περιλαμβάνονται δεδομένα που ανήκουν στην κατηγορία των προσωπικών δεδομένων όπως:

- ✓ Επίθετο, όνομα, ημερομηνία γέννησης
- ✓ Οικογενειακή κατάσταση
- ✓ Διεύθυνση κατοικίας
- ✓ Αριθμός μητρώου υπαλλήλου
- ✓ Εκπαίδευση - Πτυχία

5.3.1.2 *Εργασιακά στοιχεία υπαλλήλων - Ευαίσθητα προσωπικά δεδομένα*

Υπάρχει αναλυτική κατάσταση του μισθού κάθε υπαλλήλου με στοιχεία για τις εισφορές του ΙΚΑ, το φόρο μισθωτού υπαλλήλου και την επιπρόσθετη ασφάλιση που παρέχει η εταιρία στους υπαλλήλους της. Υπάρχει βάση δεδομένων με τις αυξήσεις που έχουν δοθεί, όπως και με τα Bonus που δικαιούται ο κάθε υπάλληλος καθώς και ο λογαριασμός μισθοδοσίας της τράπεζας. Περιέχει τις άδειες που έχει πάρει ο κάθε υπάλληλος. Οι άδειες χωρίζονται σε κανονικές, αναρρωτικές, κύησης, φοιτητικές και άλλες μικρότερες κατηγορίες. Επίσης καταγράφονται και ιατρικά στοιχεία. Πριν την πρόσληψη κάποιου υπαλλήλου, υπάρχει υποχρεωτική εξέταση από γιατρούς διαφόρων ειδικοτήτων, προκειμένου να εξασφαλιστεί η καλή κατάσταση της υγείας του κάθε εργαζομένου. Συμπεριλαμβάνονται τα δικαιολογητικά που έχουν προσκομίσει κατά καιρούς οι υπάλληλοι, σε περιπτώσεις ασθένειας και αναρρωτικής άδειας. Τέλος υπάρχουν οι μισθοί και οι συστατικές επιστολές της προηγούμενης εργασίας.

- ✓ Μισθοί
- ✓ Καρτέλα αδειών
- ✓ Ιατρικές εξετάσεις – δικαιολογητικά αδειών
- ✓ Προϋπηρεσία
- ✓ Μισθός προηγούμενης εργασίας
- ✓ Συστατικές επιστολές από προηγούμενους εργοδότες

5.3.1.3 *Έσοδα – Έξοδα - Μη – προσωπικά δεδομένα*

Είναι καταγεγραμμένα όλα τα οικονομικά στοιχεία και οικονομικές συναλλαγές της εταιρίας ανά μήνα. Υπάρχουν στοιχεία για

- ✓ Καταθέσεις χρημάτων, εισπράξεις επιταγών από τους πελάτες για την αγορά προϊόντων

- ✓ Καταθέσεις χρημάτων, εισπράξεις επιταγών από τους πελάτες για την τεχνική υποστήριξη που δέχονται από την εταιρία
- ✓ Οφειλέτες – πελάτες
- ✓ Πάγια έξοδα όπως ενοίκιο, κοινόχρηστα, λογαριασμοί ΔΕΚΟ, έξοδα σε αναλώσιμα γραφείου
- ✓ Αγορές προϊόντων από μητρική εταιρία
- ✓ Παροχές στα στελέχη της εταιρίας όπως
  - Παροχή αυτοκινήτου
  - Παροχή κινητού τηλεφώνου
  - Πληρωμές καυσίμων – διοδίων
- ✓ Οφειλές προς τρίτους (προμηθευτές, τράπεζες κτλ)

5.3.1.4 Πελάτες - Μη – προσωπικά δεδομένα

Πλήρης λίστα πελατών εταιρίας με αναλυτικά στοιχεία όπως

- ✓ Διεύθυνση, τηλέφωνο, ηλεκτρονικό ταχυδρομείο, fax
- ✓ Βάση δεδομένων με προηγούμενες αγορές
- ✓ Εκπτώσεις ανά πελάτη

5.3.1.5 Συμβάσεις έργων - Προμηθευτές – Μεταπωλητές - Μη – προσωπικά δεδομένα

Αποτελείται από σύνολο των συμβάσεων έργου που έχει υπογράψει η εταιρία με φορείς του δημοσίου αλλά και του ιδιωτικού τομέα. Αφορά σε επαγγελματικές συμφωνίες για την αγορά, τοποθέτηση και τεχνική υποστήριξη των τηλεφωνικών κέντρων, για κάποιο χρονικό ορίζοντα που καθορίζεται από τον εκάστοτε πελάτη. Στις συμβάσεις έργων εμπεριέχονται τα εξής στοιχεία:

- ✓ Το κόστος του έργου
- ✓ Ο υπό εγκατάσταση εξοπλισμός
- ✓ Το χρονικό διάστημα για το οποίο θα ισχύει η δωρεάν τεχνική υποστήριξη
- ✓ Ο τρόπος αποπληρωμής
- ✓ Ο χρόνος αποπληρωμής

Στην ίδια κατηγορία δεδομένων περιλαμβάνεται και ολοκληρωμένη λίστα με όλους τους προμηθευτές και μεταπωλητές της εταιρίας. Η εταιρία προμηθεύεται με προϊόντα από τρίτους προκειμένου να τα προωθήσει στους πελάτες της, επομένως οφείλει να έχει τα στοιχεία όλων των προμηθευτών. Επίσης γίνεται προώθηση των δικών της προϊόντων σε εξουσιοδοτημένους μεταπωλητές.

5.3.1.6 Προσωπικά αρχεία υπαλλήλων - Προσωπικά δεδομένα

Τα αρχεία του κάθε υπαλλήλου της εταιρίας αποθηκεύονται αυτόματα στον κεντρικό File Server κάθε φορά που αυτοί κάνουν αποσύνδεση (log off) από το σταθμό εργασία τους. Ελαχιστοποιείται έτσι η πιθανότητα απώλειας δεδομένων λόγω του ότι τα δεδομένα είναι αποθηκευμένα σε δύο διαφορετικά σημεία (τοπικός σκληρός δίσκος & File Server).

5.3.1.7 Πρωτόκολλο – Μη - προσωπικά δεδομένα

Τηρείται πρωτόκολλο με τις εισερχόμενες – εξερχόμενες παραγγελίες όπως επίσης για τις παραγγελίες που κάνει η εταιρία σε προμηθευτές της στο εσωτερικό και εξωτερικό. Καταγράφονται τα fax και οι επιστολές που δέχεται – στέλνει ο κάθε υπάλληλος. Επίσης περιέχει τις αιτήσεις των πελατών της εταιρίας προς το τεχνικό τμήμα για την επιδιόρθωση βλαβών αλλά και λοιπά αιτήματα.

5.4 Λογισμικό

Το λογισμικό αποτελείται από τα εργαλεία εκείνα που χρησιμεύουν για την ομαλή λειτουργία του server αλλά και χρησιμοποιούνται από τους υπαλλήλους της εταιρίας προκειμένου να φέρουν εις πέρας την εργασία τους.

Operating System: Λειτουργικό σύστημα

Prophix: Ενδοεταιρικό πρόγραμμα για την αποστολή παραγγελιών στο εξωτερικό (στη μητρική εταιρία)

Business Connect: Ενδοεταιρικό πρόγραμμα διαχείρισης τηλεφωνικών κλήσεων. Περιλαμβάνει και τον κεντρικό τηλεφωνικό κατάλογο της εταιρίας

Conference SW: Λογισμικό για ενδοεταιρικές συσκέψεις – διασκέψεις με ήχο και εικόνα

5.5 Υπηρεσίες

Στο πληροφοριακό σύστημα της εταιρίας λαμβάνουν χώρα και ορισμένες υπηρεσίες. Οι υπηρεσίες αυτές θα πρέπει συσχετιστούν (βάση της CRAMM) με τα δεδομένα που υπάρχουν:

Document Management Service (DMS): Υπηρεσία που αναλαμβάνει τη διαχείριση – προσπέλαση των δεδομένων της εταιρίας. Αφορά στο λειτουργικό σύστημα και στα δεδομένα: Προσωπικά Στοιχεία Υπαλλήλων, Εργασιακά Στοιχεία Υπαλλήλων, Έσοδα – Έξοδα. (Τύπος υπηρεσίας: Other End User Service)

Prophix (service): Υπηρεσία που αναλαμβάνει να διεκπεραιώσει τις εντολές μέσα στο περιβάλλον εργασίας του Prophix. Περιλαμβάνει τα δεδομένα: Προσωπικά Αρχεία Υπαλλήλων, Πρωτόκολλο, Συμβάσεις. (Τύπος υπηρεσίας: Application to Application, Ηλεκτρονικό ταχυδρομείο, Διαμοιρασμός αρχείων)

BCT (service): Υπηρεσία που αναλαμβάνει τη λειτουργικότητα του λογισμικού BCT. Συνδέεται με τα δεδομένα των πελατών. (Τύπος υπηρεσίας: Application to Application, Web browsing)

Conference SW: Υπηρεσία για τη λειτουργία των συνδιασκέψεων. (Τύπος υπηρεσίας: Voice Video)

6 Αποτίμηση του Πληροφοριακού Συστήματος της NEC Unified Solutions

6.1 Εισαγωγή

Με βάση τις ομάδες δεδομένων που αναλύθηκαν σε παραπάνω κεφάλαιο, γίνεται η αποτίμηση και καταγραφή τους στο κεφάλαιο αυτό. Η αξία των δεδομένων και όχι του υλικού ή του λογισμικού, είναι αυτή που λαμβάνει ως ιδιαίτερης βαρύτητας και σημασίας η μέθοδος CRAMM, με συνέπεια τα αποτελέσματα της αποτίμησης να έχουν άμεση σχέση μ' αυτά.

6.2 Αποτίμηση αξίας αγαθών – δεδομένων ΠΣ

Παρακάτω παρατίθενται οι πίνακες αποτίμησης αξίας δεδομένων

Οικονομική απώλεια – παρεμπόδιση λειτουργίας

ΑΠΩΛΕΙΑ	ΤΙΜΗ
<1000 ΕΥΡΩ	**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**

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**

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**

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**

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

ΣΥΝΕΠΕΙΑ	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	8
Σημαντική ζημιά στην εθνική οικονομία με μακροπρόθεσμες συνέπειες	9

Παραβίαση νομοθεσίας

ΣΥΝΕΠΕΙΑ	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 χρόνια	5
Πολλαπλές μηνύσεις <250.000 ευρώ ή ποινική δίωξη που επιφέρει ποινή φυλάκισης μέχρι 10 χρόνια	6
Πολλαπλές μηνύσεις, απεριόριστη ζημιά ή περισσότερα από 10 χρόνια φυλάκιση	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

Προσωπική ασφάλεια

ΑΠΩΛΕΙΑ	ΤΙΜΗ
Δεν ορίζεται	**1**
Μπορεί να προκαλέσει μικρό τραυματισμό σε αρκετά άτομα	**2**
Πιθανόν να προκαλέσει μικρό τραυματισμό σε ένα άτομο	**3**
Πιθανόν να προκαλέσει μικρό τραυματισμό σε αρκετά άτομα	**4**
Δεν ορίζεται	**5**
Απειλεί σωματική ακεραιότητα ενός ατόμου	**6**
Απειλεί σωματική ακεραιότητα πολλών ατόμων	**7**
Δύναται να θέσει σε κίνδυνο τη ζωή ενός ατόμου	**8**
Πιθανόν να προκαλέσει την απώλεια ανθρώπινης ζωής	**9**
Πιθανόν να προκαλέσει την απώλεια πολλών ανθρώπινων ζωών	**10**

6.3 Αποτελέσματα αποτίμησης

Στο συγκεκριμένο κομμάτι γίνεται αναλυτική αποτίμηση των επιπτώσεων που επιφέρει η παραβίαση της ασφάλειας στο σύνολο των δεδομένων που καταγράφηκαν για το ΠΣ της εταιρίας NEC. 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.

6.3.1 Προσωπικά στοιχεία υπαλλήλων NEC

Όπως έχει περιγραφεί στη παράγραφο *5.3.1* τα δεδομένα των υπαλλήλων περιέχουν προσωπικά δεδομένα.

6.3.1.1 Απώλεια διαθεσιμότητας δεδομένων των εργαζομένων της εταιρίας

Τα δεδομένα των εργαζομένων υπάρχουν για να χρησιμοποιηθούν όταν κι εφόσον εμφανιστεί μια συγκεκριμένη ανάγκη για την εταιρία. Δεν είναι δεδομένα που χρησιμοποιούνται καθημερινά για τη λειτουργία της, επομένως η απώλεια της διαθεσιμότητάς τους δε θα παρεμπόδιζε άμεσα τις καθημερινές της δραστηριότητες.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.1.2 Καταστροφή ή απώλεια των δεδομένων των εργαζομένων

Το συγκεκριμένο σενάριο αφορά στη μερική απώλεια των δεδομένων, λόγου του ότι έχει διασωθεί το τελευταίο αντίγραφο ασφαλείας. Τα δεδομένα που πλέον δεν υπάρχουν είναι όσα δεν υπάρχουν στο backup. Αυτό βέβαια προϋποθέτει πως τηρούνται οι σωστές και ακριβείς διαδικασίες για τη λήψη των εφεδρικών αντιγράφων ασφαλείας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των δεδομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.1.3 Καταστροφή (ολική) των δεδομένων των εργαζομένων

Η απώλεια όλων των δεδομένων μαζί με το τηρούμενο αντίγραφο ασφαλείας, έχει ως αποτέλεσμα την καταχώρηση των δεδομένων από την αρχή στη βάση δεδομένων της εταιρίας. Αυτό συνεπάγεται τη χρησιμοποίηση μέρους του προσωπικού σ' αυτόν τον τομέα για όσο χρονικό διάστημα χρειαστεί, αφήνοντας πίσω άλλες εργασίες της εταιρίας. Επομένως υπάρχουν χαμένες εργατοώρες άρα υφίσταται πρόβλημα οικονομικής φύσεως. Ενδεχομένως να δημιουργηθεί πρόβλημα στο χρόνο παράδοσης των δεδομένων που έχουν χαθεί σε υπηρεσίες που χρειάζονται αυτά τα στοιχεία (πχ ασφαλιστικά ταμεία).

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των δεδομένων	Βαθμός
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 10.001 – 30.000 ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.1.4 Αποκάλυψη των δεδομένων των υπαλλήλων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Η αποκάλυψη των προσωπικών στοιχείων των δεδομένων σε άτομα της εταιρίας που δεν έχουν την εξουσιοδότηση για πρόσβαση σ' αυτά δεν προκαλεί μεγάλο πρόβλημα στη λειτουργία ή τη φήμη της εταιρίας. Ενδεχόμενος όμως να

προκαλέσει τη δυσαρέσκεια των εργαζομένων των οποίων τα στοιχεία έχουν αποκαλυφθεί.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποκάλυψη προσωπικών πληροφοριών – Μικρή ενόχληση ενός ατόμου	1
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.1.5 Αποκάλυψη των δεδομένων των υπαλλήλων σε άτομα εκτός οργανισμού

Η δυσαρέσκεια των εργαζομένων στην περίπτωση που διαρρεύσουν τα στοιχεία τους σε υπηρεσίες και οργανισμούς εκτός εταιρίας θα είναι ιδιαίτερα έντονη. Η εταιρία χάνει μεγάλο μέρος της αξιοπιστίας της και κάνει τους εργαζομένους δύσπιστους απέναντί της.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης δεδομένων σε άτομα εκτός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποκάλυψη προσωπικών πληροφοριών – Παραβίαση νομοθεσίας και μεγάλη ενόχληση	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.1.6 Ακούσια μεταβολή των δεδομένων των εργαζομένων

Η μη ηθελημένη μεταβολή των δεδομένων των εργαζομένων εξαρτάται από το είδος των δεδομένων που θ' αλλοιωθούν. Για παράδειγμα η αλλοίωση της διεύθυνσης κατοικίας, δεν επιφέρει μεγάλα προβλήματα.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των δεδομένων των εργαζομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.1.7 Εκούσια μεταβολή των δεδομένων των εργαζομένων

Το συγκεκριμένο κομμάτι αφορά στην αλλοίωση στοιχείων όπως τα πτυχία των εργαζομένων. Η σκόπιμη αλλοίωσή τους προσβλέπει στην εξαπάτηση των προϊσταμένων της εταιρίας με απρόβλεπτες συνέπειες. Επίσης ο εργαζόμενος ενδέχεται να αμείβεται περισσότερο με βάση αυτό που δικαιούται εάν αλλοιωθούν τα παραπάνω στοιχεία (πχ αλλοίωση πτυχίων)

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των δεδομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.2 Εργασιακά στοιχεία υπαλλήλων

Τα εργασιακά στοιχεία των εργαζομένων καλύπτουν όλη τη γκάμα των δεδομένων που πρέπει να διατηρεί η εταιρία προκειμένου να υπάρχει μια αρμονική λειτουργία κυρίως στα οικονομικά αλλά και σε άλλα ευαίσθητα δεδομένα.

6.3.2.1 Απώλεια διαθεσιμότητας των εργασιακών δεδομένων των εργαζομένων της εταιρίας

Η μη-διαθεσιμότητα των εργασιακών δεδομένων των υπαλλήλων προκαλεί σίγουρα διαφόρων ειδών αρνητικές καταστάσεις για την εταιρία. Ο αριθμός λογαριασμού καταθέσεως της μισθοδοσία ή του μισθού των υπαλλήλων πρέπει να παραμένει διαθέσιμος κυρίως της ώρες που βγαίνει η μισθοδοσία. Η μη-διαθεσιμότητα μερικών ημερών θα δυσαρεστούσε το μεγαλύτερο μέρος των εργαζομένων.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.2.2 Καταστροφή ή απώλεια των εργασιακών δεδομένων των εργαζομένων

Η απώλεια μέρους των εργασιακών δεδομένων των υπαλλήλων δημιουργεί πρόβλημα στη λειτουργία της. Ένα μέρος των δεδομένων έχει διασωθεί λόγο του backup αλλά ίσως έχουν χαθεί κρίσιμα δεδομένα της τελευταίας στιγμής πριν από τη λήψη του αντιγράφου ασφαλείας. Ενδεχομένως να έχουν χαθεί κάποιες άδειες ή κάποια δικαιολογητικά αδειών με αποτέλεσμα η εταιρία να δώσει κάποιες επιπλέον άδειες που οι εργαζόμενοι δε δικαιούνται.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των εργασιακών δεδομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.2.3 Καταστροφή (ολική) των εργασιακών δεδομένων των υπαλλήλων

Η ολική απώλεια των εργασιακών δεδομένων δημιουργεί σοβαρά προβλήματα λειτουργίας στην εταιρία. Πρέπει να επαναπροσδιοριστούν οι μισθοί, να περάσουν εκ νέου από ιατρικές εξετάσεις οι εργαζόμενοι αλλά και να επαναπροσδιοριστούν οι μέρες άδειας του καθενός. Λάθη σ' αυτό το στάδιο μπορεί να προκαλέσουν τη νομική κίνηση των υπαλλήλων έναντι της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των εργασιακών δεδομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 30.001 – 100.000 Ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.2.4 Αποκάλυψη των εργασιακών δεδομένων των υπαλλήλων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Η αποκάλυψη του μισθού σε άτομα εντός της εταιρίας ενδεχομένως να προκαλέσει τριγμούς στις μεταξύ τους σχέσεις. Ίσως εκτεθούν άτομα που δε θα πρέπει να αποκαλυφθεί το ιατρικό τους ιστορικό.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης εργασιακών δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποκάλυψη προσωπικών πληροφοριών – Παραβίαση νομοθεσίας και μεγάλη ενόχληση	4
Παραβίαση νομοθεσίας – Αποζημίωση ή πρόστιμο <10.000 Ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.2.5 Αποκάλυψη των εργασιακών δεδομένων των υπαλλήλων σε άτομα εκτός οργανισμού

Η αποκάλυψη των εργασιακών δεδομένων σε άτομα εκτός οργανισμού θα προκαλέσει σίγουρα την έντονη δυσαρέσκεια των υπαλλήλων, οι οποίοι θα καταφύγουν στη δικαιοσύνη. Η δυσφήμηση της εταιρίας είναι δεδομένη. Επίσης

ενδέχεται να επωφεληθεί κάποιος ανταγωνιστής της εταιρίας προσφέροντας μεγαλύτερο μισθό σε κάποιον εργαζόμενο της NEC με σκοπό να τον προσλάβει.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης εργασιακών δεδομένων σε άτομα εκτός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Αποκάλυψη προσωπικών πληροφοριών – Παραβίαση νομοθεσίας και σοβαρή ενόχληση	5
Παραβίαση νομοθεσίας – Αποζημίωση ή πρόστιμο <50.000 Ευρώ ή φυλάκιση μέχρι 2 χρόνια	5
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 100.000 ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.2.6 Ακούσια μεταβολή των εργασιακών δεδομένων των εργαζομένων

Μεταβολές και λάθη στα εργασιακά δεδομένα των υπαλλήλων μπορεί να προκαλέσει προβλήματα στις πληρωμές των υπαλλήλων αλλά και στις χορηγήσεις αδειών.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των εργασιακών δεδομένων των εργαζομένων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική Απώλεια - 1.001 – 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.2.7 Εκούσια μεταβολή των εργασιακών δεδομένων των εργαζομένων

Η σκόπιμη αλλοίωση των εργασιακών δεδομένων προκαλεί σοβαρά προβλήματα στη λειτουργία της εταιρίας. Η αλλοίωση των μισθών και της αλλοίωσης της καρτέλας των αδειών δημιουργεί προβλήματα στην εύρυθμη λειτουργία της.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των δεδομένων	Βαθμός
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 10.001 – 30.000 Ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.3 Έσοδα – Έξοδα

Είναι ο πιο κρίσιμος τομέας σε μια επιχείρηση. Οι επιπτώσεις που μπορεί να έχει μια επικείμενη καταστροφή ίσως να καταστήσουν τη βιωσιμότητα της εταιρίας αδύνατη.

6.3.3.1 Απώλεια διαθεσιμότητας των εσόδων – εξόδων

Η απώλεια διαθεσιμότητας των εσόδων – εξόδων της εταιρίας ενδέχεται να προκαλέσει σύγχυση στα οικονομικά στοιχεία της εταιρίας. Για παράδειγμα η μη διαθεσιμότητά τους για κάποιο χρονικό διάστημα μπορεί να δημιουργήσει σοβαρό πρόβλημα στον ισολογισμό της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.3.2 Καταστροφή ή απώλεια των δεδομένων εσόδων – εξόδων

Στην περίπτωση που χαθεί μέρος των εσόδων – εξόδων της εταιρίας θα δημιουργηθεί σύγχυση για την πρόσφατη εικόνα των οικονομικών της εταιρίας, λόγω του ότι θα υπάρχει ένα αντίγραφο ασφαλείας διαθέσιμο για τα οικονομικά στοιχεία των προηγούμενων ημερών. Ίσως χρειαστούν εργατοώρες για τον εκ νέου υπολογισμό των εσόδων – εξόδων.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των δεδομένων εσόδων – εξόδων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.3.3 Καταστροφή (ολική) των εσόδων – εξόδων

Η ολική καταστροφή των εσόδων – εξόδων της εταιρίας, μαζί με το εφεδρικό αντίγραφο, σημαίνει πως πλέον η εταιρία δεν έχει καμία απολύτως εικόνα για τα οικονομικά της. Δεν υπάρχουν οι βάσεις δεδομένων από τις οποίες αντλούσε τα μηνιαία έσοδα και έξοδα. Το κόστος είναι τεράστιο.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των δεδομένων των εσόδων – εξόδων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Εμπορικά και οικονομικά συμφέροντα - Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 1.000.000 Ευρώ	4
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 100.001 – 300.000 Ευρώ	5
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.3.4 Αποκάλυψη εσόδων - εξόδων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Η συγκεκριμένη αποκάλυψη ενδεχομένως να δημιουργήσει κλιμάκωση μεταξύ των σχέσεων των υπαλλήλων. Αυτό θα οφείλεται στο ότι μπορεί να αποκαλυφθούν συγκεκριμένα έξοδα για κάποιους υπαλλήλους (πχ: παροχές κινητών τηλεφώνων) τα οποία ίσως να ήταν άγνωστα με εκείνη τη στιγμή. Άλλο παράδειγμα είναι να αποκαλυφθεί πως τα έσοδα της εταιρίας δεν είναι τα αναμενόμενα, το οποίο μπορεί να προκαλέσει ανασφάλεια και άρα μείωση αποδοτικότητας των εργαζομένων.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων των εσόδων – εξόδων της εταιρίας	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.3.5 Αποκάλυψη των εσόδων – εξόδων σε άτομα εκτός οργανισμού

Η αποκάλυψη των εσόδων – εξόδων της εταιρίας σε άτομα εκτός αυτής ενδεχομένως να προκαλέσει λανθασμένη εντύπωση για την οικονομική της εικόνα. Αν η εταιρία έχει μια προσωρινή κάμψη στα έσοδά της αυτό μπορεί να εκληφθεί λάθος από στελέχη εφάμιλλων εταιριών, με αποτέλεσμα να δημιουργηθεί η εντύπωση πως γενικά ο κλάδος δεν είναι αποδοτικός. Η γενικότερη ανασφάλεια θα είναι αυτή που θα επικρατήσει. Τέλος, οι πελάτες της εταιρίας ή οι εν δυνάμει πελάτες θα στραφούν σε άλλες εταιρίες προκειμένου να εξασφαλίσουν τη μελλοντική υποστήριξη ή εξυπηρέτησή τους.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων των εσόδων – εξόδων εκτός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 30.001 – 100.000 Ευρώ	4
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 1.000.000 ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.3.6 Ακούσια μεταβολή των εσόδων - εξόδων του οργανισμού

Λάθη στα δεδομένα των εσόδων – εξόδων ίσως δημιουργήσουν αλλαγές στην οικονομική πολιτική της εταιρίας. Για παράδειγμα αν καταχωρηθούν λάθος στοιχεία για κάποια έξοδα της εταιρίας, να αναγκαστεί η διοίκηση να σταματήσει κάποιες παροχές στους υπαλλήλους της (πχ: επιπρόσθετη ιατροφαρμακευτική περίθαλψη).

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των δεδομένων των εσόδων – εξόδων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Παραβίαση νομοθεσίας - Αποζημίωση ή πρόστιμο <10.000 Ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.3.7 Εκούσια μεταβολή των εξόδων – εξόδων του οργανισμού

Η κακόβουλη μεταβολή των στοιχείων των εσόδων – εξόδων της εταιρίας ενδεχομένως να γίνεται για την κάλυψη οικονομικών στοιχείων, δυσμενών για την εταιρία. Βέβαια μπορεί να γίνει και για τον ακριβώς αντίθετο λόγο, δηλαδή για την κάλυψη κάποιων εσόδων με σκοπό να ωφεληθεί αυτό που προέβη στην παράνομη αυτή μεταβολή.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση εκούσιας μεταβολής των δεδομένων των εσόδων – εξόδων	Βαθμός
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 30.0001 – 100.000 €	4
Παραβίαση νομοθεσίας - Αποζημίωση ή πρόστιμο <50.000 Ευρώ ή φυλάκιση μέχρι 2 χρόνια	5
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.4 Πελάτες

Ο κινητήριος μοχλός της εταιρίας. Τα δεδομένα των πελατών είναι αυτονόητο ότι πρέπει να είναι συγκεντρωμένα σε μια βάση δεδομένων αλλά και συνεχώς διαθέσιμα.

6.3.4.1 Απώλεια διαθεσιμότητας των δεδομένων των πελατών

Η απώλεια διαθεσιμότητας των δεδομένων της εταιρίας μπορεί να προκαλέσει προβλήματα στη λειτουργία της, αφού μπορεί να μη πραγματοποιηθεί μια παραγγελία που επείγει ή να δοθεί λανθασμένη έκπτωση.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 10.001 – 30.000 Ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 10.001 – 30.000 Ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.4.2 Καταστροφή ή απώλεια των δεδομένων των πελατών

Η απώλεια των δεδομένων των πελατών προκαλεί τη δυσλειτουργία της εταιρίας. Η εταιρία θα πρέπει να φροντίσει να ξαναβρεί τα χαμένα δεδομένα το οποίο θα κοστίσει σε χρόνο και χρήμα (τηλεφωνικές επικοινωνίες για την εκ νέου καταχώρηση των στοιχείων, απασχόληση υπαλλήλων). Επίσης μπορεί να ακυρωθεί κάποια παραγγελία η οποία έπρεπε να γίνει άμεσα.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.4.3 Καταστροφή (ολική) των δεδομένων των πελατών

Αυτή η απώλεια προκαλεί παύση των πελατειακών σχέσεων της εταιρίας και της διεκπεραίωσης παραγγελιών για όσο χρονικό διάστημα απαιτείται για την εύρεση των χαμένων δεδομένων. Οι οικονομικές απώλειες ίσως να είναι μεγάλες. Πρέπει να γίνει επαναπροσδιορισμός των επιμέρους εκπτώσεων ανά πελάτη αλλά και να ζητηθεί από τους πελάτες η αποστολή παλαιότερων τιμολογίων, προκειμένου να καταχωρηθούν οι προηγούμενες παραγγελίες τους. Υπάρχει το ενδεχόμενο δυσαρέσκειας του πελάτη, ο οποίος μπορεί να στραφεί σε άλλον προμηθευτή.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης - Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 10.001 – 30.000 Ευρώ	5
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 100.000 Ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.4.4 Αποκάλυψη των δεδομένων των πελατών σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Τα αποτελέσματα της αποκάλυψης των δεδομένων των πελατών σε άτομα εντός της εταιρίας, δε θα έχει ουσιαστικά κάποιο αντίκρισμα στην λειτουργία ή την εικόνα της εταιρίας. Επομένως τα προβλήματα θα είναι ελάχιστα

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.4.5 Αποκάλυψη των δεδομένων των πελατών σε άτομα εκτός οργανισμού

Τα δεδομένα του πελάτη περιέχουν πληροφορίες που μπορεί να φανούν πολύ χρήσιμες για τον οποιοδήποτε ανταγωνιστή της εταιρίας. Η ανταγωνιστική εταιρία, γνωρίζοντας την έκπτωση που προσφέρει η NEC στους πελάτες, μπορεί να αναδιαμορφώσει τις τιμές τις, προσφέροντας πιο ελκυστικά προϊόντα, από άποψη τιμής.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 100.000 ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.4.6 Ακούσια μεταβολή των δεδομένων των πελατών

Αλλαγές στα δεδομένα των πελατών που οφείλονται σε λάθη συνήθως προκαλούν προβλήματα στην διεκπεραίωση των παραγγελιών αλλά και παρεξηγήσεις μεταξύ της εταιρίας και του πελάτη. Μια λανθασμένη έκπτωση, μπορεί να δημιουργήσει διαφορετικές συμφωνίες στις τιμές πώλησης των προϊόντων, με αποτέλεσμα να προκληθούν εντάσεις μεταξύ των δύο πλευρών.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.4.7 Εκούσια μεταβολή των δεδομένων των πελατών

Η εκούσια μεταβολή των συγκεκριμένων δεδομένων ενδέχεται να προκαλέσει την παύση των πελατειακών σχέσεων της εταιρίας με τον εκάστοτε πελάτη. Για παράδειγμα, η εκούσια αλλαγή στην τιμή της έκπτωσης προς τον πελάτη μπορεί να δημιουργήσει ένταση μεταξύ των σχέσεων των δύο πλευρών, ικανή για την οριστική διακοπή των πελατειακών σχέσεών τους

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 30.0001 – 100.000 €	4
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 100.000 ευρώ	3
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.5 Προσωπικά αρχεία των υπαλλήλων

Τα προσωπικά αρχεία των υπαλλήλων περιέχουν την καθημερινή δουλεία τους. Η πρόοδος της εταιρίας είναι άμεσα συνδεδεμένη με την προσωπική δουλεία του κάθε εργαζομένου.

6.3.5.1 Απώλεια διαθεσιμότητας των προσωπικών αρχείων των υπαλλήλων

Η απώλεια της διαθεσιμότητας της προσωπικής δουλειάς του κάθε υπαλλήλου θα προκαλέσει την προσωρινή δυσλειτουργία της εταιρίας. Ίσως υπάρξει καθυστέρηση στην υλοποίηση κάποιων projects. Επίσης θα υπάρξει καθυστέρηση στη γενική λειτουργία της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας <1.000 Ευρώ	1
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 - 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 - 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.5.2 Καταστροφή ή απώλεια των προσωπικών αρχείων των υπαλλήλων

Η μερική απώλεια των αρχείων των υπαλλήλων θα προκαλέσει τη δυσαρέσκειά τους αλλά και θα τους αναγκάσει να τα δημιουργήσουν απ' την αρχή. Μέρος των αρχείων ενδεχομένως να υπάρχει στο προγραμματισμένο backup επομένως οι αντιδράσεις θα είναι μετριασμένες. Θα χαθούν χρόνος και χρήμα.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των προσωπικών αρχείων των υπαλλήλων	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.5.3 Καταστροφή (ολική) των προσωπικών αρχείων των υπαλλήλων

Ισοδυναμεί με καταστροφή της λειτουργίας της εταιρίας. Αρχεία που έχουν δημιουργηθεί από τους εργαζομένους, ξοδεύοντας πολλές εργατοώρες, χάνονται χωρίς να έχει παρθεί αντίγραφο ασφαλείας. Η λειτουργία της εταιρίας και η επιτυχημένη παρουσία της στην αγορά θα περάσει σίγουρα κρίση.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των προσωπικών αρχείων των υπαλλήλων	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 100.001 – 300.000 Ευρώ	5
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.5.4 Αποκάλυψη των προσωπικών αρχείων των υπαλλήλων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Η αποκάλυψη της προσωπικής δουλειάς των εργαζομένων σε άτομα της εταιρίας, θα δημιουργήσει δυσμενές κλίμα στις μεταξύ τους σχέσεις. Θα αποκαλυφθεί ο φόρτος εργασίας του καθενός αλλά και το κατά πόσο είναι συνεπείς στα projects που τους έχουν ανατεθεί.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων των προσωπικών αρχείων των υπαλλήλων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποκάλυψη προσωπικών πληροφοριών –Μεγάλη ενόχληση ενός ατόμου	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.5.5 Αποκάλυψη των προσωπικών αρχείων των υπαλλήλων σε άτομα εκτός οργανισμού

Η δυσαρέσκεια των εργαζομένων σ’ αυτή την περίπτωση θα είναι μεγάλη. Φυσικά ο κίνδυνος αποκάλυψης του κύκλου εργασιών της εταιρίας είναι μεγάλος. Θα αποκαλυφθούν projects που δε θα έπρεπε να γνωρίζουν οι ανταγωνιστές. Το κόστος για την εταιρία, ενός τέτοιου σεναρίου, θα είναι πολύ μεγάλο.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των προσωπικών αρχείων των υπαλλήλων σε άτομα εκτός οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 1.000.000 ευρώ	5
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.5.6 Ακούσια μεταβολή των προσωπικών αρχείων των υπαλλήλων

Τα μη ηθελημένα λάθη στα προσωπικά αρχεία των υπαλλήλων, ίσως προκαλέσουν κάποια προσωρινά λειτουργικά προβλήματα, που θα έχουν σχέση με την ορθότητα και το χρόνο διεκπεραίωσης ορισμένων projects. Δε θα προκληθούν μεγάλης έκτασης λάθη και παρατυπίες.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των προσωπικών αρχείων των υπαλλήλων	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.5.7 Εκούσια μεταβολή των προσωπικών αρχείων των υπαλλήλων

Μια τέτοια ενέργεια θα αποσκοπούσε στο να εκθέσει κάποιον εργαζόμενο, αφού θα υπήρχαν αλλαγές στην προσωπική του εργασία. Η πρόσβαση και η μεταβολή των στοιχείων αυτών είναι παράνομη και έχει ως στόχο να βλάψει τον εργαζόμενο.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των δεδομένων των πελατών	Βαθμός
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 30.0001 – 100.000 €	4
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.6 Συμβάσεις έργων - Προμηθευτές – Μεταπωλητές

Σημαντικό πακέτο δεδομένων. Είναι συγκεντρωμένα τα μεγαλύτερα έργα που έχει αναλάβει η εταιρία καθώς και όλοι οι συνεργάτες της. Η προμήθεια και η μεταπώληση των προϊόντων είναι ένας κρίκος που δεν πρέπει να σπάσει.

6.3.6.1 Απώλεια διαθεσιμότητας των συμβάσεων έργων και της λίστας των συνεργατών

Μια σύντομη απώλεια διαθεσιμότητας των συγκεκριμένων δεδομένων δε θα έχει ιδιαίτερες επιπτώσεις στη λειτουργία της εταιρίας. Τα δεδομένα αυτά χρειάζονται περιστασιακά. Για μεγαλύτερη χρονική διάρκεια της μη διαθεσιμότητας υπάρχει ο κίνδυνος οικονομικής απώλειας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 30.001 – 100.000 Ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.6.2 Καταστροφή ή απώλεια των συμβάσεων έργων και της λίστας των συνεργατών

Η μερική καταστροφή ή απώλεια των συγκεκριμένων δεδομένων θα δημιουργήσει προβλήματα που θα σχετίζονται με τη δυσαρέσκεια των συνεργατών της εταιρίας αλλά και με τα συμβόλαια που έχουν υπογραφεί με τους πελάτες της.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των συμβάσεων έργων και της λίστας των συνεργατών	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.6.3 Καταστροφή (ολική) των συμβάσεων έργων και της λίστας των συνεργατών

Πλήττεται πολύ σοβαρά το κύρος της εταιρίας. Πλέον δεν είναι σε θέση να ξέρει τι προβλέπει το κάθε συμβόλαιο που έχει υπογραφεί με τους πελάτες της, ακόμα και με ποιους έχει κάνει συμβόλαιο, αλλά χάνει και όλα τα στοιχεία των συνεργατών της (τιμές προϊόντων, προηγούμενες αγορές – πωλήσεις). Οι ενδεχόμενες οικονομικές απώλειες είναι μεγάλες.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των συμβάσεων έργων και της λίστας των συνεργατών	Βαθμός
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Απώλεια καλής φήμης - Έντονη αποδοκιμασία κοινού σε εθνική κλίμακα	7
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας - 300.001 – 1.000.000 Ευρώ	6
Αποτίμηση σε κλίμακα 1-10	**7**

6.3.6.4 Αποκάλυψη των συμβάσεων έργων και της λίστας των συνεργατών σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Το πρόβλημα που θα δημιουργηθεί θα έχει κακό αντίκτυπο στους εργαζομένους της εταιρίας. Παρόλα αυτά, οι συνέπειες θα είναι μικρές, έως μηδαμινές.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των συμβάσεων έργων και της λίστας των συνεργατών σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.6.5 Αποκάλυψη των συμβάσεων έργων και της λίστας των συνεργατών σε άτομα εκτός οργανισμού

Η αποκάλυψη αυτών των δεδομένων θα κοινοποιήσει στους ανταγωνιστές της εταιρίας όλο τον κύκλο εργασιών της και θα την εκθέσει σε πολύ μεγάλο βαθμό. Η διαρροή τέτοιων δεδομένων θα δημιουργήσει οικονομικά προβλήματα στην εταιρία αλλά και ενδεχόμενο όφελος των ανταγωνιστών της.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των συμβάσεων έργων και της λίστας των συνεργατών εκτός του οργανισμού	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 30.001 – 100.000 Ευρώ	4
Εμπορικά και οικονομικά συμφέροντα – Πρόκληση οικονομικής απώλειας και ωφέλεια ανταγωνιστή μέχρι 1.000.000 ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.6.6 Ακούσια μεταβολή των συμβάσεων έργων και της λίστας των συνεργατών

Η ακούσια αλλαγή των στοιχείων σε μέρος των δεδομένων ίσως προκαλέσει προσωρινά προβλήματα και δυσλειτουργίες στη λειτουργία της εταιρίας. Ενδεχομένως να υπάρξουν τριβές με ορισμένους συνεργάτες.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των συμβάσεων έργων και της λίστας των συνεργατών	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

6.3.6.7 Εκούσια μεταβολή των συμβάσεων έργων και της λίστας των συνεργατών

Η εκούσια αλλοίωση των συγκεκριμένων δεδομένων θα δημιουργήσει πολλά προβλήματα στις σχέσεις της εταιρίας με σύνολο των εμπλεκομένων αυτής της κατηγορίας. Αλλοιώσεις στα συμβόλαια με τους πελάτες σημαίνει λανθασμένη παροχή υλικών και υπηρεσιών.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των συμβάσεων έργων και της λίστας των συνεργατών	**Βαθμός**
Απώλεια καλής φήμης – Δημόσια παράπονα κοινού ή εθνικής κλίμακας δυσφήμηση	5
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 30.0001 – 100.000 €	4
Αποτίμηση σε κλίμακα 1-10	**5**

6.3.7 Πρωτόκολλο

Τα δεδομένα που διατηρούνται στο πρωτόκολλο συμβάλλουν άμεσα στην εύρυθμη λειτουργία της εταιρίας. Υπάρχει μια ενιαία βάση, την οποία μπορούν να προσπελάσουν οι εργαζόμενοι της εταιρίας, προκειμένου να αντλήσουν πληροφορίες για κάθε εισερχόμενη και εξερχόμενη εντολή.

6.3.7.1 Απώλεια διαθεσιμότητας των δεδομένων του πρωτοκόλλου

Μια πιθανή απώλεια της διαθεσιμότητας των δεδομένων του πρωτοκόλλου δε θα δημιουργούσε εκτεταμένα προβλήματα στη λειτουργία της εταιρίας αλλά μόνο κάποιες περιστασιακές δυσλειτουργίες.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.7.2 Καταστροφή ή απώλεια των δεδομένων του πρωτοκόλλου

Στην περίπτωση που στο τελευταίο αντίγραφο ασφαλείας δεν έχει συμπεριλήφθη μέρος του πρωτοκόλλου, τότε θα δημιουργηθεί πρόβλημα στην διεκπεραίωση συγκριμένων λειτουργιών, όπως είναι οι παραγγελίες στο εξωτερικό και εσωτερικό της χώρας αλλά και περιπτώσεις δυσλειτουργίας τους τεχνικού τμήματος, αφού δε θα έχουν άμεση εικόνα των εισερχόμενων αιτημάτων.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής ή απώλειας των δεδομένων του πρωτοκόλλου	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.7.3 Καταστροφή (ολική) των δεδομένων του πρωτοκόλλου

Η μη ύπαρξη εφεδρικού αντιγράφου ασφαλείας για τα δεδομένα που διατηρούνται στο πρωτόκολλο θα προκαλέσει δυσλειτουργία στην εταιρία, στο κομμάτι της οργάνωσης και της φύλαξης του ιστορικού των εντολών – αιτημάτων που δέχεται και στέλνει. Το τμήμα αποθήκης (logistics), δε θα είναι σε θέση να βάλει σε χρονική σειρά της παραγγελίες με αποτέλεσμα την καθυστέρηση όλης της διαδικασίας παράδοσης- παραλαβής προϊόντων. Το τεχνικό τμήμα δε θα έχει κανένα στοιχείο για τα αιτήματα των πελατών, με συνέπεια τη δυσαρέσκειά τους.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση καταστροφής (ολική) των δεδομένων του πρωτοκόλλου	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική απώλεια – Παρεμπόδιση λειτουργίας – 30.001 – 100.000 Ευρώ	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.3.7.4 Αποκάλυψη των δεδομένων του πρωτοκόλλου σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού

Δεν υπάρχει καμιά απολύτως επίπτωση στη λειτουργία της εταιρίας. Είναι δεδομένα στα οποία έχουν πρόσβαση όλοι οι υπάλληλοι της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων του πρωτοκόλλου σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού	Βαθμός
Δεν ορίζεται	-
Αποτίμηση σε κλίμακα 1-10	**-**

6.3.7.5 Αποκάλυψη των δεδομένων του πρωτοκόλλου σε άτομα εκτός οργανισμού

Η αποκάλυψη των συγκεκριμένων δεδομένων σε άτομα εκτός της εταιρίας δεν έχει κάποιο αρνητικό αποτέλεσμα στη λειτουργία της. Ενδεχόμενος να προκαλέσει μια μικρής έκτασης δυσφήμηση.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση αποκάλυψης των δεδομένων του πρωτοκόλλου	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.7.6 Ακούσια μεταβολή των δεδομένων του πρωτοκόλλου

Κάποιες ακούσιες αλλαγές μικρής έκτασης, στα δεδομένα του πρωτοκόλλου, ίσως προκαλέσουν μια προσωρινή δυσλειτουργία στην εταιρία και σύγχυση στους υπαλλήλους. Το τεχνικό τμήμα ενδέχεται να προβεί σε λάθος ενέργειες με αποτέλεσμα τη δυσαρέσκεια του πελάτη.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση ακούσιας μεταβολής των δεδομένων του πρωτοκόλλου	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 1.001 – 10.000 Ευρώ	2
Αποτίμηση σε κλίμακα 1-10	**3**

6.3.7.7 Εκούσια μεταβολή των δεδομένων του πρωτοκόλλου

Η εκούσια μεταβολή των δεδομένων θα έχει ως συνέπεια την πλήρη αποδιοργάνωση του τμήματος της αποθήκης αλλά και του ιστορικού των ενεργειών του τεχνικού τμήματος. Η δυσλειτουργία στην εταιρία είναι δεδομένη.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση της εκούσιας μεταβολής των δεδομένων του πρωτοκόλλου	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Οικονομική Απώλεια – Παρεμπόδιση λειτουργίας – 30.0001 – 100.000 €	4
Αποτίμηση σε κλίμακα 1-10	**4**

6.4 Αποτίμηση υπηρεσιών

Η αποτίμηση αξίας υπηρεσιών έχει νόημα μόνο για τον τομέα της διαθεσιμότητας καθώς και τις υπηρεσίες BCT και Prophix.

6.4.1 Business Connect

6.4.1.1 Απώλεια διαθεσιμότητας της υπηρεσίας BCT

Η απώλεια των υπηρεσιών του BCT για ορισμένο χρονικό διάστημα επιφέρει δυσλειτουργία στην εταιρία και δυσαρέσκεια στους εργαζόμενους. Υπάρχει καθυστέρηση στην εξυπηρέτηση των πελατών, ακόμα και αγνόηση τους σε περιπτώσεις που περιμένουν ενημέρωση – πληροφόρηση από τους υπαλλήλους της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	**Βαθμός**
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.4.2 Prophix

6.4.2.1 Απώλεια διαθεσιμότητας της υπηρεσίας Prophix

Η απώλεια διαθεσιμότητας της υπηρεσίας Prophix επιφέρει καθυστερήσεις στην αποστολή παραγγελιών προς το εξωτερικό. Η καθυστέρηση αυτή έχει επίπτωση στην εικόνα της εταιρίας.

Αποτίμηση δεδομένων με βάση τις κλίμακες CRAMM

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ώρας (1 ώρα)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον οργανισμό	2
Αποτίμηση σε κλίμακα 1-10	**2**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα μίας ημέρας (1 μέρα)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

Αποτίμηση απώλειας διαθεσιμότητας για διάστημα δύο ημερών (2 μέρες)	Βαθμός
Απώλεια καλής φήμης – Απώλεια περιορίζεται στον κύκλο παρόμοιων οργανισμών	3
Αποτίμηση σε κλίμακα 1-10	**3**

6.5 Συγκεντρωτική αποτίμηση αξίας δεδομένων

Παρακάτω παρατίθεται πίνακας με τη συνοπτική – συγκεντρωτική αποτίμηση της αξίας των δεδομένων.

	Απώλεια διαθεσιμότητας			Απώλεια ακεραιότητας				Αποκάλυψη σε τρίτους	
	1h	1d	2d	Καταστροφή ή απώλεια	Ολική καταστροφή	Ακούσια μεταβολή	Εκούσια μεταβολή	Μη εξουσιοδοτημένα άτομα εντός οργανισμού	Άτομα εκτός οργανισμού
Προσωπικά στοιχεία υπαλλήλων	2	3	3	2	5	2	3	2	4
Εργασιακά στοιχεία υπαλλήλων	2	3	3	2	4	2	3	4	5
Έσοδα – Έξοδα	2	3	3	2	5	4	5	2	4
Πελάτες	2	3	3	2	5	3	4	2	4
Προσωπικά αρχεία υπαλλήλων	2	3	3	2	5	2	5	2	5
Συμβάσεις έργων - Προμηθευτές - Μεταπωλητές	2	3	4	3	7	2	5	2	4
Πρωτόκολλο	2	3	3	3	4	3	4	-	3

Πίνακας 4: Συγκεντρωτικός πίνακας αποτίμησης αξίας αγαθών

7 Εισαγωγή δεδομένων μελέτης στην CRAMM - Αποτελέσματα

7.1 Εισαγωγή

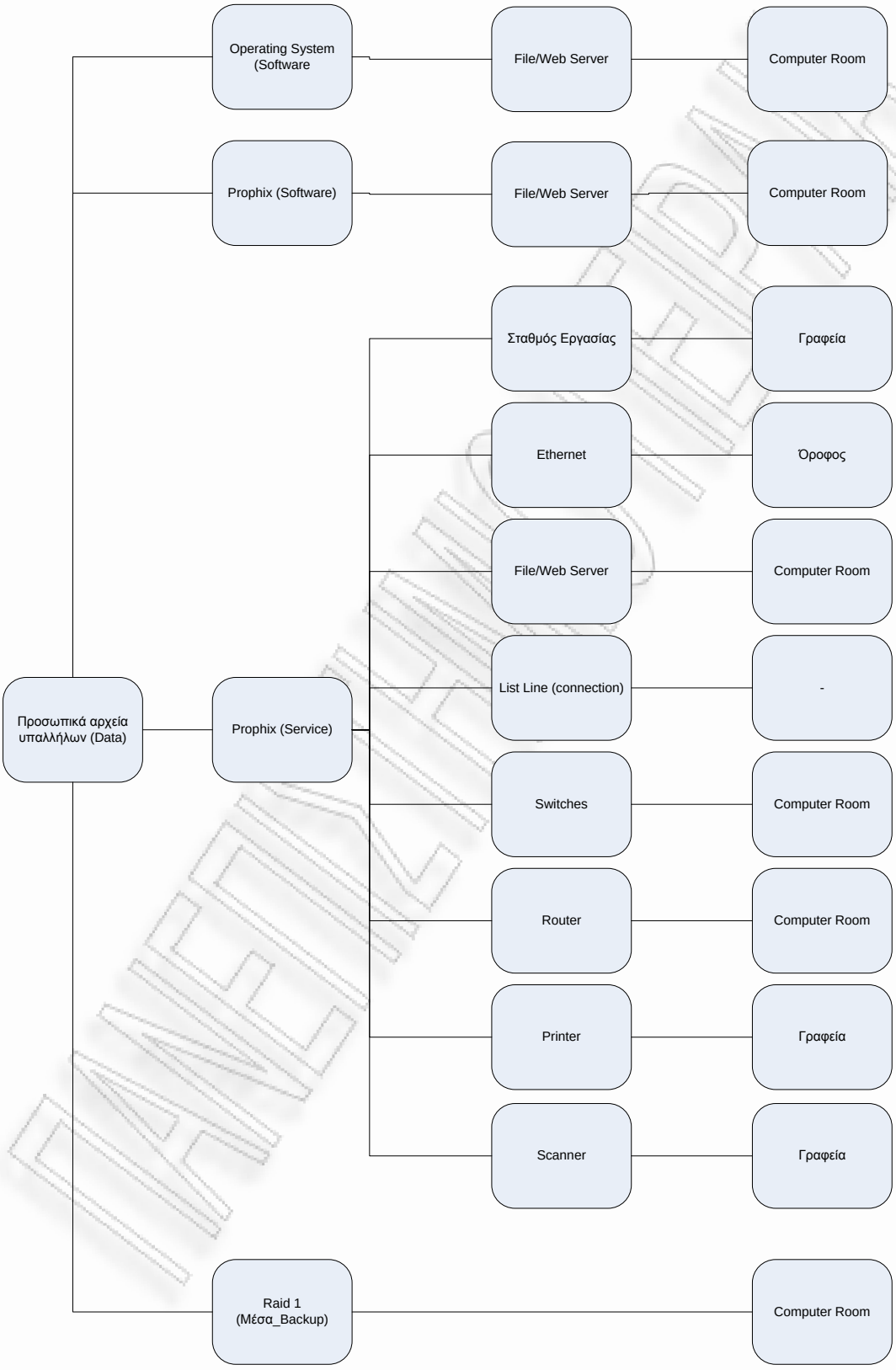
Το σύνολο των αποτελεσμάτων της αποτίμησης του προηγούμενου κεφαλαίου εισάχθηκαν στο λογισμικό CRAMM. Η μέθοδος παρήγαγε αποτελέσματα για τις απειλές και τις αδυναμίες - ευπάθειες του ΠΣ της εταιρίας, καθώς κι ένα σύνολο από προτάσεις – αντίμετρα για τις υπάρχουσες απειλές με βάση το βαθμό επικινδυνότητά τους.

7.2 Δημιουργία μοντέλων αγαθών

Σ’ αυτήν την παράγραφο δημιουργήθηκαν και παρουσιάζονται τα μοντέλα αγαθών, συσχετίζοντας τα δεδομένα με τις υπηρεσίες τελικού χρήστη και με το υλικό που τις υποστηρίζει και το υλικό με τη σειρά του με τις τοποθεσίες στις οποίες βρίσκεται, σύμφωνα με το διάγραμμα.

7.2.1 Προσωπικά αρχεία υπαλλήλων

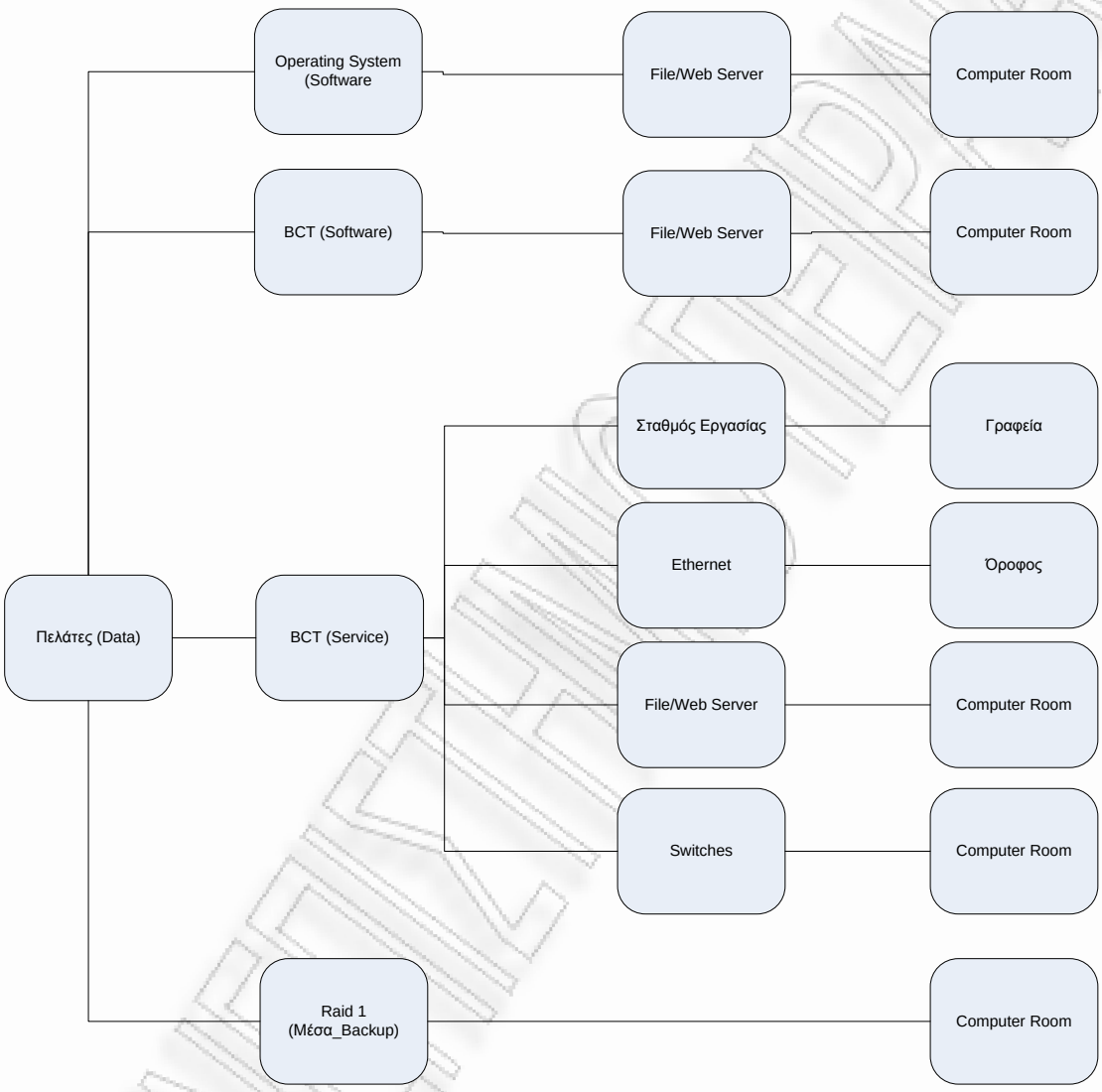
Ακολουθεί το διάγραμμα του μοντέλου των δεδομένων για τα προσωπικά αρχεία των υπαλλήλων. Το ίδιο διάγραμμα ισχύει και για τα δεδομένα «Πρωτόκολλο» και «Συμβάσεις έργων» επομένως δε χρειάζεται να ξαναδημιουργηθούν.



Εικόνα 5: Μοντέλο δεδομένων προσωπικών αρχείων υπαλλήλων

7.2.2 Πελάτες

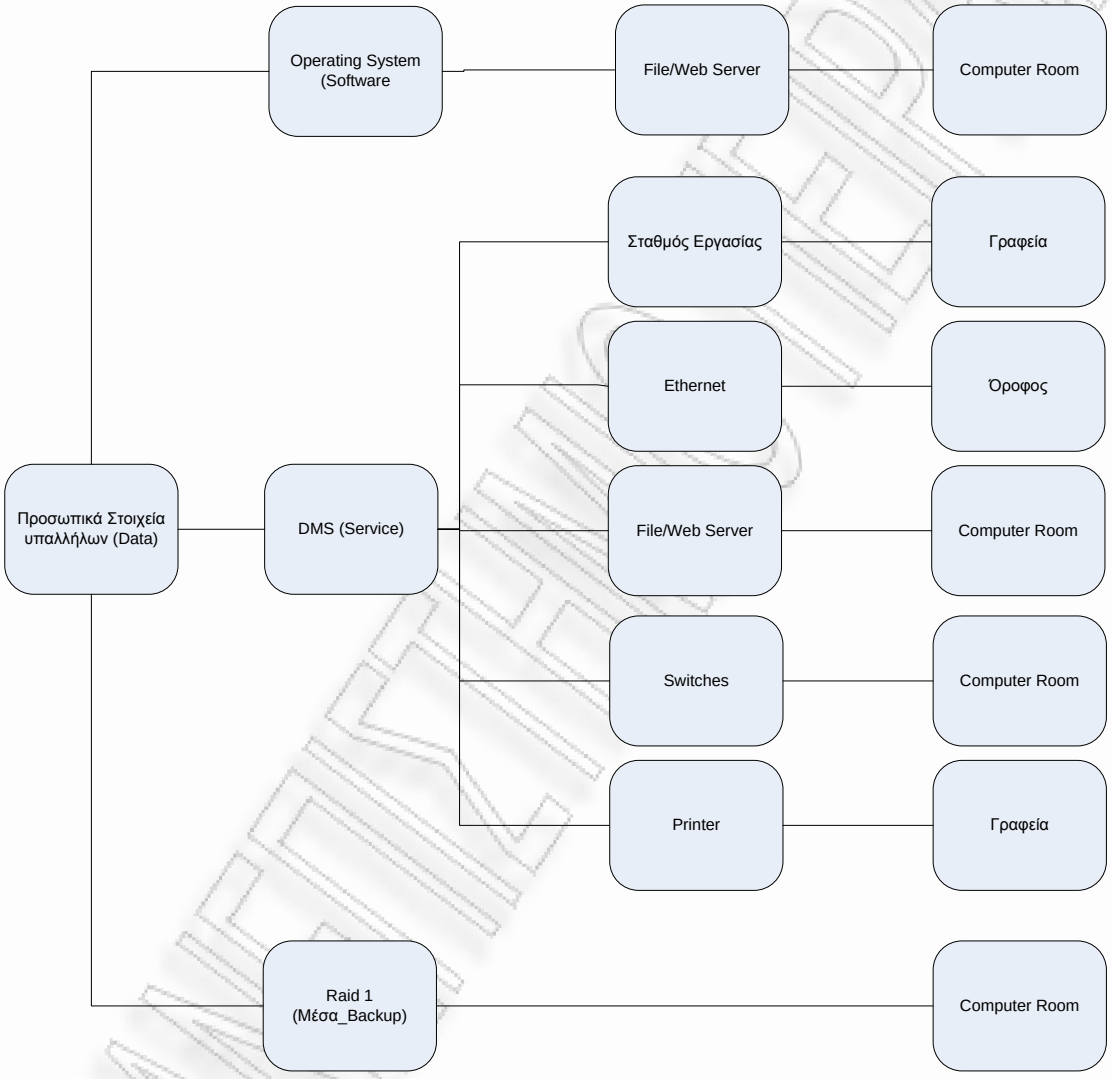
Ακολουθεί το διάγραμμα του μοντέλου των δεδομένων για τους πελάτες.



Εικόνα 6: Μοντέλο δεδομένων πελατών

7.2.3 Προσωπικά στοιχεία υπαλλήλων

Ακολουθεί το διάγραμμα του μοντέλου των δεδομένων για τα προσωπικά αρχεία υπαλλήλων. Το ίδιο διάγραμμα ισχύει και για τα δεδομένα «Εργασιακά στοιχεία υπαλλήλων» και «Έσοδα – Έξοδα».



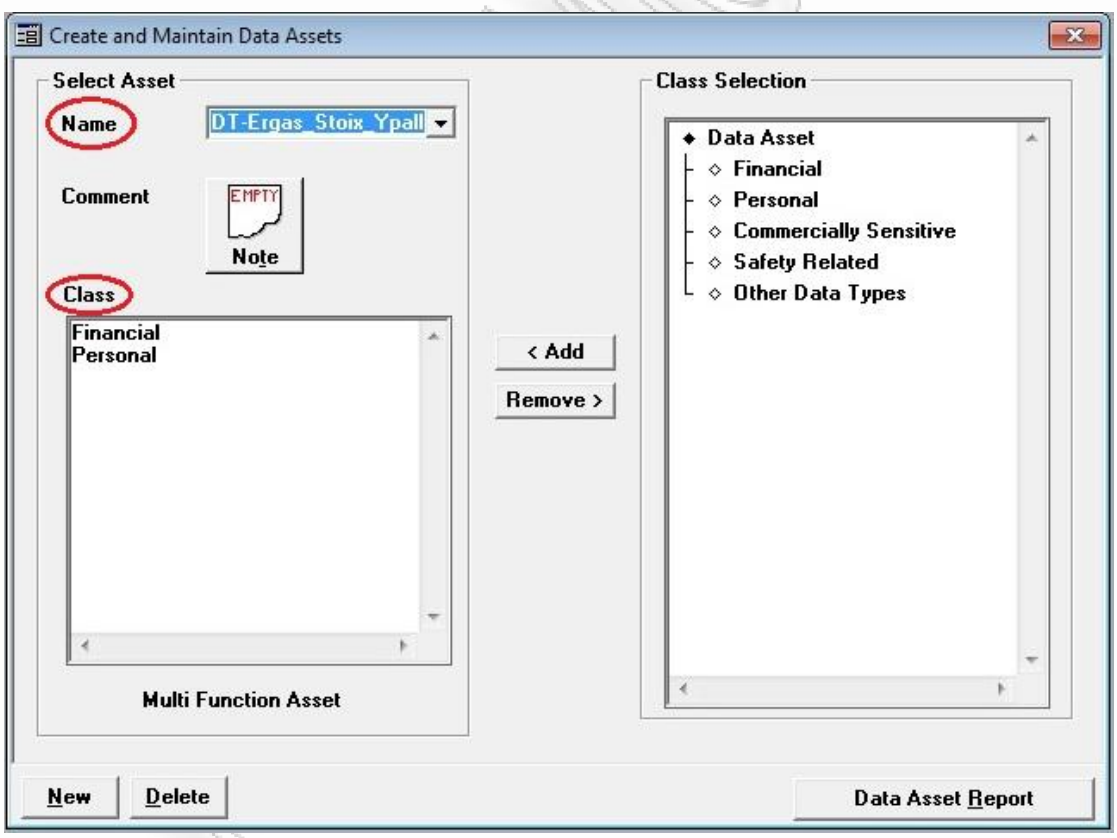
Εικόνα 7: Μοντέλο δεδομένων προσωπικών στοιχείων υπαλλήλων

7.3 Δημιουργία μοντέλου συστήματος - Εισαγωγή δεδομένων στην CRAMM

Με βάση τη συσχέτιση των δεδομένων με τις υπηρεσίες, όπως φαίνονται στα μοντέλα της προηγούμενης παραγράφου, έγινε η εισαγωγή τους στην CRAMM. Η CRAMM ορίζει πέντε κλάσεις δεδομένων και σύμφωνα μ' αυτές έγινε η κατηγοριοποίησή τους. Οι πέντε κλάσεις είναι χαρακτηριστικά οι εξής:

- Οικονομικά (Financial)
- Ευαίσθητα προσωπικά (Personal)
- Ευαίσθητα εμπορικά (Commercially Sensitive)
- Σχετικά με την ασφάλεια (Safety Related) και
- Έναν Γενικό τύπο για όλα τα υπόλοιπα (Other Data Types)

Παρακάτω φαίνεται ένα παράδειγμα (screenshot) με την κατηγοριοποίηση των εργασιακών στοιχείων των υπαλλήλων.



Εικόνα 8: Screenshot κλάσεων δεδομένων

Οι κλάσεις στις οποίες ανήκει η συγκεκριμένη κατηγορία δεδομένων είναι οικονομικά (Financial) και προσωπικά (Personal).

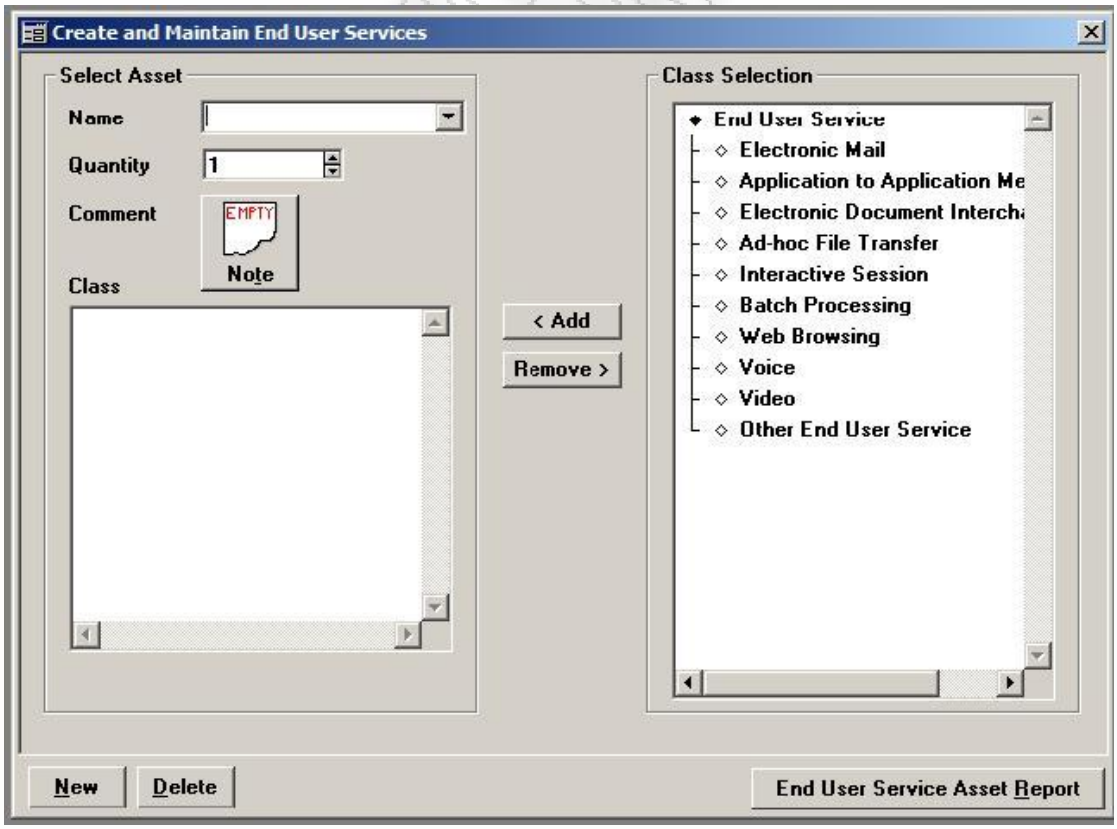
7.4 Προσδιορισμός Υπηρεσιών Τελικού Χρήστη – Identification of End User Services

Η CRAMM ορίζει τις εξής κλάσεις υπηρεσιών τελικού χρήστη:

- Electronic Mail
- Application to Application Messaging
- Electronic Document Interchange
- Ad-hoc File Transfer
- Interactive Session
- Web Browsing
- Batch Processing
- Voice - Video
- Έναν Γενικό τύπο για όλες τις υπόλοιπες (Other End User Service)

Ο προσδιορισμός έγινε στο *κεφάλαιο 5, παράγραφος 5.5*

Παρατίθεται screenshot (όχι της συγκεκριμένης εργασίας) όπου φαίνεται ο τρόπος με τον οποίο έγινε ο προσδιορισμός.



Εικόνα 9: Screenshot (δεν αφορά τη συγκεκριμένη εργασία) υπηρεσιών

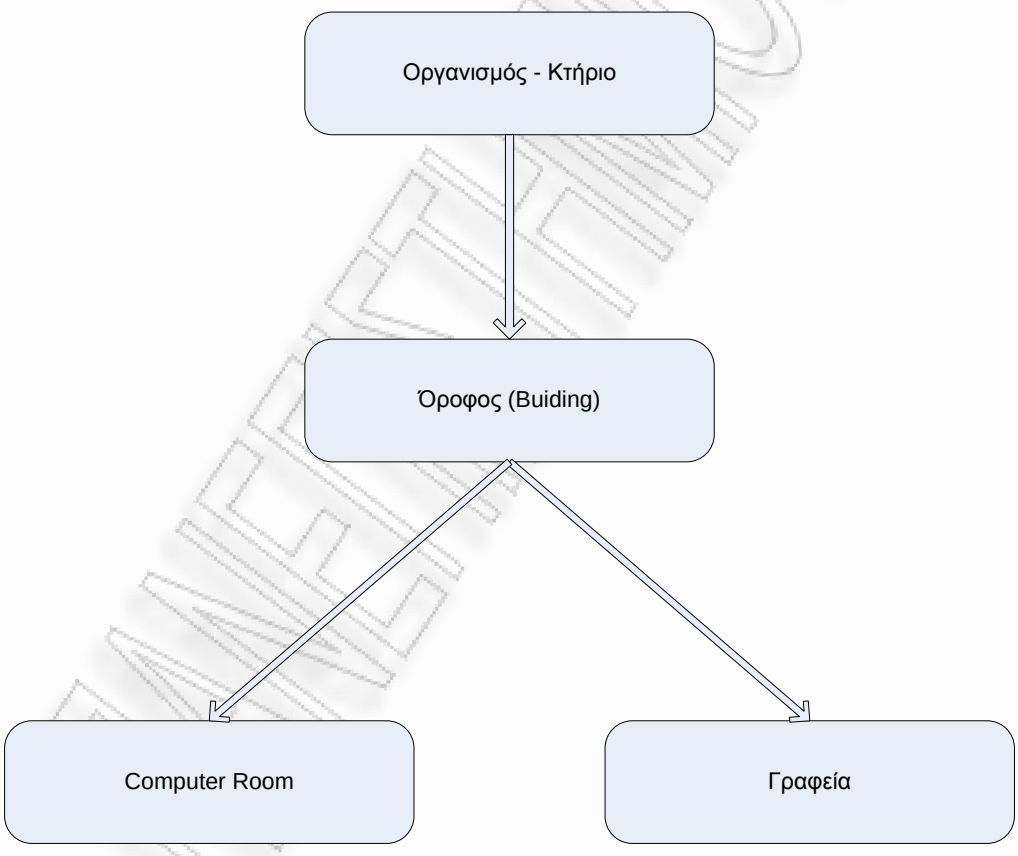
7.5 Προσδιορισμός Φυσικών Αγαθών – Identification of Physical Assets

Σ' αυτό το στάδιο της CRAMM, εισάγονται τα φυσικά αγαθά του ΠΣ τα οποία σε γενικές γραμμές είναι το hardware (workstations, printers, servers κτλ), τα καλώδια (coaxial, fiber, patch panel κτλ), τα δικτυακά στοιχεία (switch, modem, router κτλ), τα πρωτόκολλα επικοινωνίας (HTTP, WAP, FTP κτλ) κ.α.

Εισάγαμε όλα φυσικά αγαθά του ΠΣ όπως αυτά περιγράφονται στην *παράγραφο 5.2*, καθώς και τα καλώδια του εσωτερικού δικτύου με τα πρωτόκολλα επικοινωνίας.

7.6 Προσδιορισμός Τοποθεσιών – Identification of Locations

Η περιγραφή των τοποθεσιών είναι σημαντικό κομμάτι της μεθοδολογίας. Ο χώρος της εταιρίας έχει κατηγοριοποιηθεί σε τρεις συνολικά τοποθεσίες: Τον όροφο, το computer room και το χώρο των γραφείων.



Εικόνα 10: Σχεδιάγραμμα μοντέλου εταιρίας NEC

7.7 Προσδιορισμός Αγαθών τύπου Λογισμικό – Identification of Software Assets

Εισάγονται οι εφαρμογές λογισμικού που έχουν εντοπιστεί στο σύστημα. Σύμφωνα με την παράγραφο 5.4 αυτές είναι το Operating System, το Prophix, το Business Connect και το Conference Software. Η CRAMM ορίζει πέντε κλάσεις λογισμικού:

- Χρηματικών συναλλαγών (Funds Transfer)
- Οικονομικό (Financial)
- Κρίσιμο για την ασφάλεια (Safety Critical)
- Ευαίσθητα προσωπικά δεδομένα (Personal Information) και
- έναν Γενικό τύπο (General)

Για κάθε κλάση ορίζει τρεις περιπτώσεις:

- Επί παραγγελία ευαίσθητο - χρήζει προστασίας (Bespoke Sensitive)
- Επί παραγγελία μη ευαίσθητο (Bespoke Non-sensitive)
- Έτοιμο λογισμικό (Packaged)

Λογισμικό	Κλάση	Περίπτωση
Operating System	General	Packaged
Prophix	Financial	Bespoke Sensitive
Business Connect	General	Bespoke Non-sencitive
Conference Software	General	Packaged

7.8 Αποτίμηση αγαθών – Valuation of Data Assets

Στο τελικό στάδιο, η CRAMM απαιτεί από το χρήστη να εισάγει τα δεδομένα της αποτίμησης. Όλα τα αποτελέσματα της αποτίμησης υπάρχουν συνοπτικά, στον συγκεντρωτικό πίνακα αποτίμησης της παραγράφου 6.5. Η CRAMM απαιτεί την εισαγωγή των πινάκων επιπτώσεων και την κατάλληλη τιμή με βάση τη μελέτη του ΠΣ.

7.9 Αποτίμηση Φυσικών Αγαθών – Valuation of Physical Assets

Είναι το στάδιο στο οποίο έγινε αποτίμηση της αξίας των φυσικών αγαθών που εντοπίσαμε στο σύστημα. Δηλώνεται η αξία της μονάδας του κάθε υλικού.

Υλικά	Αξία	Ποσότητα
Workstations	800	11
Server	2500	1
Network	200	2
Printers/Scanners	250	2

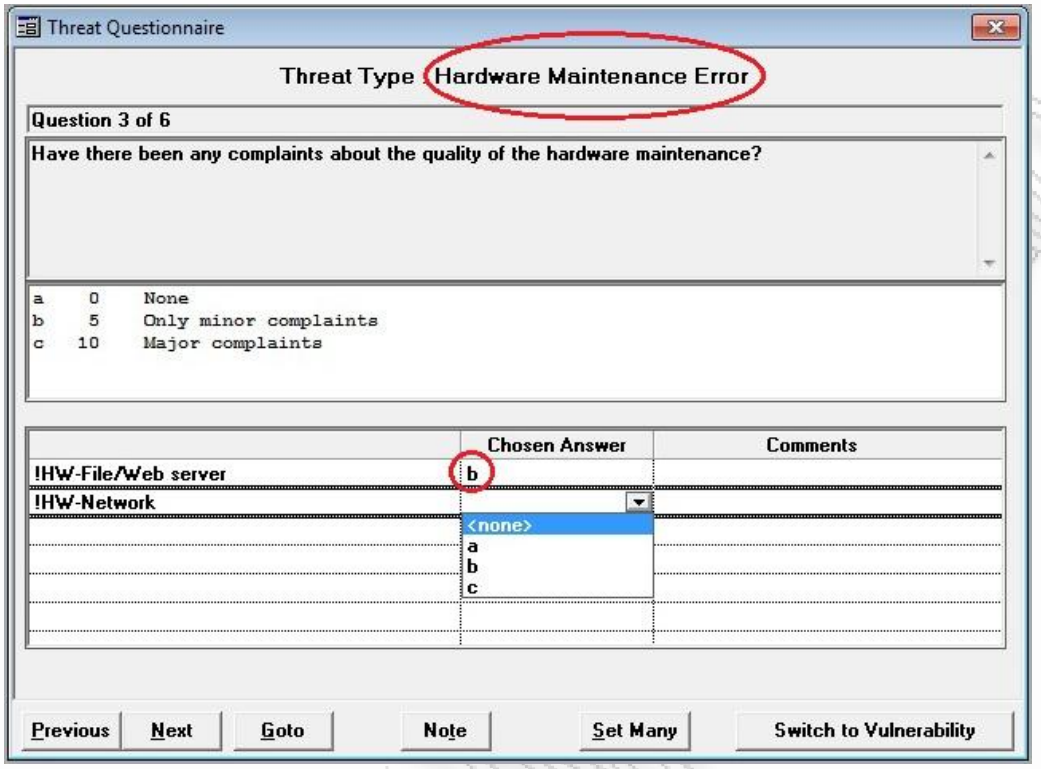
7.10 Εκτίμηση Επιπέδων Απειλών και Αδυναμιών

Το πιο χρονοβόρο κομμάτι, όσων αφορά την εισαγωγή δεδομένων από το χρήστη, είναι η εκτίμηση επιπέδων απειλών και αδυναμιών. Στο βήμα αυτό η CRAMM χρησιμοποιεί ερωτηματολόγια για να εκτιμήσει το μέγεθος της απειλής για κάθε ζεύγος αγαθού / απειλής. Για κάθε συσχέτιση δίνεται ένα ερωτηματολόγιο, που χωρίζετε σε δύο μέρη. Οι ερωτήσεις του πρώτου μέρους αφορούν την εκτίμηση των απειλών (threats) και του δεύτερου των ευπαθειών (vulnerabilities). Παρακάτω παρατίθενται screenshots της εφαρμογής με χαρακτηριστικά παραδείγματα ερωτήσεων.

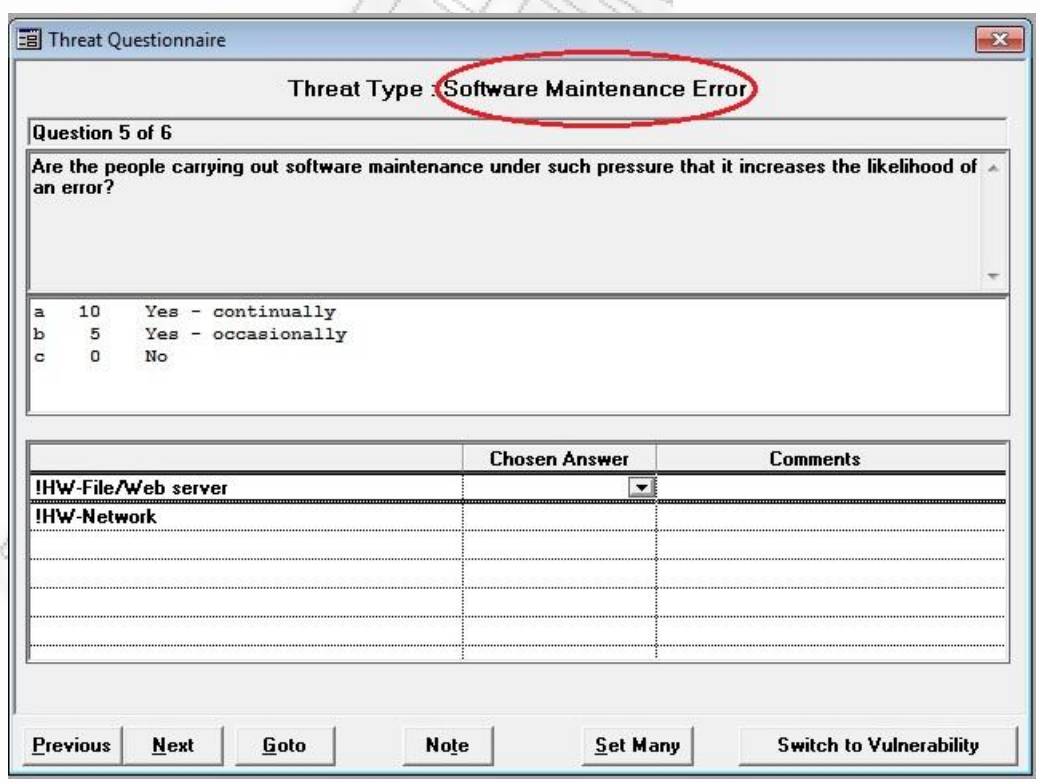
Η *Εικόνα 11* αναφέρεται στην απειλή τύπου σφάλματος συντήρησης στο hardware. Η ερώτηση η οποία απευθύνεται στο μελετητή (και όχι στους υπαλλήλους – στελέχη της εταιρίας, λόγω μεγάλου όγκου ερωτήσεων), είναι για το αν υπήρξαν παράπονα για την ποιότητα της συντήρησης του hardware. Η ερώτηση αφορά στο File/Web Server και στο δίκτυο της εταιρίας. Στην πρώτη περίπτωση (του Server) η απάντηση που δόθηκε ήταν πως γίνανε ασήμαντα παράπονα (επιλογή *b*). Όσων αφορά στο δίκτυο (Network) φαίνονται στο αναδυόμενο μενού οι επιλογές που μας δίνει η CRAMM (a, b, c).

Στην *Εικόνα 12* γίνεται ερώτηση σχετικά με τη συντήρηση του λογισμικού. Το πρόγραμμα ρωτά αν οι υπεύθυνοι για τη διενέργεια της συντήρησης του λογισμικού, βρίσκονται υπό πίεση, έτσι ώστε να αυξάνεται η πιθανότητα να υποπέσουν σε λάθη. Οι απαντήσεις είναι «ναι – συνεχώς», «ναι – περιστασιακά» και «όχι». Έχει επιλεγεί η περίπτωση *b* (δε φαίνεται στην εικόνα).

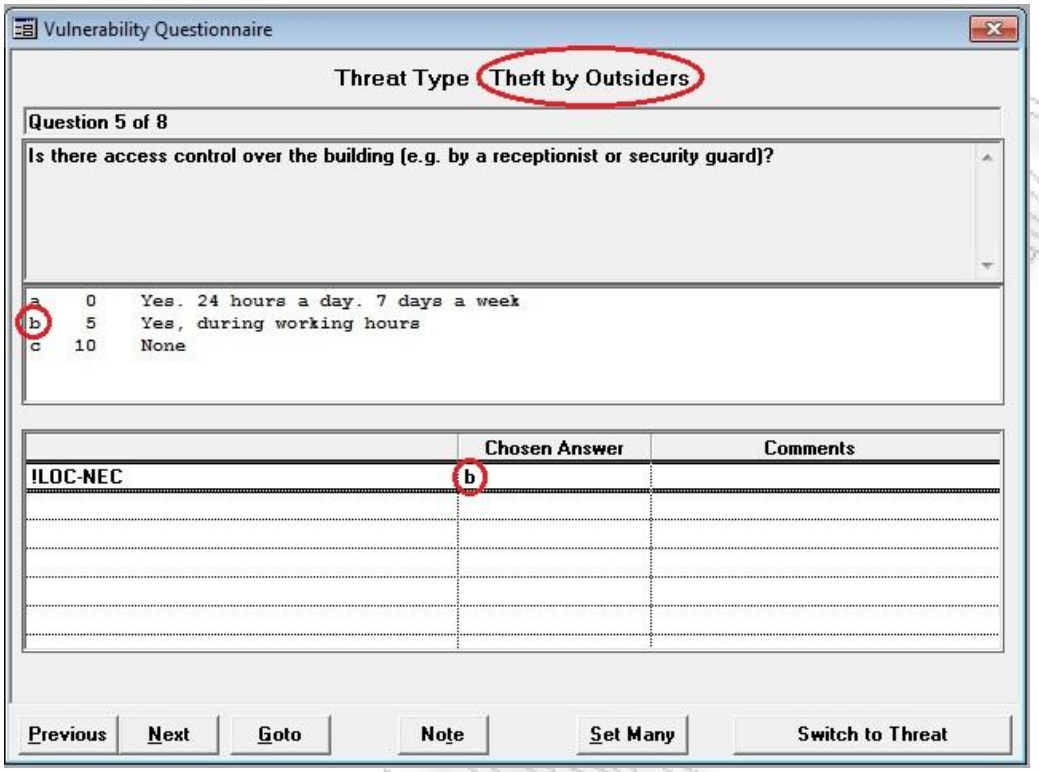
Στην *Εικόνα 13* γίνεται αναφορά στην κλοπή από άτομα εκτός εταιρίας (ξένους). Η ερώτηση που απευθύνει είναι αν υπάρχει έλεγχος εισόδου στο κτίριο από κάποιο φρουρό ή receptionist. Δόθηκε η απάντηση *b* – ναι, μόνο κατά τις εργάσιμες ώρες.



Εικόνα 11: Screenshot απειλής Hardware Maintenance Error



Εικόνα 12: Screenshot απειλής Software Maintenance Error



Εικόνα 13: Screenshot απειλής Theft by Outsiders

7.11 Αναφορά Εκτίμησης Επιπέδων Απειλών και Αδυναμιών

Οι αναφορές της μελέτης που εξήγαγε η CRAMM βρίσκονται στο ψηφιακό τεκμήριο που συνοδεύει τη μελέτη. Λόγω του μεγάλου όγκου των αναφορών επιλέχθηκαν ορισμένα τμήματά τους για να παρουσιαστούν και να σχολιαστούν.

Ακολουθούν επιλεγμένα πινακάκια της αναφοράς Εκτίμησης Επιπέδων Απειλών και Αδυναμιών – Threat and Vulnerability Summary, παίρνοντας ως κριτήριο την ένδειξη για πολύ υψηλή απειλή (Very High) ανά αγαθό.

Διείσδυση στις επικοινωνίες	Full Threat	Full Vuln
!SRV-Prophix	High	Medium
!SRV-BCT	Low	Low
!SRV-DMS	**Very High**	Medium

Πίνακας 5: Διείσδυση στις επικοινωνίες(αφορά σε υπηρεσίες)

Υποκλοπή επικοινωνιών	Full Threat	Full Vuln
!SRV-Prophix	High	Medium
!SRV-BCT	Low	Low
!SRV-DMS	**Very High**	Medium

Πίνακας 6: Υποκλοπή επικοινωνιών (αφορά σε υπηρεσίες)

Παραποίηση επικοινωνιών	Full Threat	Full Vuln
!SRV-Prophix	Low	High
!SRV-BCT	Low	Medium
!SRV-DMS	**Very High**	Medium

Πίνακας 7: Παραποίηση επικοινωνιών (αφορά σε υπηρεσίες)

Τεχνική βλάβη στοιχείου διανομής δικτύου	Full Threat	Full Vuln
!HW-Network	**Very High**	Medium

Πίνακας 8: Τεχνική βλάβη του βλάβη στοιχείου διανομής δικτύου (αφορά σε Hardware)

Αποτυχία λογισμικού στο σύστημα και στο δίκτυο	Full Threat	Full Vuln
!HW-File/Web server	**Very High**	High
!!Workstation	**Very High**	High
!HW-Network	**Very High**	High

Πίνακας 9: Αποτυχία λογισμικού στο σύστημα και στο δίκτυο (αφορά σε Hardware)

Αποτυχία εφαρμογών λογισμικού	Full Threat	Full Vuln
!SW-Software	**Very High**	High

Πίνακας 10: Αποτυχία εφαρμογών λογισμικού (αφορά σε software)

Σφάλμα χειρισμών	Full Threat	Full Vuln
!HW-File/Web server	Very High	Medium
!HW-Network	Very High	Medium

Πίνακας 11: Σφάλμα χειρισμών (αφορά σε hardware)

7.12 Ανάλυση επικινδυνότητας

Μετά το πέρας της αυτοματοποιημένης διαδικασίας της ανάλυσης επικινδυνότητας που ακολουθεί η CRAMM, εκτυπώνεται μια αναφορά που παρουσιάζει ανά απειλή, για όλες τις ομάδες αγαθών, που είχαν συσχετιστεί με την απειλή, το επίπεδο της απειλής, το επίπεδο της αδυναμίας, την τιμή της επίπτωσης και την εκτίμηση της επικινδυνότητας ανά επίπτωση (πχ απώλεια διαθεσιμότητας, ολική καταστροφή κλπ). Ακολουθούν επιλεγμένα πινακάκια της συγκεκριμένης αναφοράς, η επιλογή των οποίων έγινε με βάση την ένδειξη για πολύ υψηλή απειλή (VH).

7.12.1 Απειλή: Διείσδυση στις επικοινωνίες

	Unavailability						Dest	Disclosure			Modific	Commun Impacts
	15 M	1 H	3 H	12 H	1 D	2 D	B	I	C	O	DM	Nd
Αγαθό: SRV-DMS												
Απειλή	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
Αδυναμία	L	L	L	L	L	L	L	L	L	L	L	L
Επίπτωση		2	2	3	3	3	2	2		4	5	
Επικινδυνότητα		3	3	3	3	3	3	3		4	4	

Πίνακας 12: Απειλή: Διείσδυση στις επικοινωνίες – Αγαθό: SRV-DMS

7.12.2 Απειλή: Υποκλοπή επικοινωνιών

	Unavailability						Dest	Disclosure			Modific	Commun Impacts
								I	C	O		Tm
Αγαθό: SRV-DMS												
Απειλή								VH	VH	VH		VH
Αδυναμία								M	M	M		M
Επίπτωση								2		4		
Επικινδυνότητα								3		4		

Πίνακας 13: Απειλή: Υποκλοπή επικοινωνιών – Αγαθό: SRV-DMS

7.12.3 Απειλή: Παραποίηση επικοινωνιών

	Unavailability						Dest	Disclosure			Modification				Commun Impacts			
								I	C	O	SE	WE	DM	In	Nd	Rp	Mr	Os
Αγαθό: SRV-DMS																		
Απειλή								VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
Αδυναμία								M	M	M	M	M	M	M	M	M	M	M
Επίπτωση								2		4		4	5					
Επικινδυνότητα								3		4		5	5					

Πίνακας 14: Απειλή: Παραποίηση επικοινωνιών - Αγαθό: SRV-DMS

7.12.4 Απειλή: Τεχνική βλάβη στοιχείου διανομής δικτύου

	Unavailability						Dest	Disclosure			Modific	Commun Impacts		
	15 M	1 H	3 H	12 H								Nd	Mr	Os
Αγαθό: HW-Network														
Απειλή	VH	VH	VH	VH								VH	VH	VH
Αδυναμία	M	M	L	L								L	L	L
Επίπτωση														
Επικινδυνότητα														

Πίνακας 15: Απειλή: Τεχνική βλάβη στοιχείου διανομής δικτύου – Αγαθό HW-Network

7.12.5 Απειλή: Αποτυχία λογισμικού στο σύστημα και στο δίκτυο

	Unavailability						Dest	Disclosure			Modific		Commun Impacts	
	15 M	1 H	3 H	12 H			B	I	C	O	SE	WE	Nd	Mr
Αγαθό: Workstation														
Απειλή	VH	VH	VH	VH			H	H	H	H	H	H	H	H
Αδυναμία	H	L	L	L			L	L	L	L	L	L	L	L
Αγαθό: HW-File/Web server														
Απειλή	VH	VH	VH	VH			H	H	H	H	VH	H	H	H
Αδυναμία	H	H	H	L			L	L	L	L	L	L	L	L
Επίπτωση		2	2	2										
Επικινδυνότητα		4	4	3										

Πίνακας 16: Απειλή: Αποτυχία λογισμικού στο σύστημα και στο δίκτυο

7.12.6 Απειλή: Αποτυχία εφαρμογών λογισμικού

	Unavailability						Dest	Disclosure			Modific		Commun Impacts	
	15 M	1 H	3 H	12 H			B	I	C	O	SE	WE	Nd	Mr
Αγαθό: HW-Network														
Απειλή	VH	VH	VH	VH			H	H	H	H	VH	H	H	H
Αδυναμία	H	L	H	L			L	L	L	L	L	L	L	L
Αγαθό: SW-Software														
Απειλή	VH	VH	VH	VH			M	M	M	M	H	H	M	M
Αδυναμία	H	M	M	M			L	M	L	L	M	M	L	L
Επίπτωση		2	2	2						3				
Επικινδυνότητα		3	3	3						2				

Πίνακας 17: Απειλή: Αποτυχία εφαρμογών λογισμικού – Αγαθά: HW-Network, SW-Software

7.12.7 Απειλή: Σφάλμα χειρισμών

	Unavailability						Dest		Disclosure			Modific		Commun Impacts
	15 M	1 H	3 H	12 H			B	T	I	C	O	SE	WE	-
Αγαθό: HW-File/Web server														
Απειλή	VH	VH	VH	VH			VH	VH	VH	VH	VH	VH	VH	-
Αδυναμία	M	L	L	L			L	L	L	L	L	M	M	-
Επίπτωση		2	2	2					3		4			-
Επικινδυνότητα		3	3	3					3		4			-
Αγαθό: HW-Network														
Απειλή	VH	VH	VH	VH			VH	VH	VH	VH	VH	VH	VH	-
Αδυναμία	M	L	L	L			L	L	L	L	L	L	L	-

Πίνακας 18: Απειλή: Σφάλμα χειρισμών – Αγαθά: HW-File/Web server , HW-Network

7.12.8 Ανάλυση στοιχείων των πινάκων ανάλυσης επικινδυνότητας

i. **Unavailability - Μη διαθεσιμότητα:**
- 1 hour – 1 ώρα
- 1 day – 1 μέρα
- 2 days – 2 μέρες

ii. **Destruction – Απώλεια:**
- Destruction since the last successful back-up – Μερική απώλεια δεδομένων
- Total destruction including back-ups – Ολική καταστροφή δεδομένων συμπεριλαμβανομένου του τελευταίου αντιγράφου ασφαλείας

iii. **Disclosure - Αποκάλυψη:**
- Unauthorized disclosure to insiders - Αποκάλυψη των δεδομένων σε εσωτερικούς χρήστες
- Unauthorized disclosure to contracted service providers - Αποκάλυψη των δεδομένων σε Παρόχους Υπηρεσιών
- Unauthorized disclosure to outsiders - Αποκάλυψη των δεδομένων σε τρίτους

iv. **Modification - Αλλαγή:**
- small-scale errors - Περιορισμένη ύπαρξη λαθών στα δεδομένα
- widespread errors - Εκτεταμένη ύπαρξη λαθών στα δεδομένα
- deliberate modification - Σκόπιμη αλλοίωση των δεδομένων
- small-scale errors (for example, keying errors, duplication of input)
- widespread errors (for example, caused by a programming error)

v. **Insertion of false message** – Καταχώρηση λάθος μηνυμάτων

vi. **Communication Impacts** – Επιπτώσεις στην επικοινωνία

Ακολουθεί πίνακας με τις επεξηγήσεις των συντομογραφιών που συναντούνται στους πίνακες ανάλυσης επικινδυνότητας.

Συντομογραφία	Επεξήγηση
P	Physical destruction
15 M	Unavailability - 15 minutes
1 Hr	Unavailability - 1 hour
3 Hr	Unavailability - 3 hours
12 Hr	Unavailability - 12 hours
1 Dy	Unavailability - 1 day
2 Dy	Unavailability - 2 days
1 W	Unavailability - 1 week
2 W	Unavailability - 2 weeks
1 M	Unavailability - 1 month
2 M	Unavailability - 2 months
B	Loss of data since last back-up
T	Total loss of all data
I	Unauthorised disclosure to insiders
C	Unauthorised disclosure to contracted third parties
O	Unauthorised disclosure to outsiders
S E/T	Small-scale errors (for example, keying errors)/small-scale errors in transmission
W E/T	Widespread errors (for example, programming errors)/widespread errors in transmission
D S/T	Deliberate modification of stored data/deliberate modification of data in transit
Or	Repudiation of origin
Rc	Repudiation of receipt
Nd	Non-delivery
Rp	Replay
Mr	Mis-routing
Tm	Traffic monitoring
Os	Out-of-sequence
In	Insertion of false message

Πίνακας 19: Συντομογραφίες πινάκων επιπτώσεων

7.13 Αναφορές Αντιμέτρων

Έχουν επιλεγεί ορισμένες, μόνο, αναφορές αντιμέτρων προκειμένου να παρουσιαστούν. Το πλήθος των αναφορών ήταν τέτοιο που δεν επέτρεψε την εισαγωγή τους στην εργασία. Η επιλογή έγινε με βάση το αγαθό στο οποίο αναφέρονται τα αντίμετρα ανά κατηγορία και έγινε προσπάθεια να καλυφθούν όσο το δυνατόν περισσότερες κατηγορίες. Οι εκτεταμένες αναφορές αντιμέτρων υπάρχουν στο ψηφιακό τεκμήριο που συνοδεύει τη μελέτη.

7.13.1 Mobile Computing και τηλεργασία

Ομάδα Αντιμέτρων: Mobile computing και τηλεργασία
Υποομάδα Αντιμέτρων: Τηλεργασία κι εργασία από το σπίτι
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Η απομακρυσμένη πρόσβαση στις πληροφορίες της εταιρίας μέσω κινητών υπολογιστικών συσκευών χρήζει ιδιαίτερης προστασίας

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Η τηλεργασία θα πρέπει να επιτρέπεται μόνο αν οι κατάλληλες ρυθμίσεις ασφαλείας είναι ενεργοποιημένες	SRV – DMS
1.1	Πρέπει να διενεργηθεί έρευνα της προτεινόμενης τοποθεσίας για το περιβάλλον τηλεργασίας	SRV – DMS
1.1.1	Έρευνα για την ύπαρξη φυσικής ασφάλειας της προτεινόμενης τοποθεσίας για την τηλεργασία	SRV – DMS
1.1.2	Έρευνα της προτεινόμενης τοποθεσίας για το περιβάλλον τηλεργασίας	SRV – DMS
1.1.3	Έρευνα για τις απαιτήσεις της ασφάλειας τηλεπικοινωνιών	SRV – DMS
1.1.4	Έρευνα για την απειλή χρήσης της τηλεργασίας από άλλα άτομα	SRV – DMS
1.2	Δημιουργία κατάλληλων ρυθμίσεων ασφαλείας που θα δημιουργηθούν στο χώρο τηλεργασίας	SRV – DMS
1.2.1	Παροχή κατάλληλου εξοπλισμού και επίπλων αποθήκευσης	SRV – DMS
1.2.2	Ορισμός των εργασιών που επιτρέπεται να διενεργηθεί εντός της τηλεργασίας	SRV – DMS
1.2.3	Παροχή κατάλληλου εξοπλισμού επικοινωνιών, συμπεριλαμβανομένων των μεθόδων, για την εξασφάλιση της απομακρυσμένης πρόσβασης	SRV – DMS
1.2.4	Κανόνες και οδηγίες για την πρόσβαση των οικείων και των επισκεπτών στον εξοπλισμό και τις πληροφορίες	SRV – DMS
1.2.5	Παροχή υποστήριξης hardware και software	SRV – DMS
1.2.6	Διαδικασίες για Back-up και επιχειρηματικής	SRV – DMS

	συνέχειας	
1.2.7	Διαδικασίες ελέγχου και παρακολούθησης της ασφάλειας	SRV – DMS
1.2.8	Διαδικασίες για την επιστροφή του εξοπλισμού και την ανάκληση των δικαιωμάτων πρόσβασης, όταν παύσει οι δραστηριότητες της τηλεργασίας δραστηριοτήτων παύσει	SRV – DMS

7.13.2 Προστασία ενάντια σε κακόβουλο λογισμικό (1/3)

Ομάδα Αντιμέτρων: Προστασία ενάντια σε κακόβουλο λογισμικό

Υποομάδα Αντιμέτρων: Παρεμπόδιση ενάντια σε κακόβουλο λογισμικό

Άποψη Ασφαλείας: Διαδικαστικό

Δήλωση Πολιτικής: Οι διαδικασίες θα πρέπει να ελαχιστοποιούν το ενδεχόμενο για την εισαγωγή κακόβουλου λογισμικού στο Πληροφοριακό σύστημα

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Οι δυνατότητες για την εισαγωγή του κακόβουλου λογισμικού στο πληροφοριακό σύστημα θα πρέπει να ελαχιστοποιούνται	HW-File/Web server
1.1	Καθορισμένη πολιτική για την αντιμετώπιση ηθελημένης εισαγωγής κακόβουλου λογισμικού	HW-File/Web server
1.1.1	Η πολιτική να έχει κοινοποιηθεί σε όλο το προσωπικό	HW-File/Web server
1.2	Χρησιμοποίηση μόνο εγκεκριμένου λογισμικού από αξιόπιστους προμηθευτές	HW-File/Web server
1.3	Να εξασφαλιστεί ότι η πληροφόρηση σχετικά με την απειλή κακόβουλου λογισμικού, παρέχεται σε όλο το προσωπικό	HW-File/Web server
1.4	Ελαχιστοποίηση των συνδέσεων / πηγών των ανεξέλεγκτων λογισμικών και δεδομένων	HW-File/Web server

7.13.3 Προστασία ενάντια σε κακόβουλο λογισμικό (2/3)

Ομάδα Αντιμέτρων: Προστασία ενάντια σε κακόβουλο λογισμικό

Υποομάδα Αντιμέτρων: Ανίχνευση κακόβουλου λογισμικού

Άποψη Ασφαλείας: Λογισμικό

Δήλωση Πολιτικής: Το πληροφοριακό σύστημα θα πρέπει να παρακολουθείται για πιθανή δραστηριότητα κακόβουλου λογισμικού

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Το σύστημα θα πρέπει να παρακολουθείται για πιθανή δραστηριότητα κακόβουλου λογισμικού	HW-File/Web server
1.1	Εγκατάσταση λογισμικού για την ανίχνευση κακόβουλου λογισμικού	HW-File/Web server
1.1.1	Λογισμικό μόνιμης μνήμης	HW-File/Web server
1.1.2	Κρυπτογραφικό λογισμικό checksum	HW-File/Web server
1.2	Εκτέλεση λογισμικού ελέγχου κακόβουλου κώδικα	HW-File/Web server
1.2.1	Στην εκκίνηση του συστήματος	HW-File/Web server
1.2.2	Στην εκκίνηση κάθε εφαρμογής	HW-File/Web server
1.3	Έλεγχος όλων των εισερχόμενων λογισμικών και δεδομένων	HW-File/Web server
1.3.1	Εκτέλεση ελέγχου κακόβουλου λογισμικού στο σημείο εισόδου	HW-File/Web server
1.3.2	Εκτέλεση ελέγχου λογισμικού σε ξεχωριστό μηχάνημα	HW-File/Web server
1.4	Συχνή αναβάθμιση του λογισμικού ανίχνευσης	HW-File/Web server
1.4.1	Το λιγότερο κάθε χρόνο	HW-File/Web server
1.4.2	Το λιγότερο κάθε έξι μήνες	HW-File/Web server

7.13.4 Προστασία ενάντια σε κακόβουλο λογισμικό (3/3)

Ομάδα Αντιμέτρων: Προστασία ενάντια σε κακόβουλο λογισμικό

Υποομάδα Αντιμέτρων: Απομάκρυνση κακόβουλου λογισμικού

Άποψη Ασφαλείας: Διαδικαστικό

Δήλωση Πολιτικής: Το πληροφοριακό σύστημα θα πρέπει να παρακολουθείται για πιθανή δραστηριότητα κακόβουλου λογισμικού

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Το κακόβουλο λογισμικό θα πρέπει να προσδιοριστεί, να απομονωθεί και να απομακρυνθεί	HW-File/Web server
1.1	Διαδικασίες που περιγράφουν τα κατάλληλα μέτρα για την αντιμετώπιση της μόλυνσης με κακόβουλο λογισμικό	HW-File/Web server
1.1.1	Παύση τρέχουσας δραστηριότητας	HW-File/Web server
1.1.2	Απομόνωση μηχανήματος	HW-File/Web server
1.1.3	Ενημέρωση κατάλληλου προσωπικού	HW-File/Web server
1.1.4	Προσδιορισμός προβλήματος / κακόβουλου λογισμικού	HW-File/Web server
1.1.5	Απομάκρυνση κακόβουλου λογισμικού	HW-File/Web server
1.1.6	Επαναφορά συστήματος	HW-File/Web server
1.1.7	Προσδιορισμός αιτίας μόλυνσης	HW-File/Web server
1.2	Διατήρηση των πρωτοτύπων όλων των εγκεκριμένων λογισμικών σε ασφαλές σημείο	HW-File/Web server
1.3	Διατήρηση τακτικού αντιγράφου ασφαλείας όλων των δεδομένων	HW-File/Web server
1.3.1	Διατήρηση παλαιότερων αντιγράφων ασφαλείας	HW-File/Web server
1.3.2	Έλεγχος των αντιγράφων ασφαλείας για κακόβουλο λογισμικό πριν την επαναφορά συστήματος	HW-File/Web server
1.4	Παροχή εκπαίδευσης στο αρμόδιο προσωπικό για την ανίχνευση και απομάκρυνση κακόβουλου λογισμικού	HW-File/Web server

7.13.5 Ακεραιότητα λογισμικού

Ομάδα Αντιμέτρων: Ακεραιότητα λογισμικού
Υποομάδα Αντιμέτρων: Έλεγχοι ακεραιότητας λογισμικού
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Η ακεραιότητα του λογισμικού θα πρέπει να διατηρηθεί την ώρα που χρησιμοποιείται

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Παραβιάσεις της ακεραιότητας του λογισμικού θα πρέπει να ανιχνευθούν και να αποτραπούν	SRV-DMS , SW-BCT, SW-Prophix
1.1	Το Configuration Management (χειροκίνητο ή αυτόματο), οφείλει να διασφαλίζει ότι το σύστημα ελέγχεται για λογισμικό χωρίς άδεια (unauthorized)	SRV-DMS , SW-BCT, SW-Prophix
1.2	Να παρέχεται χειροκίνητος μηχανισμός ελέγχου ακεραιότητας για τη διασφάλιση της ακεραιότητας του λογισμικού	SRV-DMS , SW-BCT, SW-Prophix
1.2.1	Εκθέσεις που να προβάλλουν τα προβλήματα, συμπεριλαμβανομένων των ανησυχιών σχετικά με τα προνόμια του λογισμικού και των δεδομένων	SRV-DMS , SW-BCT, SW-Prophix

7.13.6 Επιλογές ανάκτησης για τη στέγαση

Ομάδα Αντιμέτρων: Επιλογές ανάκτησης για τη στέγαση
Υποομάδα Αντιμέτρων: Ανάκτηση στέγασης
Άποψη Ασφαλείας: Φυσικό
Δήλωση Πολιτικής: Η στέγαση πρέπει να είναι διαθέσιμη όταν απαιτείται

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Εντοπισμός και παρακολούθηση των stand-by καταλυμάτων	LOC - 4th floor, LOC – Ktirio
1.1	Η εσωτερική περιουσία ελέγχεται από τον οργανισμό	LOC - 4th floor, LOC – Ktirio
1.1.1	Μέσω του τμήματος περιουσίας	LOC - 4th floor, LOC – Ktirio
1.2	Εξωτερική περιουσία	LOC - 4th floor, LOC – Ktirio
1.2.1	Μέσω εμπορικών αντιπροσώπων περιουσίας	LOC - 4th floor, LOC – Ktirio

7.13.7 Φυσική ασφάλεια δωματίου/ζώνης

Ομάδα Αντιμέτρων: Φυσική ασφάλεια δωματίου/ζώνης
Υποομάδα Αντιμέτρων: Σχέδιο δωματίου
Άποψη Ασφαλείας: Φυσικό
Δήλωση Πολιτικής: Η αίθουσα θα πρέπει να σχεδιαστεί ώστε να μειωθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης. Το επίπεδο προστασίας που προσφέρεται από ένα δωμάτιο εξαρτάται από την ισχύ και τη δομή των τοίχων, δαπέδου και οροφής

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Η αίθουσα θα πρέπει να προσφέρει ένα βαθμό προστασίας, στο περιεχόμενό της, όταν αφήνεται αφύλακτη	LOC – Computer Room
1.1	Το δωμάτιο θα πρέπει να μπορεί να κλειδώνεται όταν παραμείνει αφύλακτο	LOC – Computer Room
2	Η κλειδαριά στην πόρτα του δωματίου θα πρέπει να παρέχει ένα μέτριο βαθμό αντοχής σε μη εξουσιοδοτημένο άνοιγμα	LOC – Computer Room
2.1	Το κλείδωμα που υπάρχει στην πόρτα θα πρέπει να εφαρμόζει καλά	LOC – Computer Room
2.2	Η πόρτα θα πρέπει να ανοίγει δύσκολα σε βίαιο άνοιγμα	LOC – Computer Room
2.2.1	Οι κλειδαριές που μπαίνουν σε υποδοχή ξύλου, δε θα πρέπει να εφαρμόζουν σε πόρτες πάχους μικρότερο των 44mm	LOC – Computer Room
2.3	Η κλειδαριά στην πόρτα να είναι κυλινδρικού τύπου κλειδαριά	LOC – Computer Room
2.4	Η κλειδαριά στην πόρτα να είναι τύπου υποδοχής σε ξύλο	LOC – Computer Room

7.13.8 Προστασία από πυρκαγιά (1/2)

Ομάδα Αντιμέτρων: Προστασία από πυρκαγιά
Υποομάδα Αντιμέτρων: Αποτροπή πυρκαγιάς
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Τα μέτρα θα πρέπει να είναι σε θέση να αποτρέψουν μια πυρκαγιά που συμβαίνει εκείνη τη στιγμή

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Πρέπει να υπάρχει πρόγραμμα πρόληψης πυρκαγιών στη θέση του	LOC – Ktirio
1.1	Πρέπει να υπάρχει εμφανές πιστοποιητικό πυρκαγιάς σε ισχύ	LOC – Ktirio
1.2	Πρέπει να υπάρχει καθορισμένος υπεύθυνος πρόληψης πυρκαγιών	LOC – Ktirio
1.3	Κάθε στοιχείο του εξοπλισμού πρέπει να προστατεύεται με κατάλληλη ασφάλεια ή αυτόματο διακόπτη	LOC – Ktirio
1.3.1	Για τον εξοπλισμό που χρησιμοποιεί 13 amp socket outlets	LOC – Ktirio
1.4	Εφαρμογή πολιτικής απαγόρευσης καπνίσματος	LOC – Ktirio
1.4.1	Απαγορευμένες ζώνες καπνίσματος	LOC – Ktirio
1.4.2	Απαγόρευση του καπνίσματος	LOC – Ktirio
1.5	Τα εύφλεκτα υλικά θα πρέπει να αφαιρούνται κάθε βδομάδα από τις κρίσιμες περιοχές	LOC – Ktirio
1.5.1	Απορρίμματα χαρτιού	LOC – Ktirio
1.5.2	Ρευστό toner	LOC – Ktirio
1.5.3	Κύλινδροι αερίου	LOC – Ktirio
1.6	Εύφλεκτα υλικά δεν πρέπει να αποθηκεύονται σε κρίσιμες περιοχές	LOC – Ktirio
1.6.1	Περιοχές που περιέχουν εξοπλισμό ο οποίος χειρίζεται βασικές επιχειρησιακές διαδικασίες, ή να είναι δαπανηρές	LOC – Ktirio

7.13.9 Προστασία από πυρκαγιά (2/2)

Ομάδα Αντιμέτρων: Προστασία από πυρκαγιά
Υποομάδα Αντιμέτρων: Καταστολή και έλεγχος
Άποψη Ασφαλείας: Φυσικό
Δήλωση Πολιτικής: Τα μέτρα θα πρέπει να είναι σε θέση να εξασφαλίσουν ότι εάν ξεσπάσει μια πυρκαγιά, μπορεί να ελεγχθεί

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Πρέπει να εφαρμόζονται φυσικά μέτρα για τον περιορισμό της εξάπλωσης της φωτιάς	LOC –4th floor
1.1	Οι πυρίμαχες πόρτες πρέπει να παραμένουν κλειστές	LOC –4th floor
1.2	Δημιουργία κάτοψης πυροσβεστικό εξοπλισμό και εξόδων κινδύνου πυρκαγιάς	LOC –4th floor
1.3	Επονομασμένο προσωπικό που θα εκπαιδευτεί στη χρήση της πυρόσβεσης και της προστασίας	LOC –4th floor
1.4	Οι συναγερμοί πρέπει να ακούγονται	LOC –4th floor
1.4.1	Συναγερμοί καπνού	LOC –4th floor
1.4.2	Συναγερμοί φωτιάς	LOC –4th floor
1.5	Παροχή εξοπλισμού καταστολής φωτιάς	LOC –4th floor
1.5.1	Πυροσβεστήρες	LOC –4th floor
1.5.2	Κουβέρτες φωτιάς	LOC –4th floor
1.6	Τα έπιπλα πρέπει να είναι ανεκτικά στη φωτιά	LOC –4th floor
1.6.1	Καρέκλες	LOC – Computer Room, LOC - Offices
1.6.2	Γραφεία	LOC – Computer Room, LOC - Offices
1.6.3	Κάδοι απορριμμάτων	LOC – Computer Room, LOC - Offices
1.7	Εγκατάσταση θυρών πυρασφάλειας και διαχωριστικά	LOC – Computer Room, LOC - Offices
1.7.1	Ανθεκτικά στη θερμότητα για 30 λεπτά	LOC – Computer Room, LOC - Offices
1.7.2	Ανθεκτικά στη θερμότητα για 30 λεπτά	LOC – Computer Room, LOC - Offices
1.8	Διατήρηση ενημερωμένης λίστας ατόμων που διαθέτουν κλειδιά, κατατεθειμένη στην αστυνομία	LOC –4th floor
1.8.1	Για το κτίριο που δεν είναι συνεχώς επανδρωμένο	LOC –4th floor
1.9	Οι έξοδοι των κλιματιστικών, δεν πρέπει να είναι τοποθετημένοι στους διαδρόμους	LOC –4th floor

7.13.10 Ασφάλιση

Ομάδα Αντιμέτρων: Ασφάλιση
Υποομάδα Αντιμέτρων: Ασφάλιση ακινήτων
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Οι ιδιοκτησίες θα πρέπει να ασφαλίζονται έναντι απώλειας ή ζημιάς. Σε κυβερνητικές υπηρεσίες / οργανισμούς η απόφαση μπορεί να ληφθεί για «προσωπική ασφάλιση». Στην περίπτωση αυτή οι έλεγχοι αυτοί δεν μπορούν να εφαρμόζονται

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Οι ιδιοκτησίες θα πρέπει να ασφαλίζονται έναντι απώλειας ή ζημιάς	LOC - 4th floor
1.1	Πολιτική ασφάλισης ακινήτων για την κάλυψη της ανησυχίας απειλών	LOC - 4th floor
1.1.1	Πολιτική ασφάλισης ακινήτων για την κάλυψη καταστροφής από πυρκαγιά	LOC - 4th floor
1.1.2	Πολιτική ασφάλισης ακινήτων για την κάλυψη καταστροφής από πλημύρα	LOC - 4th floor
1.1.3	Πολιτική ασφάλισης ακινήτων για την κάλυψη από φυσικές καταστροφές	LOC - 4th floor
1.1.4	Πολιτική ασφάλισης ακινήτων για την κάλυψη από δράση τρομοκρατών	LOC - 4th floor
1.2	Πολιτική ασφάλισης ακινήτων για την κάλυψη του κόστους ανακατασκευής του ακινήτου μετά από ένα περιστατικό	LOC - 4th floor
1.3	Πολιτική ασφάλισης ακινήτων για την κάλυψη του κόστους προσωρινής στέγασης που απαιτείται μετά από ένα περιστατικό	LOC - 4th floor
1.4	Πολιτική ασφάλισης ακινήτων για την κάλυψη επακόλουθων ζημιών που προκύπτουν από απώλεια ή ζημιά στην περιουσία	LOC - 4th floor

7.13.11 Έλεγχοι ανάπτυξης εφαρμογών (1/2)

Ομάδα Αντιμέτρων: Έλεγχοι ανάπτυξης εφαρμογών
Υποομάδα Αντιμέτρων: Αποτυχία ανάκτησης
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Η ανάπτυξη των εφαρμογών θα πρέπει να διενεργείται κατά τέτοιο τρόπο ώστε να είναι δυνατή η ανάκτηση, σε περίπτωση οποιουδήποτε προβλήματος

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Το σύστημα θα πρέπει να διευκολύνει την ανάκτηση, εάν παρουσιαστούν προβλήματα	SW – BCT, SW - Prophix
1.1	Διαδικασίες λήψης αντιγράφων ασφαλείας για τις βιβλιοθήκες των προγραμμάτων	SW – BCT, SW - Prophix
1.2	Παροχή δυνατότητας να επανέλθει το σύστημα σε μια προηγούμενη έκδοση του λογισμικού	SW – BCT, SW - Prophix

7.13.12 Έλεγχοι ανάπτυξης εφαρμογών (2/2)

Ομάδα Αντιμέτρων: Έλεγχοι ανάπτυξης εφαρμογών
Υποομάδα Αντιμέτρων: Διαδικασίες προσωπικού
Άποψη Ασφαλείας: Διαδικαστικό
Δήλωση Πολιτικής: Οι προγραμματιστές εφαρμογών θα πρέπει να ελέγχονται από κατάλληλες διαδικασίες προσωπικού

No	Περιγραφή αντιμέτρου	Αγαθό
1.	Οι διαδικασίες προσωπικού θα πρέπει να υποστηρίζουν το κατάλληλο περιβάλλον ανάπτυξης	SW – BCT, SW - Prophix
1.1	Διαχωρισμός καθηκόντων	SW – BCT, SW - Prophix
1.1.1	Να παρεμποδίζονται οι προγραμματιστές από το να ενημερώνουν live αρχεία – δεδομένα	SW – BCT, SW - Prophix
1.1.2	Να παρεμποδίζονται οι προγραμματιστές από το να εκκινούν λογιστικές συναλλαγές	SW – BCT, SW – Prophix
1.1.3	Να παρεμποδίζονται οι προγραμματιστές από το να έχουν πρόσβαση σε προσωπικά / ευαίσθητα live δεδομένα	SW – BCT, SW - Prophix
1.2	Οι προγραμματιστές να λαμβάνουν επίσημη εκπαίδευση για όλες τις πτυχές του ρόλου τους, ιδιαίτερα σε νέες τεχνικές	SW – BCT, SW - Prophix
1.2.1	EDI (Electronic Data Interchange), συστήματα Knowledge-based, αντικειμενοστραφείς γλώσσες	SW – BCT, SW - Prophix

8 Συμπεράσματα – Παρατηρήσεις

Με την ολοκλήρωση της μελέτης και την εξαγωγή των αποτελεσμάτων από τη μεθοδολογία CRAMM, μπορούν να εξαχθούν κάποια συμπεράσματα για το ΠΣ της εταιρίας NEC. Όπως φάνηκε στα αποτελέσματα της ανάλυσης επικινδυνότητας, το υπό μελέτη ΠΣ έχει απειλές, αδυναμίες και υψηλό ρίσκο επικινδυνότητας σε ορισμένα αγαθά, που μπορεί να είναι δεδομένα, υπηρεσίες ή υλικό. Η αναφορά αντιμέτρων, μέσα από πολλές προτάσεις για την αντιμετώπιση των προβλημάτων, προσπαθεί να καλύψει όλες αυτές τις αδυναμίες και απειλές που είναι ικανές να βλάψουν το ΠΣ.

Η απειλή της διείσδυσης στις επικοινωνίες παρουσιάζεται πολύ υψηλή με την υπηρεσία του Document Management Service να είναι εξίσου πολύ υψηλή. Η αντίστοιχη αδυναμία της συγκεκριμένης υπηρεσίας φαίνεται πως είναι μέτρια, όπως και των υπολοίπων υπηρεσιών με βάση την ίδια απειλή.

Στην απειλή της υποκλοπής των επικοινωνιών, η CRAMM υπολογίζει την απειλή πολύ υψηλή στην ενότητα της απόκρυψης. Η υπηρεσία Document Management Service παρουσιάζει πολύ υψηλή απειλή με την αντίστοιχη ευπάθεια να είναι χαρακτηρισμένη ως μέτρια. Οι υπόλοιπες υπηρεσίες κυμαίνονται στα ίδια επίπεδα ευπάθειας και απειλής.

Η απειλή της παραποίησης των επικοινωνιών παρουσιάζεται πολύ υψηλή τόσο στον τομέα της αποκάλυψης και τη όσο και της παραποίησης, όσο και στο αντίκτυπο των επικοινωνιών. Η υπηρεσία Document Management Service παραμένει σε επίπεδο πολύ υψηλό, όχι όμως και η ευπάθειά της που χαρακτηρίζεται μέτρια.

Στην τεχνική βλάβη στοιχείου δικτύου η μη διαθεσιμότητα χαρακτηρίζεται με υψηλή απειλή, όπως και η επίδραση στις επικοινωνίες. Υψηλή απειλή παίρνει και το δίκτυο σαν αγαθό του ΠΣ, με την ευπάθεια να είναι μέτρια.

Η αποτυχία λογισμικού στο σύστημα και στο δίκτυο χαρακτηρίζεται από υψηλή απειλή σε όλες τις κατηγορίες για τις οποίες αξιολογήθηκε. Τα αγαθά που πήραν το χαρακτηρισμό της υψηλής απειλής είναι ο File/Web server, τα workstations και το δίκτυο. Χαρακτηριστικό είναι πως η αδυναμία των συγκεκριμένων αγαθών χαρακτηρίστηκε υψηλή.

Η αποτυχία εφαρμογών λογισμικού παίρνει το χαρακτηρισμό της υψηλής απειλής σε όλα τα πεδία – κατηγορίες στις οποίες εξετάστηκε. Το δίκτυο και το λογισμικό χαρακτηρίστηκαν με την ένδειξη πολύ υψηλής απειλής.

Τέλος, σφάλμα χειρισμών παρουσιάζουν με υψηλή απειλή, ο File/Web server και το δίκτυο. Υψηλή απειλή αξιολογήθηκαν στη μη διαθεσιμότητα, στην αποκάλυψη, στην παραποίηση και στην επίδραση στις επικοινωνίες.

Σε γενικά πλαίσια, το ΠΣ της εταιρίας NEC, είναι ένα ασφαλές ΠΣ, προστατευόμενο από πολλών ειδών απειλές, είτε αυτές είναι ανθρώπινος παράγοντας, είτε φυσικό φαινόμενο. Οι αδυναμίες που παρουσιάζει δεν είναι σε θέση να το καταστήσουν εξαιρετικά ευάλωτο, ενώ το ποσοστό των απειλών που μπορεί να είναι επιβλαβείς παραμένει σε χαμηλά επίπεδα. Υπάρχουν περιθώρια βελτίωσης, προκειμένου να αυξηθεί η ασφάλειά του και να μειωθεί ο βαθμός επικινδυνότητας των απειλών. Οι προτάσεις των αντιμέτρων, που παρουσιάζει η αναφορά αντιμέτρων, είναι ικανές να μειώσουν αυτόν το βαθμό.

9 Πηγές – Αναφορές

[1]. **Σωκράτης Κάτσικας, Ανοιχτό Πανεπιστήμιο:** "Ασφάλεια Υπολογιστών", Τόμος Α' , 2001

[2]. **Σπύρος Κοκολάκης, Εκδόσεις Νέων Τεχνολογιών:** "Ασφάλεια Πληροφοριακών Συστημάτων", 2004

[3]. **Δ. Πολέμη:** "Διαχείριση Επικινδυνότητας Πολιτική Ασφάλειας", 2003

[4]. **©Crown Copyright:** "Cramm User Guide", Issue 5.1, July 2005

[5]. **SANS Institute:** "A Qualitative Risk Analysis and Management Tool – CRAMM", 2002

[6]. **Σωκράτης Κάτσικας, Πανεπιστήμιο Πειραιά:** "Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων"

[7]. **Νικήτας Γεώργιος, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης:** "Ανάλυση κινδύνων Πληροφοριακών Συστημάτων", 2004

[8]. **Δοκοπούλου Ιωάννα Πολυξένη:** "Αποτίμηση των παγίων και της εγκατάστασης για το ολοκληρωμένο πληροφοριακό σύστημα του Πανεπιστημίου Πειραιά – Τμήμα Ψηφιακών Συστημάτων", 2009

[9]. **Σπύρος Κοκολάκης, Πανεπιστήμιο Σάμου:** "Ανάλυση, αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"

[10]. **Ρεκλείτης Ευάγγελος, Πανεπιστήμιο Πειραιά:** "Πρακτικός οδηγός του εργαλείου ασφάλειας CRAMM"