Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Σχεδίαση και υλοποίηση μεθοδολογιών διαχείρισης ασφάλειας πληροφοριακών συστημάτων** Design and Development of Information Systems Risk Assessment Methodologies
Ονοματεπώνυμο Φοιτητή	**Γεώργιος Ευαγγελιάς**
Πατρώνυμο	**Απόστολος**
Αριθμός Μητρώου	**ΜΠΣΠ 14024**
Επιβλέπων	**Δουληγέρης Χρήστος**, **Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος** 2017

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Μιχαήλ Ψαράκης Επίκουρος Καθηγητής	Παναγιώτης Κοτζανικολάου Επίκουρος Καθηγητής

ΕΥΧΑΡΙΣΤΙΕΣ

Μετά το πέρας της Μεταπτυχιακής Διατριβής, νιώθω την ανάγκη να εκφράσω τη βαθιά και ειλικρινή μου ευγνωμοσύνη για τα πρόσωπα που με βοήθησαν στην εκπόνηση της.

Αρχικά θα ήθελα να ευχαριστήσω τον Καθηγητή του Πανεπιστημίου Πειραιώς και επιβλέποντα της διατριβής κ. Δουληγέρη Χρήστο για την πολύτιμη βοήθεια και αγόγγυστη συμπαράσταση καθ' όλη τη διάρκεια της εκπόνησής της.

Ταυτόχρονα, εκφράζω τις ευχαριστίες μου προς τον υποψήφιο Διδάκτορα του Πανεπιστημίου Πειραιώς Μακροδημήτρη Γεώργιο, του οποίου η συμβολή ήταν καταλυτική και καθοριστική για τη διεξαγωγή και ολοκλήρωση του ερευνητικού μέρους της παρούσας διατριβής.

Τέλος, οφείλω να εκφράσω την ειλικρινή μου ευγνωμοσύνη προς όλα εκείνα τα πρόσωπα που στάθηκαν στο πλευρό μου καθ' όλη τη διάρκεια αυτής της δύσκολης περιόδου και με ενίσχυσαν ποικιλοτρόπως στην αντιμετώπιση αυτής της πρόκλησης που ονομάζεται 'Μεταπτυχιακή Διατριβή'.

ΠΕΡΙΛΗΨΗ

Το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων ήταν -από γενέσεως πληροφορικής- πάντα κρίσιμο. Αναμφισβήτητα, σήμερα ο κίνδυνος είναι πιο συνειδητός, καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων. Η πληροφορία, οποιαδήποτε κι αν είναι η μορφή της, εφόσον είναι σημαντική απαιτείται να διαφυλάσσεται κατάλληλα και να είναι σωστά προστατευμένη. Αυτός είναι ο απώτερος σκοπός της ασφάλειας πληροφοριών: να προστατεύει την πληροφορία από ένα ευρύ φάσμα απειλών παρέχοντας εξασφάλιση στην επιχειρηματική κοινωνία, ελαχιστοποιώντας τη ζημία των επιχειρήσεων και αυξάνοντας το κέρδος από επενδύσεις και επιχειρηματικές ευκαιρίες. Η ασφάλεια των συστημάτων και των δεδομένων τους ορίζεται σε τρεις άξονες: διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα.

Τα τελευταία χρόνια παρατηρείται ότι η αξία των περιουσιακών στοιχείων μιας εταιρείας προέρχεται κυρίως από άυλα στοιχεία. Αναπόφευκτα, η εξάρτηση πάνω στα πληροφοριακά συστήματα και υπηρεσίες σημαίνει ότι οι οργανισμοί είναι πιο ευάλωτοι στις απειλές ασφάλειας. Τα δεδομένα, οι πληροφορίες, οι υποστηρικτικές διαδικασίες, τα συστήματα και τα δίκτυα είναι σημαντικά επιχειρηματικά αγαθά, οπότε διαφυλάσσοντας τα μία εταιρεία μπορεί να αποφύγει ανυπολόγιστα προβλήματα τα οποία ενδέχεται να προκύψουν. Η αλματώδης ανάπτυξη και αύξηση των εταιρειών, έχει ως συνέπεια να γίνονται πιο “ θελκτικός ” στόχος, άρα τα συστήματα πληροφοριών και τα δίκτυα τους να έχουν να αντιμετωπίσουν απειλές από ένα ευρύ φάσμα πηγών, περιλαμβάνοντας computer-assisted fraud, espionage, sabotage, βανδαλισμό, φωτιά ή πλημμύρα. Πηγές ζημιάς, όπως ιοί υπολογιστών και computer hacking έχουν γίνει ολοένα και πιο συχνοί, πιο φιλόδοξοι και εντυπωσιακά ειδικευμένοι. Αντιλαμβανόμαστε λοιπόν την σπουδαιότητα που πρέπει να έχει η ασφάλεια των πληροφοριών σε μία επιχείρηση.

Στην παρούσα μεταπτυχιακή διατριβή, γίνεται παρουσίαση μερικών από των πιο γνωστών και διεθνώς αποδεκτών μεθόδων ανάλυσης επικινδυνότητας και στη συνέχεια επιχειρείται μια αναλυτική σύγκριση των αποτελεσμάτων που προκύπτουν μεταξύ των CRAMM, MAGERIT και MEHARI για το επιλεγμένο σενάριο προσομοίωσης ενός χρηματοπιστωτικού οργανισμού που αποτελεί κρίσιμή υποδομή με στόχο την εύρεση της κατάλληλης μεθοδολογίας για την υλοποίηση ανάλυσης επικινδυνότητας σε αυτόν, όπως απαιτείται από τα διεθνή πρότυπα τα οποία διέπουν την λειτουργία αυτού.

ABSTRACT

The problem of the security of information systems has always been critical from computer science. Undoubtedly, today the risk is more conscious, as the systems are exposed to a wide range of users and hence risks. Information, whatever its form, if it is important, needs to be properly protected. This is the ultimate goal of information security: to protect information from a wide range of threats by providing security to the business community, minimizing business damage and increasing profit from investment and business opportunities. The security of their systems and data is defined in three axes: availability, confidentiality, integrity.

In the last few years, has been observed that the value of a company's assets comes mainly from intangibles. Inevitably, dependence on information systems and services means that organizations are more vulnerable to security threats. Data, information, support processes, systems and networks are important business assets, so preserving one company can avoid immeasurable problems that may arise. The rapid growth and growth of companies has resulted in a more "attractive" target, so their information systems and networks have to deal with threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses and computer hacking have become increasingly common, more ambitious and impressively skilled. So, we understand the importance of information security in an enterprise.

In this dissertation, are presented some of the most well-known and internationally accepted methods of risk analysis and a detailed comparison of the results between CRAMM, MAGERIT and MEHARI is made for the selected simulation scenario of a financial institution that is a critical infrastructure, in order to find the appropriate methodology for carrying out a risk analysis on it, as required by the international standards regarding information security.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

ΕΥΡΕΤΗΡΙΟ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ

Η απόκριση σε περίπτωση γεγονότων ασφαλείας ηλεκτρονικού υπολογιστή αποτελεί ζωτική συνιστώσα του σύγχρονου περιβάλλοντος πληροφορικής, καθώς οι επιθέσεις που σχετίζονται με την ασφάλεια στον κυβερνοχώρο είναι πολυάριθμες και ποικίλες, με καταστροφικές συνέπειες. Διάφορα είδη συμβάντων που σχετίζονται με την ασφάλεια εμφανίζονται συχνά, οι προληπτικές δραστηριότητες με βάση τα αποτελέσματα των αξιολογήσεων κινδύνου μπορούν να μειώσουν τον αριθμό των περιστατικών, ωστόσο, δεν μπορούν να προληφθούν όλα τα περιστατικά. Ως εκ τούτου, είναι απαραίτητη η ικανότητα αντιμετώπισης περιστατικών για την ταχεία ανίχνευση περιστατικών, την ελαχιστοποίηση των απωλειών και καταστροφών, την άμβλυνση των αδυναμιών που εκμεταλλεύθηκαν και την αποκατάσταση των υπηρεσιών πληροφορικής. Οι αποτελεσματικές κατευθυντήριες γραμμές για τον χειρισμό περιστατικών, ιδίως για την ανάλυση των δεδομένων που σχετίζονται με τα περιστατικά και τον καθορισμό της κατάλληλης απάντησης σε κάθε περιστατικό, έχουν καταστεί πλέον επιτακτικοί στον τομέα της τεχνολογίας της πληροφορίας. Καθώς, μια αποτελεσματική αντιμετώπιση των περιστατικών είναι ένα σύνθετο καθήκον, η καθιέρωση επιτυχών διαδικασιών αντιμετώπισης περιστατικών απαιτεί ουσιαστικό σχεδιασμό και πόρους. Οι οδηγίες πρέπει να είναι διαλειτουργικές σε διάφορες πλατφόρμες υλικού, λειτουργικά συστήματα, πρωτόκολλα ή εφαρμογές. Η συνεχής παρακολούθηση της επίθεσης είναι απαραίτητη και ο καθορισμός ξεχωριστών διαδικασιών για την ιεράρχηση του χειρισμού των περιστατικών είναι ζωτικής σημασίας. Είναι, επίσης, σημαντικό να δημιουργηθούν σχέσεις και να δημιουργηθούν κατάλληλα μέσα επικοινωνίας με εσωτερικές ομάδες (ανθρώπινοι πόροι, νομικές) και εξωτερικές ομάδες (άλλες ομάδες αντιμετώπισης περιστατικών, επιβολή του νόμου).

Η εξέλιξη της τεχνολογίας των υπολογιστών τα τελευταία χρόνια είναι γρήγορη. Είναι παρόμοιο με το φαινόμενο των παρατηρούμενων επιθέσεων στον κυβερνοχώρο, οι οποίες γίνονται όλο και πιο συχνές στους χρήστες και στους οργανισμούς. Οι ηλεκτρονικές συναλλαγές και η συλλογή δεδομένων από κυβερνητικούς οργανισμούς, μεγάλες εταιρείες, τράπεζες και επιχειρήσεις αποτελούν τον πόλο έλξης για χάκερ για πρόσβαση ή κλοπή δεδομένων ή επίθεση σε ένα σύστημα πληροφοριών. Παρόλο που χρησιμοποιούνται ανεπτυγμένοι αλγόριθμοι και λογισμικό για την προστασία των συστημάτων πληροφοριών, κανείς δεν μπορεί να εγγυηθεί απόλυτη ασφάλεια. Τον τελευταίο καιρό παρατηρήθηκε μεγάλος αριθμός επιθέσεων στον κυβερνοχώρο, έγιναν τακτικές απόπειρες και διάπραξη επιθέσεων στον κυβερνοχώρο από οργανισμούς μικρής έως μεγάλης κυβέρνησης και ασφάλειας, νοσοκομεία κλπ. Σε όλο τον κόσμο, οι επιχειρήσεις αγωνίζονται να κατανοήσουν τα βήματα που πρέπει να λάβουν για να

προστατεύσουν τον εαυτό τους. Ορισμένες τρέχουσες τάσεις και αναδυόμενες τάσεις επίθεσης περιλαμβάνουν:

- Καταστροφικές επιθέσεις DDoS (distributed denial-of-service*)* IoT (Internet of Things): αυτές έχουν τεράστιο καταστρεπτικό δυναμικό λόγω των ανασφαλών συσκευών καταναλωτών IoT (Internet of Things). Αυτές οι επιθέσεις εκμεταλλεύονται μόνο ένα μικρό αριθμό συσκευών και ευπάθειες και χρησιμοποιούν βασικές τεχνικές ανίχνευσης κωδικού πρόσβασης.
- Στοχοθετημένες κοινωνικές επιθέσεις: Οι κυβερνοεγκληματίες γίνονται όλο και καλύτεροι στην εκμετάλλευση της τελικής ευπάθειας στους ανθρώπους, προκαλώντας τους χρήστες να υπονομεύσουν τον εαυτό τους. Είναι σύνηθες να βλέπετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που απευθύνεται στον παραλήπτη με το όνομα και ισχυρίζεται ότι έχει ένα ανεξόφλητο χρέος στον οποίο ο αποστολέας έχει εξουσιοδοτηθεί να συλλέξει.
- Η χρήση στοχευμένου phishing ("ψάρεμα") συνεχίζει να αυξάνεται με την οικονομική υποδομή να διατρέχει μεγαλύτερο κίνδυνο επίθεσης. Αυτές οι επιθέσεις χρησιμοποιούν λεπτομερείς πληροφορίες σχετικά με στελέχη της εταιρείας για να εξαπατήσουν τους υπαλλήλους να πληρώνουν απατεώνες ή να παίρνουν τον έλεγχο λογαριασμών. Η απειλή είναι πολύ επίμονη, προσαρμοστική και εξελιγμένη.
- Εκμετάλλευση της εγγενώς αβέβαιης υποδομής του Διαδικτύου: Όλοι οι χρήστες του Διαδικτύου βασίζονται σε αρχαία πρωτόκολλα και ως πανταχού παρόντα τους καθιστούν σχεδόν αδύνατο να ανανεωθούν ή να αντικατασταθούν. Αυτά τα αρχαϊκά πρωτόκολλα, τα οποία υπήρξαν μακράν η ραχοκοκαλιά του Διαδικτύου και των επιχειρηματικών δικτύων, είναι μερικές φορές εκπληκτικά ευάλωτα. Για παράδειγμα, οι επιθέσεις εναντίον του BGP (Border Gateway Protocol)
- Αυξημένη πολυπλοκότητα επίθεσης: Οι επιθέσεις συγκεντρώνουν ολοένα και περισσότερα τεχνικά και κοινωνικά στοιχεία και αντικατοπτρίζουν την προσεκτική και μακρά διερεύνηση του δικτύου του οργανισμού θύματος. Οι επιτιθέμενοι θέτουν σε κίνδυνο πολλούς διακομιστές και σταθμούς εργασίας πολύ πριν αρχίσουν να κλέβουν δεδομένα ή να ενεργούν επιθετικά.
- Επιθέσεις που χρησιμοποιούν ενσωματωμένες γλώσσες και εργαλεία διαχείρισης: αυτά είναι εκμεταλλεύσεις που βασίζονται στο PowerShell, γλώσσα της Microsoft για αυτοματοποίηση διοικητικών εργασιών κ.λπ. Υπάρχουν επίσης επιθέσεις που χρησιμοποιούν δοκιμές διείσδυσης και άλλα εργαλεία διαχείρισης που μπορεί ήδη να υπάρχουν στο δίκτυο.
- Το Ransomware εξελίσσεται: οι κίνδυνοι επίθεσης ransomware μέσω ηλεκτρονικού ταχυδρομείου καθίστανται όλο και πιο διαδεδομένοι, οι κυβερνοεγκληματίες διερευνούν και άλλους φορείς. Μερικοί πειραματίζονται με κακόβουλο λογισμικό που επανεμφανίζεται πολύ αργότερα, πολύ μετά την καταβολή λύτρων.
- Η εμφάνιση προσωπικών επιθέσεων IoT: Οι χρήστες οικιακών συσκευών IoT ενδέχεται να μην παρατηρήσουν ή και να προσέξουν αν τα μόνιτορ μωρών τους είναι διαβεβλημένα για να επιτεθούν στον ιστότοπο κάποιου άλλου. Αλλά μόλις οι εισβολείς κατέχουν μια συσκευή σε οικιακό δίκτυο, μπορούν να θέσουν σε κίνδυνο άλλες συσκευές, π.χ. φορητούς υπολογιστές που περιέχουν σημαντικά προσωπικά δεδομένα.
- Η αύξηση της κακοποίησης και της διαφθοράς των διαδικτυακών οικοσυστημάτων διαφήμισης: Το Malvertising, το οποία εξαπλώνει κακόβουλα προγράμματα μέσω διαδικτυακών διαφημιστικών δικτύων και ιστοσελίδων, βρίσκεται εδώ και χρόνια, αλλά συνεχίζει να αναπτύσσεται. Αυτές οι επιθέσεις υπογραμμίζουν μεγαλύτερα προβλήματα σε όλο το διαφημιστικό οικοσύστημα
- Το μειονέκτημα της κρυπτογράφησης: Καθώς η κρυπτογράφηση καθίσταται πανταχού παρούσα, είναι πολύ πιο δύσκολο για τα προϊόντα ασφαλείας να επιθεωρούν την κυκλοφορία, καθιστώντας ευκολότερο για τους εγκληματίες να γλιστρήσουν μέσω ανιχνεύσεων. Δεν αποτελεί έκπληξη το

γεγονός ότι οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν κρυπτογράφηση με δημιουργικούς νέους τρόπους.

- Αύξηση της εστίασης στις εκμεταλλεύσεις εναντίον των εικονικών συστημάτων και του cloud: Οι επιθέσεις κατά φυσικών συστημάτων αυξάνουν την πιθανότητα επικίνδυνων νέων εκμεταλλεύσεων ενάντια στα εικονικά συστήματα στο cloud.
- Τεχνικές επιθέσεις εναντίον κρατών και κοινωνιών: Οι επιθέσεις που βασίζονται στην τεχνολογία έχουν γίνει ολοένα και πιο πολιτικές. Οι κοινωνίες αντιμετωπίζουν αυξανόμενους κινδύνους τόσο από παραπληροφόρηση (π.χ. ψεύτικα νέα) όσο και από διαβολές στο σύστημα ψηφοφορίας.

Οφέλη οι οργανισμοί ορθώς θεωρούν τις πληροφορίες που χειρίζονται, επεξεργάζονται και αποθηκεύονται από τις υπηρεσίες e/m τους ως περιουσιακό στοιχείο που μοιάζει με οποιοδήποτε άλλο επιχειρηματικό περιουσιακό στοιχείο, πρέπει να διαχειρίζεται στρατηγικά και να προστατεύεται. Η προστασία των πληροφοριακών περιουσιακών στοιχείων προσφέρει τα εξής:

- *Όφελος # 1:*

"Βελτίωση της ανταγωνιστικότητας των οργανισμών". Οι επιχειρήσεις θα προσφέρουν υπηρεσίες ασφάλειας και προστασίας της ιδιωτικής ζωής που θα υποστηρίζουν την τήρηση νομικών και κανονιστικών πλαισίων και προτύπων, γεγονός που αποτελεί προϋπόθεση για μια εμπιστευτική ψηφιακή ευρωπαϊκή οικονομία. Έτσι, μπορούν να ενισχύσουν την εταιρική τους φήμη κερδίζοντας την εμπιστοσύνη των πελατών τους, ενισχύοντας την ασφάλεια και το επίπεδο προστασίας προσωπικών δεδομένων των ηλεκτρονικών/ψηφιακών υπηρεσιών τους· να αυξήσουν την αειφορία των επιχειρησιακών διεργασιών τους και να βελτιώσουν την ανταγωνιστικότητά τους.

- *Όφελος # 2:*

"Δυνατότητα οι οργανώσεις να αυξήσουν τις αγορές τους και να επεκτείνουν / διεθνοποιήσουν τις επιχειρηματικές τους δραστηριότητες σε πρακτικές λεπτομέρειες". Η συμμόρφωση με επιβαλλόμενα νομικά και ρυθμιστικά πλαίσια, βέλτιστες πρακτικές και πρότυπα σε ολόκληρη την ΕΕ επιτρέπει στους οργανισμούς να κερδίσουν την εμπιστοσύνη των πελατών στην ψηφιακή ευρωπαϊκή οικονομία, απαιτώντας μέτρα διασφάλισης της ασφάλειας και ιδιωτικότητας, διευκολύνοντας έτσι τη διασυνοριακή επέκταση των επιχειρηματικών δραστηριοτήτων των επιχειρήσεων.

- *Όφελος # 3:*

"Δρόμους προς νέα και βελτιωμένα προϊόντα, διαδικασίες ή υπηρεσίες με σαφές δυναμικό αγοράς". Η παροχή ασφαλών πρωτοποριακών υπηρεσιών ηλεκτρονικού ταχυδρομείου B2B (Business-to-Business) ή B2C (Business-to-Costumer) που παρέχονται από ασφαλείς και υποστηριζόμενες από πλευράς απορρήτου διαδικασίες back-office θα επιτρέψει στους οργανισμούς να προσεγγίσουν ένα μεγαλύτερο, διασυνοριακό ακροατήριο, να προσελκύσουν περισσότερους πελάτες και έτσι να αποκτήσουν μεγαλύτερο μερίδιο αγοράς.

- *Όφελος # 4:*

"Προσκόλληση τις κανονιστικές απαιτήσεις και τους στόχους πολιτικής σε βασικούς τομείς". Συμβολή σε πολλούς στόχους και κατευθυντήριες γραμμές πολιτικής, με έμφαση στην ασφάλεια και ειδικότερα στην 1) Ευρώπη 2020, η οποία προωθεί (i) την έξυπνη ανάπτυξη μέσω της ανάπτυξης μιας οικονομίας βασισμένης στην καινοτομία και (ii) της αειφόρου ανάπτυξης που προωθεί μια πιο ανταγωνιστική οικονομία, διευκόλυνση της παροχής ασφαλών ηλεκτρονικών υπηρεσιών και 2) Ψηφιακό θεματολόγιο για την Ευρώπη, συμβάλλοντας στον πυλώνα I (διευκόλυνση μιας ασφαλούς ψηφιακής ηλεκτρονικής αγοράς), στον πυλώνα II (προώθηση της χρήσης προτύπων), στον πυλώνα VII μια αξιόπιστη κοινωνία της Ευρωπαϊκή Ένωση) και τον πυλώνα III (Ενίσχυση της εμπιστοσύνης και της ασφάλειας).

Όσον αφορά τον αντίκτυπό της ειδικά στις οργανώσεις και πιο συγκεκριμένα σε εκείνες που εκθέτουν δεδομένα στο διαδίκτυο και ανταλλάσσουν πληροφορίες είτε μέσω διαδικτύου είτε μέσω intranets -Ευρωπαϊκό επίπεδο, τα αναμενόμενα οφέλη για τις επιχειρήσεις είναι τα εξής:

(i) *Διαφοροποίηση της αγοράς:* Η συμμόρφωση των οργανισμών με ένα σύνολο νομικών, κανονιστικών και το πλαίσιο ασφάλειας τυποποίησης αποτελεί προϋπόθεση της συνεργασίας με άλλους οργανισμούς που θέτουν παρόμοιες απαιτήσεις ασφάλειας στους προμηθευτές τους

(ii) *Εφαρμογή στις ανάγκες του νέου επιχειρηματικού περιβάλλοντος:* Το επιχειρηματικό περιβάλλον έχει συνδεθεί ολοένα και περισσότερο με τα ιδιωτικά δεδομένα των πελατών να μοιράζονται ολοένα και περισσότερο σε όλη την αλυσίδα εφοδιασμού και να απαιτούν προστασία της ιδιωτικής ζωής και της ασφάλειας, με τρόπο εμπιστευτικό. Η υιοθέτηση και η εφαρμογή αυστηρών προσεγγίσεων ασφαλείας στην προστασία των δεδομένων των πελατών από τους οργανισμούς θα τους επιτρέψει να αντιμετωπίσουν το νέο επιχειρηματικό περιβάλλον.

(iii) *Προστασία της φήμης και βελτίωση της εικόνας:* Η υπεύθυνη και προοδευτική στάση της ασφάλειας των πληροφοριών και της προστασίας των πληροφοριών, συμπεριλαμβανομένης της προστασίας της ιδιωτικής ζωής των πελατών και των ιδιοκτησιακών πληροφοριών των ίδιων των επιχειρήσεων, προστατεύει τη φήμη και το εμπορικό σήμα τους.

(iv) *Μεγαλύτερα περιθώρια κέρδους και διατήρηση κερδοφορίας:* Αυξημένη ταχύτητα παραβίασης πληροφοριών σε δεδομένα ευαίσθητων πελατών λόγω ανεπαρκών προσεγγίσεων ασφαλείας εκ μέρους οργανισμών μπορεί να επηρεάσει αρνητικά τη χρηματιστηριακή τους αξία, μειώνοντας την εμπιστοσύνη των καταναλωτών και μειώνοντας τις πωλήσεις.

(v) *Πρόσθετη προσφορά υπηρεσιών/προϊόντων:* Η καλή διαχείριση της ασφάλειας αποτελεί προϋπόθεση για τη διατήρηση των υφιστάμενων προϊόντων και υπηρεσιών και τη δημιουργία νέων προϊόντων και υπηρεσιών.

(vi) *Μείωση των δαπανών παραβίασης της ασφάλειας:* Οι οργανώσεις που αντιμετωπίζουν παραβιάσεις της ασφάλειας ενδέχεται να βρίσκονται σε οικονομική δυσπραγία. Η παραβίαση μπορεί να προκαλέσει είτε άμεσες δαπάνες, όπως επιβληθέντα πρόστιμα από τις ρυθμιστικές αρχές ή τις αντισταθμιστικές πληρωμές στους πελάτες ή ακόμη και τις έμμεσες δαπάνες. Εκτός αυτού, το κόστος απόκρισης περιστατικών σχετίζεται με το χρόνο και τα χρήματα που απαιτούνται για την αποκατάσταση των πραγματικών περιστατικών. Με αυτόν τον τρόπο, οι οργανισμοί είναι σε θέση να εξοικονομήσουν ένα σημαντικό χρηματικό ποσό μακροπρόθεσμα για περαιτέρω επενδύσεις και οικονομική επέκταση.

Παρά το γεγονός ότι η ασφάλεια στον κυβερνοχώρο είναι ένα κρίσιμο ζήτημα στις μέρες μας, η γνώση των πραγματικών επιζήμιων επιπτώσεων μιας επίθεσης στον κυβερνοχώρο παραμένει σε μεγάλο βαθμό αναποτελεσματική. Έχει γίνει όλο και πιο επιτακτική η ανάγκη τόσο οι τμηματάρχες του IT όσο και οι διευθύνοντες σύμβουλοι των επιχειρήσεων να διαπιστώσουν τις οικονομικές και κοινωνικές επιπτώσεις αυτών των επιθέσεων στον κυβερνοχώρο. Η ακριβής απεικόνιση των επιπτώσεων στον κυβερνοχώρο θα επιτρέψει στις επιχειρήσεις να εντοπίσουν επαρκείς κινδύνους στον κυβερνοχώρο, να κατανοήσουν τι κινδυνεύει και να διαμορφώσουν καλύτερα τα προγράμματα για τον κυβερνοχώρο για να προστατεύσουν την κοινωνία γενικότερα, τα στρατηγικά συμφέροντα των οργανώσεών τους και τελικά να βελτιώσουν την ικανότητα του οργανισμού να ευδοκιμούν απέναντι στις επιθέσεις στον κυβερνοχώρο. Μια εις βάθος ανάλυση ορισμένων από τους πολλούς τρόπους που οι επιθέσεις στον κυβερνοχώρο έχουν επιπτώσεις στις κοινωνίες και στις επιχειρήσεις μας δείχνουν σαφώς ότι η ανάκαμψη των επιχειρήσεων μπορεί να είναι πολύ πιο δύσκολη, πιο πολύπλοκη και δαπανηρή από ό, τι φανταζόταν. Μετά την ανάλυση των επιχειρηματικών επιπτώσεων από την Deloitte Advisory, οι επιπτώσεις "πάνω από την επιφάνεια" και "κάτω από την επιφάνεια" μπορούν να απαριθμηθούν ως εξής. Οι πιο πάνω επιπτώσεις στην επιφάνεια είναι το γνωστό κόστος της επίπτωσης στον κυβερνοχώρο, όπως το κόστος που συνδέεται με: τις παραβιάσεις των πελατών, την προστασία των πελατών μετά την παραβίαση, την κανονιστική

συμμόρφωση (πρόστιμα), τις επικοινωνίες δημόσιων σχέσεων/κρίσεων, τις αμοιβές δικηγόρων και τις διαφορές, διερευνήσεις. Τα κάτω από το κόστος επιφάνειας περιλαμβάνουν αυξήσεις ασφαλίστρων, αυξημένο κόστος για τη συγκέντρωση χρεών, διακοπή λειτουργίας ή καταστροφή λειτουργίας, απώλεια αξίας σχέσεων με πελάτες, αξία απώλειας εσόδων από συμβάσεις, υποτίμηση εμπορικού ονόματος και απώλεια πνευματικής ιδιοκτησίας. Αρκετές μελέτες έχουν διαπιστώσει ότι το άμεσο κόστος που συνήθως συνδέεται με παραβιάσεις δεδομένων είναι πολύ λιγότερο σημαντικό για το κρυφό κόστος και η χρονική διάρκεια για την οποία γίνεται αισθητή η επίπτωση είναι αρκετά συχνά μεγαλύτερη από την αναμενόμενη. Ένα μεγάλο μέρος των επιπτώσεων στον κυβερνοχώρο ενδέχεται να εμπίπτει σε κατηγορίες που είναι άυλες και γνωρίζοντας ότι αυτές είναι λιγότερο μελετημένες και πιο δύσκολο να προσδιοριστούν ποσοτικά, οι οργανώσεις μπορούν να βρεθούν χωρίς να γνωρίζουν αυτές τις δαπάνες σε τομείς όπως η απώλεια της πνευματικής ιδιοκτησίας, στην εμπορική ονομασία. Με τα προαναφερθέντα, είναι επομένως σημαντικό να είναι δυνατή η ποσοτικοποίηση των άυλων ζημιών, προκειμένου να προβλεφθούν επαρκείς επιχειρηματικές επιπτώσεις.

Σε αυτό το σημείο εγείρεται το ερώτημα σχετικά με το ποιες διαδικασίες και ποιους μηχανισμούς πρέπει να ακολουθήσει μια επιχείρηση έτσι ώστε να εξασφαλίσει την ακεραιότητά της και να προστατέψει τα δεδομένα της. Σε θεωρητικό επίπεδο είναι κατανοητό ότι θα πρέπει να εφαρμοστούν έλεγχοι και διαδικασίες οι οποίες θα διασφαλίσουν την συνοχή των δεδομένων της επιχείρησης. Είναι απολύτως κατανοητό και αναμενόμενο πολλά πληροφοριακά συστήματα να μην έχουν σχεδιαστεί με τις σωστές προδιαγραφές ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί μέσα από τεχνικά μέσα είναι περιορισμένη και θα πρέπει να υποστηρίζεται από κατάλληλη διαχείριση και διαδικασίες.

Η διαχείριση της ασφάλειας πληροφοριών χρειάζεται συμμετοχή, όχι μόνο από τους εργαζομένους στην επιχείρηση, αλλά και όλους όσους συνεργάζονται με αυτήν, ενδεχομένως και με ειδικούς εμπειρογνώμονες έτσι ώστε να εξασφαλιστεί το καλύτερο δυνατό αποτέλεσμα. Αναγνωρίζοντας τι είδους έλεγχοι χρειάζονται και ποιες είναι οι απαιτήσεις της επιχείρησης σε ασφάλεια προχωράμε με προσοχή στη λεπτομέρεια στον προσεχτικό σχεδιασμό της πολιτικής ασφάλειας. Είναι σαφές, λοιπόν, το ότι στις μέρες μας είναι απαραίτητο να ακολουθείται και να εφαρμόζεται πολιτική ασφάλειας εδραιώνοντας έτσι την ασφάλεια σε κάθε δυνατό επίπεδο και παρέχοντας την απαιτούμενη προστασία στην επιχείρηση.

Καθώς, οι περισσότεροι οργανισμοί βασίζουν πλέον ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφαλείας που χρειάζονται για να επιτευχθεί ικανοποιητική ασφάλεια. Μεγάλες ποσότητες πόρων ξοδεύονται με σκοπό την αποφυγή αποτυχιών. Παρόλα αυτά, τελικά είναι αδύνατο να υπάρξει η εγγύηση ότι το Πληροφοριακό Σύστημα (ΠΣ) είναι τέλειο, όπως είναι επίσης αδύνατο να προβλεφθεί και να εξαλειφθεί κάθε τι από τον εξωτερικό κόσμο που πιθανόν να απειλήσει το ΠΣ. Αυτό που όμως είναι δυνατό να επιτευχθεί, είναι η μείωση της πιθανότητας εμφάνισης κινδύνου, η οποία θα επιφέρει και ελάττωση της αβεβαιότητας.

Προϋπόθεση για την επίτευξη αυτής της ελάττωσης αποτελεί η εφαρμογή μιας κατάλληλης μεθόδου μελέτης επικινδυνότητας ώστε να επιτευχθεί επαρκής αναγνώριση και αποτελεσματική αντιμετώπιση των διαφόρων κινδύνων που απειλούν το σύστημα. Όπως διαφαίνεται, η επιλογή της κατάλληλης μεθόδου μελέτης επικινδυνότητας, αποτέλεσε το έναυσμα για την εκπόνηση της παρούσας διπλωματικής εργασίας.

1.1. ΣΚΟΠΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ

Ένας οργανισμός/υπηρεσία προκειμένου να έχει τη δυνατότητα να επιτυγχάνει τους στόχους του θα πρέπει, μεταξύ άλλων, να διασφαλίσει όσο το δυνατό καλύτερα την απαιτούμενη ασφάλεια της υπολογιστικής υποδομής του καθώς και των ευαίσθητων δεδομένων (βάσει νομικών υποχρεώσεων ή λόγω της φύσης του οργανισμού) που αποθηκεύονται ή διακινούνται σε αυτή. Το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων ήταν πάντα κρίσιμο. Αναμφισβήτητα, σήμερα ο κίνδυνος είναι πιο συνειδητός, καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων.

Η πληροφορία, οποιαδήποτε και αν είναι η μορφή της, εφόσον είναι σημαντική απαιτείται να διαφυλάσσεται κατάλληλα και να είναι σωστά προστατευμένη. Αυτός είναι ο απώτερος σκοπός της ασφάλειας πληροφοριών: να προστατεύει την πληροφορία από ένα ευρύ φάσμα απειλών παρέχοντας εξασφάλιση στην επιχειρηματική κοινωνία, ελαχιστοποιώντας τη ζημία των επιχειρήσεων και αυξάνοντας το κέρδος από επενδύσεις και επιχειρηματικές ευκαιρίες. Η εφαρμογή ενός σχεδίου ασφάλειας σήμερα, σύμφωνα με διεθνείς μεθόδους και πρακτικές, αντιμετωπίζεται σαν μία σημαντική διαχειριστική λειτουργία και όχι απλά ως μία τεχνική λειτουργία.

Για τη μελέτη και την εκπόνηση ενός αποτελεσματικού σχεδίου, απαιτείται η χρήση της κατάλληλης μεθόδου μελέτης επικινδυνότητας. Ωστόσο, υπάρχει πληθώρα μεθόδων, καθεμιά από τις οποίες έχει ιδιαίτερα χαρακτηριστικά τα οποία την καθιστούν πιο ικανή να ανταπεξέλθει στις εκάστοτε συνθήκες που επικρατούν σε ένα οργανισμό.

Σκοπός της συγκεκριμένης μεταπτυχιακής διατριβής, είναι η παρουσίαση μερικών από των πιο γνωστών και διεθνώς αποδεκτών μεθόδων μελέτης και διαχείρισης κινδύνων και επιχειρείται μια αναλυτική σύγκριση των μεθόδων CRAMM (με το ομώνυμο εργαλείο), MAGERIT (με το εργαλείο PILAR) και MEHARI (με το ομώνυμο εργαλείο) βάσει ενός σεναρίου από τη πραγματική αγορά.

Συνοπτικά η δομή της διπλωματικής κινήθηκε στους παρακάτω άξονες:

- Περιγραφή των μεθοδολογιών
- Σύγκριση των μεθοδολογιών σε πραγματικό περιβάλλον CRAMM, MAGERIT και MEHARI (με τη χρήση των αντίστοιχων εργαλείων).
- Εξαγωγή συμπερασμάτων βάσει των αποτελεσμάτων της σύγκρισης

Ο σκοπός της μεταπτυχιακής διατριβής είναι η σύγκριση της ανάλυσης επικινδυνότητας των ανωτέρω μεθοδολογιών, και *όχι* η σύγκριση και των προτεινόμενων αντιμέτρων των μεθοδολογιών.

1.2. ΜΕΘΟΔΟΛΟΓΙΕΣ ΥΠΟ ΜΕΛΕΤΗ-ΠΡΟΣΕΓΓΙΣΗ

Στην παρούσα μεταπτυχιακή διατριβή γίνεται μελέτη ενός οργανισμού, ο οποίος ανήκει στον οικονομικό τομέα (Financial sector). Ο συγκεκριμένος τομέας αποτελεί μέρος των κρίσιμων υποδομών (Critical Infrastructure). Ως κρίσιμη υποδομή ορίζεται ένα στοιχείο ή ένα σύστημα που είναι απαραίτητο για τη διατήρηση ζωτικών κοινωνικών λειτουργιών. Η ζημιά σε μια κρίσιμη υποδομή, η καταστροφή ή η διατάραξη της από φυσικές καταστροφές, η τρομοκρατία, η εγκληματική δραστηριότητα ή η κακόβουλη συμπεριφορά μπορεί να έχουν σημαντικές αρνητικές επιπτώσεις στην ασφάλεια του οργανισμού που ανήκουν και στην ομαλή λειτουργία του.

Οι περισσότερες κρίσιμες υποδομές πληροφοριών (CIIs) περιλαμβάνουν περίπλοκα συστήματα Τεχνολογίας Πληροφορικής και Επικοινωνίας (ΤΠΕ - ICT) με δυναμικές αλληλεπιδράσεις με αρκετές άλλες οντότητες. Αυτή η περίπλοκη αλληλεπίδραση μιας κρίσιμης υποδομής απεικονίζεται στο Σχήμα 1 [28]. Για παράδειγμα, οι λιμένες αλληλοεπιδρούν με άλλα λιμάνια, πλοία (με επιβάτες, πλήρωμα ή / και

φορτίο), λιμενικές αρχές, ναυτιλιακές και ασφαλιστικές εταιρείες, τελωνεία, τράπεζες, κυβερνητικά υπουργεία, άλλους εμπορικούς παρόχους και άλλες υποδομές ζωτικής σημασίας (π.χ. σιδηροδρομικές γραμμές, αεροδρόμια).

Σχήμα 1: Διασυνδέσεις του περιβάλλοντος ΤΠΕ σε κρίσιμη υποδομή

Όσον αφορά την προστασία αυτής της πολύπλοκης υποδομής ΤΠΕ, τα υφιστάμενα σχετικά πρότυπα, μεθοδολογίες και εργαλεία επικεντρώνονται είτε στην ασφάλεια (φυσική ασφάλεια) είτε στην ασφάλεια ΤΠ. Επιπλέον, διαπιστώνεται μια κοινή παρεξήγηση μεταξύ των μεθοδολογιών που χρησιμοποιούνται και των διαθέσιμων εργαλείων για την εφαρμογή των μεθοδολογιών αυτών. Μια μεθοδολογία περιγράφει την ακολουθία των γενικών βημάτων που απαιτούνται για την εφαρμογή μιας ανάλυσης αξιολόγησης κινδύνου. Αυτά τα βήματα είναι οι διαδικασίες ταυτοποίησης, ποσοτικοποίησης και συσχέτισης του κινδύνου με τα αγαθά. Από την άλλη πλευρά, ένα εργαλείο αξιολόγησης κινδύνου προσανατολίζεται προς τη μέτρηση του δυναμικού απώλειας που θα μπορούσε να έχει μια απειλή σε έναν οργανισμό. Τα εργαλεία βασίζονται σε μεθοδολογίες και συχνά αναπτύσσονται ειδικά εργαλεία για μια συγκεκριμένη μεθοδολογία [59].

Σύμφωνα με τον El Fray I [23], υπάρχουν περισσότερες από 200 μεθοδολογίες αξιολόγησης κινδύνου. Οι πιο γνωστές και αποδεκτές από την αγορά μεθοδολογίες είναι η CRAMM, η OCTAVE, η EBios, η MAGERIT, η MEHARI, η STORM, η IT - Grundschutz και η ISAMM. Ένα κοινό χαρακτηριστικό αυτών των μεθοδολογιών είναι ότι ασχολούνται μόνο με την αξιολόγηση του κινδύνου ασφάλειας IT και δεν ασχολούνται με την φυσική ασφάλεια. Ο Πίνακας 1 παρουσιάζει τα βασικά

χαρακτηριστικά κάθε μεθοδολογίας και παρουσιάζει μερικά από τα μοναδικά χαρακτηριστικά της κάθε μεθοδολογίας [28].

		Characteristics			
		Κλίμακα αξιολόγησης	**Αξιολόγηση Επίπτωσης**	**Δυνατότητα συνεργασίας**	**Απαιτούμενες δεξιότητες**
Methods	**OCTAVE**	Ποιοτική	Βασισμένη σε κρίσιμα αγαθά	Μέτρια	Τυπικές
	CRAMM	Ποιοτική	Βασισμένη σε ανοικτά σενάρια ζημίας	Χαμηλή	ITC Εξειδίκευση
	Ebios	Ποιοτική	Βασισμένη σε ανάγκες ασφαλείας	Μέτρια	Τυπικές
	MAGERIT	Ποιοτική/ Ποσοτική	Βασισμένη σε ανοικτά σενάρια ζημίας	Χαμηλή	ITC Εξειδίκευση
	MEHARI	Ποιοτική	Βασισμένη σε συγκεκριμένα σενάρια ζημίας	Χαμηλή	ITC Εξειδίκευση
	STORM	Ποιοτική	Βασισμένη σε ανοικτά σενάρια ζημίας	Υψηλή	Χαμηλές
	IT-Grundschutz	Ποιοτική	Βασισμένη σε ανοικτά σενάρια ζημίας	Χαμηλή	Τυπικές
	ISAMM	Ποιοτική	Βασισμένη σε απώλεια χρημάτων	Χαμηλή	Τυπικές

Πίνακας 1: Χαρακτηριστικά των υφιστάμενων μεθοδολογιών εκτίμησης κινδύνου

Στο πλαίσιο της διατριβής θα ακολουθηθεί το ακόλουθο μοντέλο υλοποίησης της μελέτης:

- Περιγραφική μελέτη των τριών πιο γνωστών και χρησιμοποιούμενων μεθοδολογιών ανάλυσης επικινδυνότητας σε πληροφοριακά συστήματα κρίσιμων υποδομών (CRAMM, MAGERIT, MEHARI),
- Περιγραφή του οργανισμού που πρόκειται να μελετηθεί και να αναλυθεί
- Εφαρμογή των τριών μεθοδολογιών στο συγκεκριμένο περιβάλλον του οργανισμού
- Εξαγωγή αποτελεσμάτων με την χρήση κατάλληλων εργαλείων
- Σύγκριση αποτελεσμάτων, και
- Εξαγωγή συμπερασμάτων και προτάσεις για περαιτέρω μελέτη

Έχει επιλεχθεί ο οικονομικός τομέας επειδή αποτελεί ένα πολύ ιδιαίτερο περιβάλλον και πολύ κρίσιμο για την παγκόσμια αγορά και οικονομία. Ο επιλεγμένος οργανισμός προς μελέτη που ανήκει σε αυτόν τον τομέα αποτελεί έναν από τους τέσσερις κρίσιμους οργανισμούς της Ελλάδος για την εύρυθμη λειτουργία της οικονομίας. Για την υλοποίηση της διατριβής και λόγω της διαφορετικότητας της κάθε μεθοδολογίας σε επόμενο κεφάλαιο θα παρουσιαστεί η αντιστοίχιση των τιμών μεταξύ των μεθοδολογιών, καθώς επίσης θα γίνει παρουσίαση και σύγκριση των αποτελεσμάτων για εξαγωγή κατάλληλων συμπερασμάτων.

2. ΜΕΘΟΔΟΛΟΓΙΕΣ ΑΝΑΛΥΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Στην παρούσα φάση της μεταπτυχιακής διατριβής θα γίνει μια εκτενή αναφορά σε τρεις (3) από τις πιο δημοφιλείς μεθοδολογίες ανάλυσης επικινδυνότητας που επιλέγονται από ένα μεγάλο πλήθος οργανισμών κρίσιμων υποδομών. Πιο συγκεκριμένα παρακάτω θα γίνει μια αναφορά στα χαρακτηριστικά, στο κοινό που απευθύνονται καθώς και στα εργαλεία και στους τομείς ενδιαφέροντος των μεθοδολογιών CRAMM, MAGERIT και MEHARI.

2.1. CRAMM

Η μέθοδος CRAMM αναπτύχτηκε από το CCTA (Central Computer and Telecommunications Agency, 1996) της βρετανικής κυβέρνησης το 1985, ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Στη συνέχεια η χρήση της επεκτάθηκε και στη μελέτη επικινδυνότητας σε μεγάλης κλίμακας ιδιωτικούς και δημόσιους οργανισμούς. Η μέθοδος CRAMM είναι ικανή να καλύψει ένα ευρύ φάσμα διοικητικών, επιχειρησιακών και τεχνικών απαιτήσεων.

Η CRAMM έχει κερδίσει διεθνή αναγνώριση για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε χιλιάδες περιπτώσεων, συνεπώς είναι ώριμη μέθοδος ευρισκόμενη ήδη στην 5η έκδοσή της (version 5.2.2011).
- 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 κ.λπ.

Η CRAMM υλοποιείται από έναν αναλυτή ή από μια ομάδα αναλυτών, οι οποίοι είναι υπεύθυνοι για την αξιολόγηση του επιπέδου ασφάλειας και κινδύνου του οργανισμού που αναλύει και συνδυάζει τις ποικίλες γνώσεις που διανέμονται στο εταιρικό περιβάλλον (El Fray I, 2012). Όπως είναι κατανοητό, οι απαιτούμενες δεξιότητες των συμμετεχόντων είναι πολύ υψηλές και η συνεργασία αυτής της μεθοδολογίας είναι επίσης χαμηλή.

Η υπολογιστική μέθοδος και η τεχνική την οποία υιοθετεί η CRAMM για το συσχετισμό και τον προσδιορισμό των αποτελεσμάτων βασίζεται σε μια ποιοτική προσέγγιση. Η βασική ιδέα είναι ότι από την ανάλυση επικινδυνότητας μπορεί να προβλεφθεί η πιθανή ζημία που θα προκαλέσει η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ενός αγαθού. Παράλληλα, παρέχει επαρκή βεβαιότητα ότι έχουν εντοπιστεί όλοι οι πιθανοί κίνδυνοι, οι αδυναμίες και οι απειλές και ότι όλα τα αποτελέσματα είναι συνεπή σε όλο το φάσμα του πληροφοριακού συστήματος που αξιολογείται. Η μέθοδος CRAMM περιέχει μια πολύ μεγάλη βιβλιοθήκη αντιμέτρων που αποτελείται από περίπου 3.500 λεπτομερή αντίμετρα οργανωμένα σε περισσότερες από 70 κατηγορίες.

Το κόστος για την εξάλειψη όλων των κινδύνων που απειλούν ένα πληροφοριακό σύστημα είναι απαγορευτικό. Ωστόσο, σύμφωνα με την CRAMM, η επικινδυνότητα μπορεί να αντιμετωπισθεί αποτελεσματικά και οικονομικότερα, μέσα από την δομημένη ανάλυση και αποτίμηση των αγαθών. Σύμφωνα με την μέθοδο CRAMM, η επικινδυνότητα θεωρείται ότι είναι ο συνδυασμός της πιθανότητας να συμβεί ένα ανεπιθύμητο περιστατικό και των επιπτώσεων που θα μπορούσαν να προκύψουν από αυτό. Επομένως, η μέθοδος CRAMM καταδεικνύει το δυνητικό κόστος που μπορεί να επιβαρύνει έναν οργανισμό, συντελώντας καταλυτικά στη δικαιολόγηση του κόστους των προτεινόμενων αντιμέτρων.

Η CRAMM είναι συνεργατική μέθοδος και αποτελείται από τρία βασικά στάδια:

1. Προσδιορισμός-αποτίμηση αγαθών (identification and valuation of assets),
2. Ανάλυση επικινδυνότητας (risk analysis) και
3. Διαχείριση επικινδυνότητας (risk management).

Στάδιο	Βήματα
Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
Ανάλυση επικινδυνότητας (risk analysis)	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
Διαχείριση επικινδυνότητας (risk management)	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Πίνακας 2: **Τα 3 βασικά στάδια της μεθοδολογίας** CRAMM **σε βήματα**

Η μέθοδος CRAMM είναι η κύρια μέθοδος πιστοποίησης για τα πρότυπα ISO 27000, ενώ επικεντρώνεται στα ISO/IEC 27001:2005. Παράλληλα, καλύπτει τις απαιτήσεις της ευρωπαϊκής και της ελληνικής νομοθεσίας, που απαιτούν από τα πληροφοριακά συστήματα που επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας. Με τον τρόπο αυτό, εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.

Επιπλέον, διαχωρίζει τα αγαθά στις εξής κατηγορίες: εξοπλισμός, υπηρεσίες, λογισμικό, δεδομένα και τοποθεσίες. Κατά την αποτίμηση των αγαθών η CRAMM εξετάζει τις παρακάτω πτυχές: διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα. Για την αποτίμηση αγαθών η CRAMM διαθέτει 10 επίπεδα. Το εργαλείο CRAMM καλύπτει τα παρακάτω είδη απειλών: λογικές απειλές, απειλές επικοινωνιών, τεχνικές βλάβες, ανθρώπινα σφάλματα και φυσικές απειλές. Η μέθοδος CRAMM εξετάζει κάθε συνδυασμό του γινομένου επισφάλεια και επίπτωση και βρίσκει ποιο είναι το πιο επικίνδυνο. Αυτό το γινόμενο είναι που καθορίζει ποια μέτρα θα ληφθούν, λαμβάνοντας υπόψη μόνο το worst-case scenario.

Οι τύποι που ορίζει η CRAMM είναι: μείωση απειλής, μείωση τρωτότητας, μείωση επίπτωσης, ανίχνευση και ανάκαμψη. Πολύ σημαντική κρίνεται και η δυνατότητα επανιχνηλάτησης για την εξέταση συγκεκριμένου συνδυασμού αγαθού/απειλής/ευπάθειας που οδήγησε στην επιλογή των αντίστοιχων αντιμέτρων.

Κάθε ομάδα αντιμέτρων στο εργαλείο CRAMM, έχει την ακόλουθη δομή:

- Δήλωση πολιτικής, η οποία εξάγεται αυτολεξεί από το κατάλληλο έγγραφο ασφάλειας.
- Ο στόχος και η ανάγκη που θα ικανοποιηθεί από την εφαρμογή των συγκεκριμένων αντιμέτρων.
- Λεπτομερής περιγραφή της σχετιζόμενης επιχειρησιακής λειτουργίας με το αντίμετρο.
- Τρόποι ή επιλογές που μπορούν να διασφαλίσουν την επιθυμητή λειτουργικότητα.

2.2. MAGERIT

Η μέθοδος MAGERIT αναπτύχθηκε το 1997 από το Ανώτατο Ισπανικό Συμβούλιο για την Ηλεκτρονική διακυβέρνηση (Consejo Superior de Administración Electrónica). Η MAGERIT μπορεί να χρησιμοποιηθεί και να συντηρείται μόνο από ειδικούς χρήστες IT. Αυτοί οι χρήστες είναι υπεύθυνοι για την εφαρμογή της διαδικασίας ανάλυσης κινδύνου χρησιμοποιώντας εργαστήρια και συνεντεύξεις με συγκεκριμένους εκπροσώπους του οργανισμού. Συμμετέχουν μόνο σε συγκεκριμένες φάσεις της διαδικασίας αξιολόγησης. Ως εκ τούτου, οι απαιτούμενες δεξιότητες των συμμετεχόντων είναι πολύ υψηλές και η συνεργασία της μεθοδολογίας είναι χαμηλή, παρότι υπάρχουν αλληλεπιδράσεις μεταξύ των εμπειρογνωμόνων και ορισμένων μελών του προσωπικού της οργάνωσης. Αυτή τη στιγμή βρίσκεται στην τρίτη έκδοση με έτος θεώρησης το 2012.

Η μεθοδολογία MAGERIT αποσκοπεί στα εξής:

- Να αναδείξει την ύπαρξη απειλών, κινδύνων και την ανάγκη έγκαιρης αντιμετώπισής τους.
- Να προσφέρει μια συστηματική μέθοδο ανάλυσης των κινδύνων.
- Να υποβοηθήσει στην περιγραφή και το σχεδιασμό των κατάλληλων μέτρων ελέγχου της επικινδυνότητας.
- Να προετοιμάσει τον Οργανισμό για μία διαδικασία αξιολόγησης (valuation), ελέγχου (auditing) και πιστοποίησης (certification).

- Να επιτύχει ομοιομορφία στις αναφορές που εμπεριέχουν τα ευρήματα και τα συμπεράσματα της ανάλυσης, προτείνοντας μια ενιαία δομή.

Το λογισμικό που υποστηρίζει τη μέθοδο MAGERIT αποτελεί αναπόσπαστο τμήμα της και ονομάζεται EAR/Pilar. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή βήμα προς βήμα εφαρμογή της μεθόδου, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που 201συλλέγονται κατά την εφαρμογή της μεθόδου. Το εργαλείο διατέθηκε στην αγορά το 2004 και υποστηρίζεται από τον A.L.H.J. Mañas (Manas, 2009).

Τα στάδια και τα βήματα της μεθόδου παρουσιάζονται συνοπτικά στον Πίνακα Α-3 και περιγράφονται λεπτομερώς στη συνέχεια.

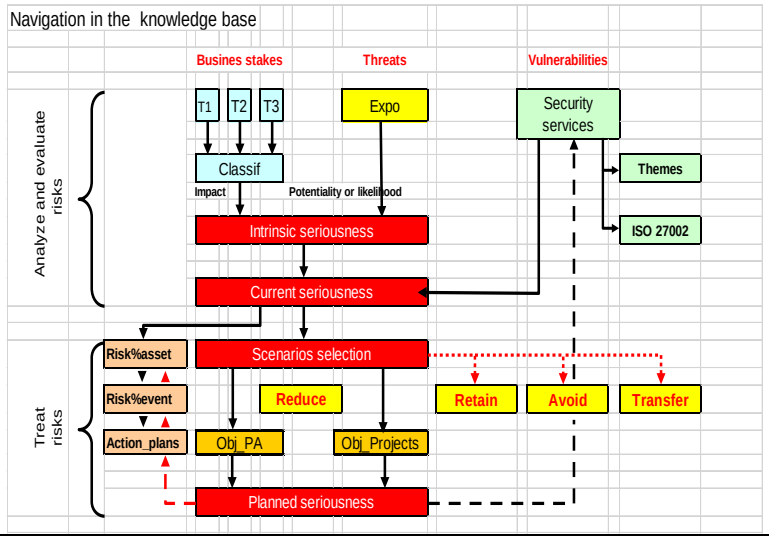
Στάδιο	Βήματα σταδίου
1. Προετοιμασία και προγραμματισμός έργου (Preparation & Planning of implementation)	*Βήμα 1*: Μελέτη σκοπιμότητας *Βήμα 2*: Καθορισμός πλαισίου αναφοράς *Βήμα 3*: Προγραμματισμός έργου *Βήμα 4*: Έναρξη έργου
2. Ανάλυση επικινδυνότητας (Risk analysis)	*Βήμα 1:* Αναγνώριση και Αποτίμηση Αγαθών *Βήμα 2:* Χαρακτηρισμός και Εκτίμηση Απειλών *Βήμα 3:* Χαρακτηρισμός Αντιμέτρων *Βήμα 4:* Εκτίμηση Επικινδυνότητας
3. Διαχείριση επικινδυνότητας (Risk management)	*Βήμα 1*: Λήψη αποφάσεων *Βήμα 2*: Προετοιμασία σχεδίου ασφάλειας *Βήμα 3*: Υλοποίηση σχεδίου ασφάλειας

Πίνακας 3: Τα 3 βασικά στάδια της μεθοδολογίας MAGERIT σε βήματα

2.3. MEHARI

Η MEHARI (Methode Harmonisee d'Analyse de Risques) είναι μία μέθοδος αξιολόγησης κινδύνου και αναπτύχθηκε από την CLUSIF το 1996. Απευθύνεται κυρίως σε στελεχιακό δυναμικό (διευθυντές λειτουργίας, CISO, CIO, ελεγκτές, διευθυντής διαχείρισης κινδύνων) για τη διαχείριση της ασφάλειας των πληροφοριών και των πόρων των πληροφοριακών συστημάτων, και τη μείωση των κινδύνων. Η MEHARI είναι συμβατή με το πρότυπο διαχείρισης κινδύνου ISO/IEC27005 και είναι κατάλληλη για τη διαδικασία ISMS που περιγράφεται στο πρότυπο ISO 27001.

Περιγράφει μία περίπλοκη διαδικασία συμπεριλαμβάνοντας τα κυκλικά βήματα της διαχείρισης κινδύνων καθώς και τη δημιουργία μιας προσαρμοσμένης βάσης γνώσεων. Μετά τη δημιουργία βάσης γνώσεων ξεκινάει μία διαδικασία για την ανάλυση των κινδύνων κάθε σεναρίου.



Σχήμα 2: Η βάση γνώσης της MEHARI μεθοδολογίας

Αυτή η διαδικασία ακολουθεί τα παρακάτω βήματα:

1) Ταυτοποίηση μιας κατάστασης κινδύνου (είτε χρησιμοποιώντας τη βάση γνώσεων είτε με τον εντοπισμό πιθανών δυσλειτουργιών)
2) Αξιολόγηση της φυσικής έκθεσης
3) Αξιολόγηση των αποτρεπτικών και προληπτικών παραγόντων
4) Αξιολόγηση της προστασίας
5) Αξιολόγηση της πιθανότητας του κινδύνου
6) Αξιολόγηση των εγγενών επιπτώσεων (πχ. συνέπειες) με την συμπλήρωση ενός πίνακα
7) Αξιολόγηση και μείωση των επιπτώσεων μέσω αυτοματοποιημένου υπολογισμού
8) Σφαιρική αξιολόγηση του κινδύνου
9) Απόφαση αν ο κίνδυνος είναι αποδεκτός

Πλεονεκτήματα της μεθόδου MEHARI

- Πλήρως συμβατή με όλα τα πρότυπα ασφαλείας πληροφοριών ISO
- Περιέχει εκτεταμένη βάση γνώσεων σε μορφή Microsoft Excel

Μειονεκτήματα της μεθόδου MEHARI

- Χρησιμοποιείται μόνο σε συνδυασμό με ειδικό λογισμικό ή υπολογιστικά φύλλα
- Το πρώτο παράδειγμα της ανάλυσης απαιτεί μια περίπλοκη προσαρμογή στη βάση γνώσεων.

2.4. ΟΜΟΙΟΤΗΤΕΣ ΚΑΙ ΔΙΑΦΟΡΕΣ

Από τα παραπάνω, είναι σαφές ότι οι μεθοδολογίες που παρουσιάζονται δεν μπορούν να καταγράψουν την πολυπλοκότητα των διασυνδέσεων υποδομής, των διατομεακών επιπτώσεων, των εξαρτήσεων από άλλα συστήματα ή υποδομές και των επικαλυπτόμενων επιπτώσεων σε έναν τομέα ή σε διάφορους τομείς. Θεωρούν τον κίνδυνο τόσο ως ένα συνδυασμό της πιθανότητας και του αντίκτυπου μιας απειλής που πλήττει μια ομάδα assets όσο και ως το επίπεδο ευπάθειας αυτής της ομάδας assets.

Όσον αφορά τη συμμόρφωση προς τα διεθνή πρότυπα, μόνο η MAGERIT συμμορφώνονται πλήρως με τους κανόνες και τις διαδικασίες του ISO. Οι άλλες μεθοδολογίες καλύπτουν μόνο εν μέρει τις υποχρεώσεις που επιβάλλονται από την οικογένεια προτύπων ISO. Επιπλέον, όλες οι μεθοδολογίες είτε δεν συνεργάζονται καθόλου είτε βρίσκονται σε αξιοσημείωτα χαμηλό επίπεδο.

Όπως γίνεται κατανοητό από τα ανωτέρω, για να εξαχθούν τα κατάλληλα συμπεράσματα για το ποια μεθοδολογία μπορεί να χρησιμοποιηθεί σε μία κρίσιμη υποδομή, ανάλογα το τι είδους είναι, θα πρέπει να πραγματοποιηθεί μία συγκριτική μελέτη βασιζόμενη σε ένα σενάριο του πραγματικού περιβάλλοντος [28].

2.5. ΑΝΙΣΤΟΙΧΙΣΕΙΣ

Λόγω της διαφορετικής φύσης της κάθε μεθοδολογίας και του διαφορετικού θεωρητικού υποβάθρου στη κάθε μία από αυτές, η διατριβή αυτή προβαίνει σε συγκεκριμένες παραδοχές θέτοντας κάποιες υποθέσεις.

Όπως παρουσιάστηκε παραπάνω, ο βαθμός επικινδυνότητας της CRAMM χρησιμοποιεί κλίμακα της τάξης από 1 έως 7, η MAGERIT της τάξης 1 έως 7 και η MEHARI της τάξης 1 έως 4. Γι' αυτό το λόγο έγινε η ακόλουθη αντιστοίχιση τιμών:

CRAMM	MAGERIT	MEHARI
1	1	1
2	2	2
3	3	2
4	4	3
5	5	3
6	6	4
7	7	4

Πίνακας 4: Αντιστοιχία τιμών μεταξύ των μεθοδολογιών CRAMM, MAGERIT και MEHARI

Η ανωτέρω αντιστοίχιση τιμών θα χρησιμοποιηθεί μετά την προσομοίωση για την αξιολόγηση των ευρημάτων από την κάθε μεθοδολογία με στόχο την εξαγωγή των κατάλληλων συμπερασμάτων.

3. ΣΕΝΑΡΙΟ ΠΡΟΣΟΜΟΙΩΣΗΣ

3.1. ΤΟΜΕΑΣ ΣΕΝΑΡΙΟΥ

Τα χρηματοπιστωτικά ιδρύματα, που αποτελούν μέρος των κρίσιμων υποδομών, αντιμετωπίζουν προκλήσεις σχετικά με τη διατήρηση της ασφάλειας και της ευρωστίας του θεσμικού οργάνου και της ικανότητάς του να διαχειρίζεται τα κέρδη και το κεφάλαιο. Οι νέες τεχνολογίες απαιτούν αυξημένη επιμέλεια από οικονομικές διαισθήσεις [69].

Το FBI, στην έκθεσή του για το 2001 "Έκθεση για την απάτη και την αποτυχία χρηματοπιστωτικών ιδρυμάτων", λέει Η Απάτη Χρηματοπιστωτικών Ιδρυμάτων (FIF) αποτελεί προτεραιότητα βαθμίδας 1 στο στρατηγικό της σχέδιο και προσδιορίζει τις αποτυχίες των τραπεζών, τον εντοπισμό κλοπής, τον έλεγχο της απάτης, τα πλαστά διαπραγματεύσιμα μέσα, υποθήκη και δάνεια απάτης ως κύριοι τομείς της έρευνας και μια αύξηση σημασία στις έρευνές της σχετικά με τις αναδυόμενες τεχνολογίες και την τραπεζική πληροφορική.

Το FBI αναφέρει ότι σε όλη τη δεκαετία του 1980 και στις αρχές της δεκαετίας του 1990 οι περισσότεροι της απάτης ήταν αποτέλεσμα της κατάχρησης από τους εμπλεκόμενους. Σήμερα προκύπτουν τα κυρίαρχα συστήματα από τους ξένους. "Η διαπερατότητα του ελέγχου της απάτης και των πλαστών διαπραγματεύσιμων τα συστήματα οργάνων, την τεχνολογική πρόοδο, καθώς και τη διαθεσιμότητα προσωπικού μέσω των δικτύων πληροφοριών, πυροδότησε την αύξηση της εξωτερικής απάτης".

Εκτός από τις άμεσες πράξεις απάτης και κατάχρησης, τα χρηματοπιστωτικά ιδρύματα συχνά γίνονται τα μέσα πλύσης χρημάτων και τις παράνομες φιλανθρωπικές εισφορές σε τρομοκράτες. Το Διεθνές Νομισματικό Ταμείο εκτιμά ότι η νομιμοποίηση εσόδων από παράνομες δραστηριότητες θα μπορούσε να είναι οπουδήποτε από το 2-5% του παγκόσμιου ακαθάριστου εγχώριου προϊόντος και έχει χαρακτηριστεί ως η "δεύτερη μεγαλύτερη υπόγεια οικονομία στον κόσμο." Τόσο οι ΗΠΑ όσο και οι διεθνείς οργανισμοί έχουν επιβαρύνει τα χρηματοπιστωτικά ιδρύματα αποτροπή της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης των τρομοκρατών. Στις ΗΠΑ, αυτό επιτυγχάνεται με τη χρήση λογισμικού για την εφαρμογή των απαιτήσεων του τμήματος 314 του νόμου Patriot και του Office of Foreign Assets Control (OFAC), Τμήμα Προγράμματος Συμμόρφωσης.

Όταν οι τράπεζες αποτυγχάνουν να παράσχουν επαρκή έλεγχο στην τεχνολογία των πληροφοριών, μπορούν αναμένουν να υποστούν επιχειρησιακές ζημίες από μαζικές επιθέσεις εναντίον τους το Διαδίκτυο και την κρίσιμη υποδομή του έθνους. Στις 26 Ιανουαρίου 2003, μια επίθεση τύπου "ιού τύπου" κατά του MS-SQL Server 2000 επιβράδυνε την παγκόσμια κίνηση στο Internet και προκάλεσε τεχνικά προβλήματα που κατέστρεψαν 13.000 μηχανές ATM της Τράπεζας Αμερικής και της Canadian Imperial Bank of Commerce. Ενώ αυτά τα είδη ευπάθειας συλλάβουν συχνά την αρνητική προσοχή του κοινού, αντιπροσωπεύουν μόνο ένα μικρό μέρος των επιχειρηματικών κινδύνων που πρέπει να ελέγχουν τα χρηματοπιστωτικά ιδρύματα.

Το Γραφείο του Comptroller of the Currency (OCC) εντόπισε τέσσερα από τα εννέα κατηγοριών στο πλαίσιο κινδύνου στις οποίες εκτίθενται συχνότερα τα προϊόντα, οι υπηρεσίες, τα κανάλια παράδοσης και οι διαδικασίες που σχετίζονται με την τεχνολογία:

1. Κίνδυνοι συναλλαγών - τους κινδύνους για τα κέρδη ή τα κεφάλαια που προκύπτουν από προβλήματα με την παροχή υπηρεσιών ή προϊόντων, όπως για παράδειγμα τα εσωτερικά και εξωτερικά συστήματα και διαδικασίες που δεν έχουν ρυθμιστεί ή είναι ασυμβίβαστα.
2. Στρατηγικοί κίνδυνοι - τους κινδύνους για τα κέρδη ή τα κεφάλαια που προκύπτουν από δυσμενείς επιχειρηματικές αποφάσεις ή την εσφαλμένη εφαρμογή των εν λόγω αποφάσεων.
3. Φήμη - ο κίνδυνος για τα κέρδη ή τα κεφάλαια που απορρέουν από αρνητική κοινή γνώμη.
4. Συμμόρφωση- τον κίνδυνο για κέρδη ή κεφάλαια που προκύπτουν από παραβιάσεις ή μη συμμόρφωση με καθορισμένες πρακτικές ή δεοντολογικά πρότυπα.
5. Η μη τήρηση των κανονιστικών κατευθυντήριων γραμμών μπορεί να οδηγήσει σε αυστηρές κυρώσεις για τα χρηματοπιστωτικά ιδρύματα.

Πιο πρόσφατα, το Office of Thrift Supervision (OTS), ομαδοποίησε την τεχνολογία κινδύνους που αντιμετωπίζουν τα χρηματοπιστωτικά ιδρύματα σε τρεις κατηγορίες:

1. Κίνδυνοι ακεραιότητας πληροφοριών - οι πληροφορίες πρέπει να είναι διαθέσιμες, ακριβείς, πλήρεις, έγκυρες και ασφαλείς.
2. Οι κίνδυνοι συνέχισης της επιχείρησης την ικανότητα του θεσμικού οργάνου να προετοιμάζει και να εκπληρώνει επαρκώς τις ευθύνες του κατά τη διάρκεια μιας καταστροφής.
3. Οι κίνδυνοι διαχείρισης προμηθευτών- ο κίνδυνος ότι ο πάροχος υπηρεσιών δεν θα εκτελέσει τους συμβατικούς όρους και προϋποθέσεις όπως καθορίστηκαν προκαλώντας ανεπιθύμητες συνέπειες για τις πράξεις του ιδρύματος.

Αυτό αντικατοπτρίζει την υποχρέωση των χρηματοπιστωτικών ιδρυμάτων να παρέχουν υπηρεσίες μέσω Διαδικτύου υπηρεσίες, να χρησιμοποιούν και να επιβλέπουν τους παρόχους υπηρεσιών, και να αποδείξει, ιδιαίτερα το Διοικητικό Συμβούλιο της Διευθυντές και Αξιωματούχοι, η δέουσα επιμέλεια στην προστασία των πληροφοριών και των συναντήσεων των πελατών άλλες ρυθμιστικές απαιτήσεις.

"Η διοίκηση μπορεί να μειώσει την έκθεση σε κίνδυνο μιας τράπεζας υιοθετώντας και επανεξετάζοντας τακτικά το σχέδιο εκτίμησης κινδύνου, τους ελέγχους μετριασμού του κινδύνου, τις πολιτικές και διαδικασίες αντίδρασης στις διαδικασίες εισβολής και τις διαδικασίες δοκιμών".

Τα χρηματοπιστωτικά ιδρύματα εξαρτώνται σε μεγάλο βαθμό από εξωτερικούς παρόχους υπηρεσιών για τοποθεσίες Web και άλλα βασικά συστήματα πληροφοριών. Επιπλέον τα χρηματοπιστωτικά ιδρύματα έχουν μια ισχυρή επιχειρησιακή απαίτηση για ανάλυση καθημερινών χρηματοοικονομικών συναλλαγών προκειμένου να εντοπιστούν οι τάσεις χαρτοφυλακίου, δανεισμού και χρηματοπιστωτικών αγορών, οι απαιτήσεις των πελατών και να βελτιωθούν Υπηρεσίες. Αυτό απαιτεί τη μεταφορά δεδομένων από πολλαπλά συστήματα βασισμένα σε συναλλαγές σε εφαρμογές αναλυτικής βάσης δεδομένων ή αποθήκες δεδομένων [69].

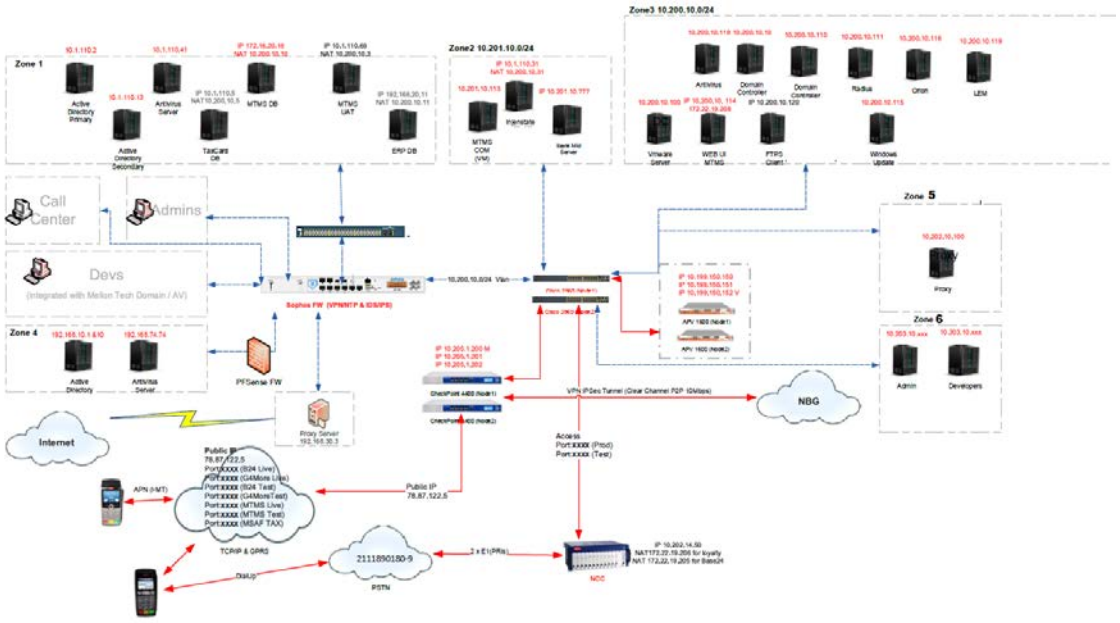
3.2. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ- ΑΓΑΘΑ

Για το σενάριο της προσομοίωσης θα χρησιμοποιηθεί το IT περιβάλλον διατραπεζικών συναλλαγών ενός χρηματοπιστωτικού ιδρύματος. Το περιβάλλον αυτό διακρίνεται σε δύο σημαντικές κατηγορίες αυτή του πρωτεύοντος συστήματος (Primary Side) και αυτή του συστήματος εκτάκτου ανάγκης (Disaster side).

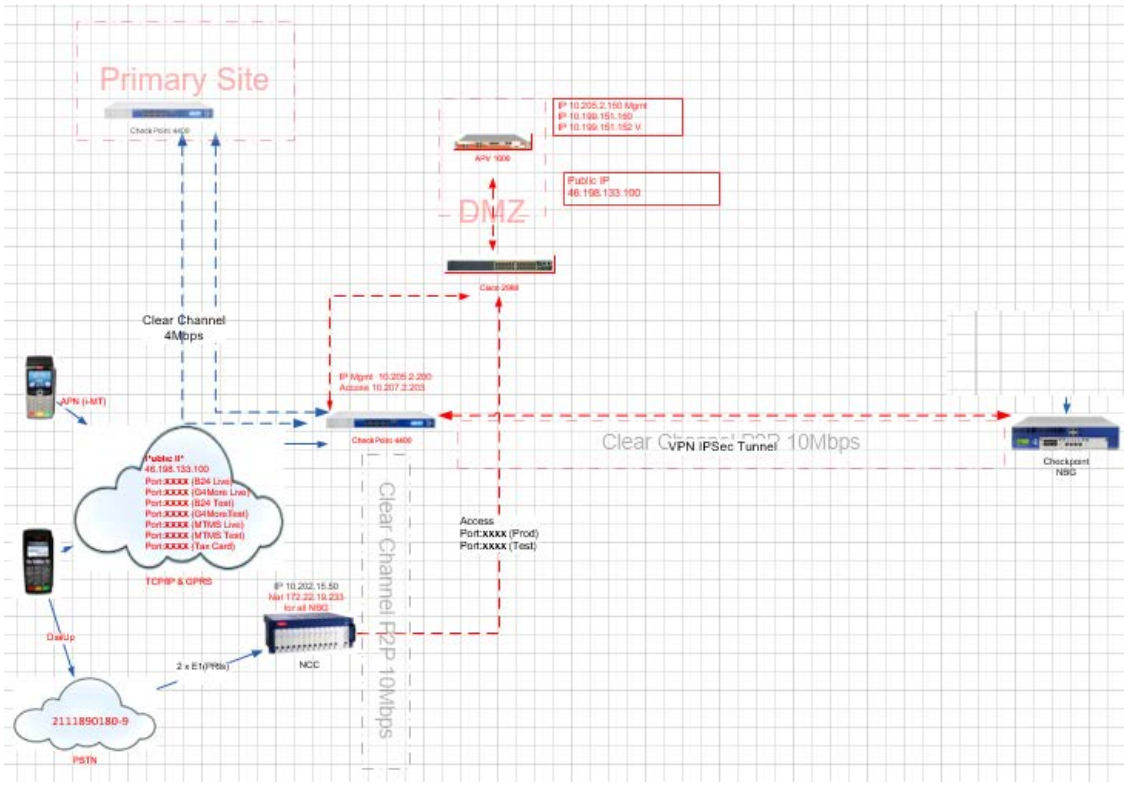
Το Primary Side περιλαμβάνει όλα εκείνα τα αγαθά (assets) που απαιτούνται για την ομαλή και εύρυθμη εκτέλεση διατραπεζικών συναλλαγών με πλήρη υποστήριξη του IT τομέα (call center, admins, peripheral devices) και επίβλεψη της ασφαλούς λειτουργίας των από ένα πλήθος firewalls, antivirus servers, data bases και proxy servers.

Το Disaster Side περιλαμβάνει τ΄ αγαθά εκτάκτου ανάγκης που είναι ικανά να υποστηρίξουν την συνέχιση εκτέλεσης διατραπεζικών συναλλαγών μέχρις ότου αποκατασταθεί το πρόβλημα στο Primary Side.

Στα παρακάτω δύο (2) σχήματα φαίνεται η δομή σε ζώνες και τα αγαθά του Primary και Disaster Side.



Σχήμα 3: Τα Primary Side αγαθά του σεναρίου προσομοίωσης κατανεμημένα σε ζώνες



Σχήμα 4: Τα Disaster Side αγαθά του σεναρίου προσομοίωσης

Ενώ, στον παρακάτω πίνακα γίνεται μια συνολική παρουσίαση των αγαθών του σεναρίου.

		Network & Security Equipment	**OS / Firmware/DB Type**
CDE (Primary)	**Zone 1**	Active Directory Primary PC	
		Active Directory Secondary PC	
		Antivirus Server	
		TaxCard DB	
		MTMS DB	Win Server 2008 R2/ Oracle 11g (11g,11,2,0,10)
		MTMS UAT	Win Server 2008 R2
		ERP DB	Win Server 2008 R3/ MS SQL 2008
	Zone 2	MTMS COM (VM)	Win Server 2012 R2
		ibank Mid server	
		Ingestate	
	Zone 3	Antivirus	
		Domain Controller 1	

		Domain Controller 2	
		Radius	
		Orion	
		LEM	
		Vmware Server	
		WEB UI MTMS	
		FTPS Client	
		Windoçs Update	
	Zone 4	Active Directory PC	
		Antivirus Server	
	Zone 5	Proxy	
	Zone 6	Admin PCs	
		Developers PCs	
	Interconnecting Zones Area	Call Center	
		Admins PCs	
		Devs (Devices)	
		PFSense FW	
		Proxy Server	
		NCC (Injenico)	
		150-2a.EX5	150-2a.EX5
		Cisco 2960 (Node 1)	
		Cisco 2960 (Node 2)	
		APV 1600 (Node 2)	ArrayOS Rel.APV.8.4.0.56
		APV 1600 (Node 1)	ArrayOS Rel.APV.8.4.0.56
		77,20 Checkpoint 4406	R77.20
		77,20 Checkpoint 4406	R77.20
		Sophos FW (VPN/NTP & IDS/IPS)	9.3
CDE (Disaster)	**Disaster Zone**	APV 1600	ArrayOS Rel.APV.8.5.0.64
		77,20 Checkpoint 4406	R77.20
		Cisco 2960CX	152-3.E
		NCC (Injenico)	

Πίνακας 5: Το σύνολο των αγαθών της κρίσιμης υποδομής του σεναρίου προσομοίωσης

3.3. ΣΚΟΠΟΣ ΜΕΛΕΤΗΣ ΣΥΓΚΕΚΡΙΜΕΝΟΥ ΣΕΝΑΡΙΟΥ

Όπως αναφέρθηκε στην Εισαγωγή, ο συγκεκριμένος υπό μελέτη οργανισμός αποτελεί μέρος κρίσιμης υποδομής. Έχει επιλεχθεί ο συγκεκριμένος οργανισμός με στόχο να βρεθεί η καταλληλότερη μεθοδολογία για την υλοποίηση ανάλυσης επικινδυνότητας σε αυτόν, όπως απαιτείται από τα διεθνή πρότυπα τα οποία διέπουν την λειτουργία αυτού. Σκοπός μελέτης του συγκεκριμένου σεναρίου είναι η σύγκριση της ανάλυσης επικινδυνότητας των ανωτέρων μεθοδολογιών, και όχι η σύγκριση και των προτεινόμενων αντιμέτρων των μεθοδολογιών.

Για την εκπόνηση των κατάλληλων αντιμέτρων και των προτάσεων ενδυνάμωσης της υποδομής του συγκεκριμένου οργανισμού απαιτείται η υλοποίηση ελέγχου διείσδυσης (penetration test). Ακολούθως, μετά την εφαρμογή των αντιμέτρων και της ενδυνάμωσης θα πρέπει να πραγματοποιηθεί ξανά ανάλυση επικινδυνότητας. Αυτό δεν αποτελεί μέρος της παρούσας μεταπτυχιακής διατριβής.

4. ΠΡΟΣΟΜΟΙΩΣΗ ΣΕΝΑΡΙΟΥ

4.1. ΕΡΓΑΛΕΙΑ ΠΟΥ ΘΑ ΧΡΗΣΙΜΟΠΟΙΗΘΟΥΝ

Κάθε μεθοδολογία, όπως αναλύθηκε και σε παραπάνω κεφάλαιο, χρησιμοποιεί ένα δικό της εργαλείο για να εφαρμοστούν τα μαθηματικά μοντέλα και να εξαχθούν αποτέλεσμα σε μορφές αξιοποιήσιμες από τους τους οργανισμούς που αποτελούν κρίσιμες υποδομές. Έτσι και για το σενάριο του χρηματοπιστωτικού ιδρύματος και ειδικότερα το κομμάτι του IT που εμπλέκεται στην εκτέλεση διατραπεζικών συναλλαγών χρησιμοποιήθηκαν για κάθε μεθοδολογία (CRAMM, MAGERIT και MEHARI) τα κατάλληλα εργαλεία.

Πιο συγκεκριμένα για την υλοποίηση της προσομοίωσης της μεθοδολογίας ανάλυσης επικινδυνότητας CRAMM χρησιμοποιήθηκε μια φόρμα υπολογιστικού φύλλου (MS Excel) στην ελληνική γλώσσα που προσαρμόστηκε στα είδη των αγαθών και των υπηρεσιών που περιλαμβάνει το σενάριο που έχει επιλεγεί.

Για την υλοποίηση της προσομοίωσης της μεθοδολογίας ανάλυσης επικινδυνότητας MAGERIT χρησιμοποιήθηκε ως εργαλείο το πρόγραμμα PILAR 6.2.6 (24.4.2017**)** που κατασκεύασαν οι ίδιοι οι δημιουργοί της μεθοδολογίας αυτής. Η άδεια που χρησιμοποιήθηκε ήταν evaluation license και είχε διάρκεια για ένα (1) μήνα.

Ενώ, για την μεθοδολογία ανάλυσης επικινδυνότητας MEHARI για να επιτευχθεί η υλοποίηση της προσομοίωσης του επιλεγμένου σεναρίου έγινε χρήση ενός υπολογιστικού φύλλου (MS Excel) στην αγγλική γλώσσα που αποτελεί το εργαλείο της εταιρείας CLUSIF που είναι και οι δημιουργοί της συγκεκριμένης μεθοδολογίας.

Τέλος για την δημιουργία κατάλληλων διαγραμμάτων, με σκοπό την καλύτερη παρουσίαση των αποτελεσμάτων των προσομοιώσεων του επιλεγμένου σεναρίου καθώς και την σύγκριση μεταξύ αυτών, χρησιμοποιήθηκε υπολογιστικό φύλλο (MS Excel).

Για κάθε μεθοδολογία ξεχωριστά, για την συλλογή των απαιτούμενων πληροφοριών που χρησιμοποιήθηκαν ως είσοδοι (inputs) στα παραπάνω εργαλεία, απαιτήθηκε η διενέργεια συγκεκριμένων ερωτηματολογίων που ορίζονται από αυτές σε άτομα που καταλαμβάνουν συγκεκριμένες θέσεις ευθύνης στο τομέα του χρηματοπιστωτικού ιδρύματος του εξεταζόμενου σεναρίου.

Ειδικότερα, διενεργήθηκαν συνεντεύξεις, συμπλήρωση ερωτηματολογίων καθώς και συνεχή ανατροφοδότηση πληροφορίας με τους:

- Προϊστάμενο Ασφαλείας Πληροφοριακών Συστημάτων (Information Security Chief Officer)
- Διαχειριστή Πληροφοριακών Συστημάτων (Information Systems Administrator)
- Διαχειριστή του Δικτύου Πληροφοριακών Συστημάτων (Information Network Administrator)
- Προϊστάμενο Μηχανικό Ασφαλείας Πληροφοριακών Συστημάτων (Information Security Chief Engineer)

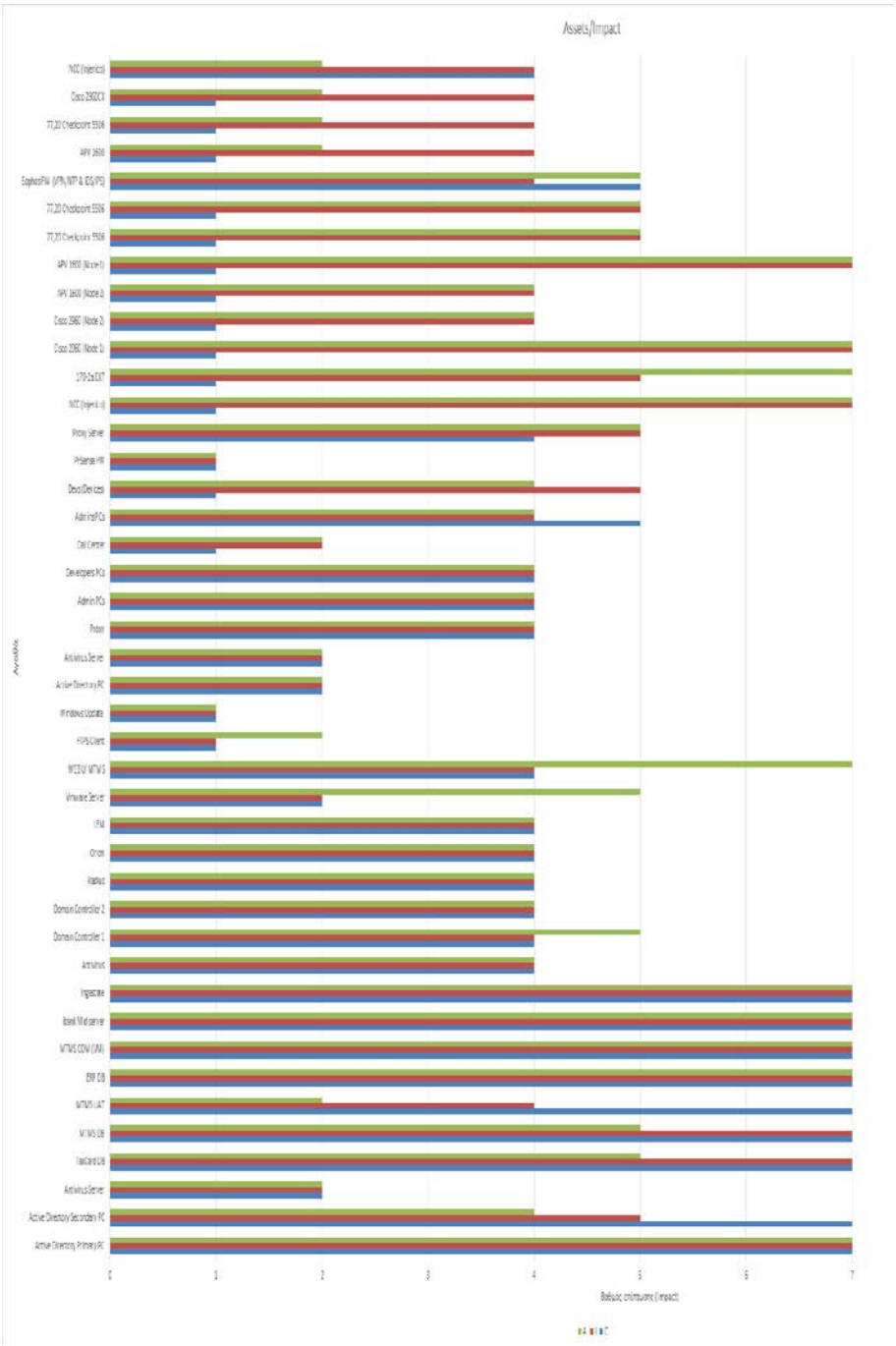
4.2. ΠΡΟΣΟΜΟΙΩΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ CRAMM

Μετά από εκτέλεση των απαιτούμενων προπαρασκευαστικών βημάτων που ορίζει η μεθοδολογία CRAMM, από το εργαλείο (ειδικά διαμορφωμένο υπολογιστικό φύλλο MS Excel) που χρησιμοποιήθηκε προέκυψαν τα παρακάτω αποτελέσματα που αφορούν την αξιολόγηση των αγαθών του σεναρίου ως προς τον βαθμό επίπτωσης (impact) στους τρείς άξονες της Διαθεσιμότητας (Availability-A), Εμπιστευτικότητας (Confidentiality-C) και Ακεραιότητας (Integrity-I).

Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επίπτωσης, όπως αυτό έχει οριστεί από την CRAMM με την εννοιολογική της περιγραφή.

Επίπεδο Επίπτωσης	Περιγραφή
1	Πολύ μικρή επίπτωση
2	Μικρή επίπτωση
3	Μέτρια επίπτωση
4	Σημαντική επίπτωση
5	Μεγάλη επίπτωση
6	Πολύ μεγάλη επίπτωση
7	Κρίσιμη επίπτωση

Πίνακας 6: Η κλίμακα του επιπέδου επίπτωσης (impact) της μεθοδολογίας CRAMM



Διάγραμμα 1**: Το επίπεδο επίπτωσης (**impact**) ανά αγαθό ως προς** A, I **και** C, CRAMM

4.2.1. **Γενικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** CRAMM - **Επίπτωση**

Μετά από μελέτη του ανωτέρω σχήματος προκύπτει ότι ως προς τον άξονα της Διαθεσιμότητας (Availability-A) τα αγαθά που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι τα Active Directory Primary PC, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, NCC (Injenico), Cisco 2960 (Node 1) και το APV 1600 (Node1). Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα TaxCard DB, MTMS DB, Domain Controller 1, VMware Server, Proxy Server τα δυο 77,20 Checkpoint 5506 και το Sophos FW. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality-C) κρίσιμο επίπεδο επίπτωσης παρουσιάζουν τα αγαθά Active Directory Primary PC, Active Directory Secondary PC, TaxCard DB, MTMS DB, MTMS COM (VM), MTMS UAT, ERP DB, ibank Mid Server και Ingestate. Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα Admins PCs και Sophos FW. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Τέλος, ως προς τον άξονα της Ακεραιότητας (Integrity-I) κρίσιμο επίπεδο επίπτωσης παρουσιάζουν τα αγαθά τα Active Directory Primary PC, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, Web UI MTMS, NCC (Injenico), 170.2a.EX7, Cisco 2960 (Node 1) και το APV 1600 (Node1). Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα Active Directory Secondary PC, Devs (Devices), Proxy Server τα δυο 77,20 Checkpoint 5506. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Στην συνέχεια, γίνεται παράθεση και σχολιασμός των αποτελεσμάτων του επιπέδου επικινδυνότητας (risk) κάθε αγαθού συναρτήσει των κινδύνων που πρόκειται να αντιμετωπίσει κατά την λειτουργία του.

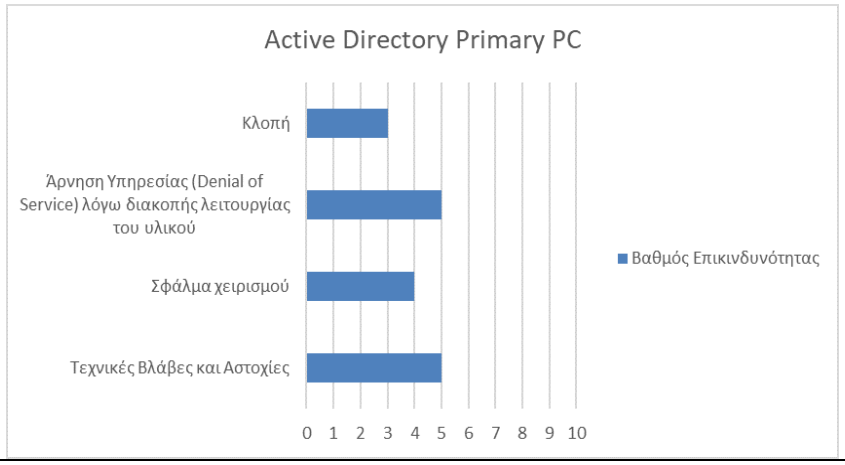
Η CRAMM ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν μόνο την μέγιστη τιμή της επίπτωσης (impact) μεταξύ των τριών (3) αξόνων (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα) για κάθε απειλή που πλήττει το αγαθό. Συνεπώς η επικινδυνότητα που προκύπτει για κάθε απειλή κάθε αγαθού παρουσιάζεται ως μία μπάρα αφού η τιμή της είναι κοινή και για του τρείς άξονες μελέτης.

Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από την CRAMM με την εννοιολογική της περιγραφή.

Επίπεδο Επικινδυνότητας	Περιγραφή
1	Πολύ μικρός κίνδυνος
2	Μικρός κίνδυνος
3	Μέτριος κίνδυνος
4	Σημαντικός κίνδυνος
5	Μεγάλος κίνδυνος
6	Πολύ μεγάλος κίνδυνος
7	Κρίσιμος κίνδυνος

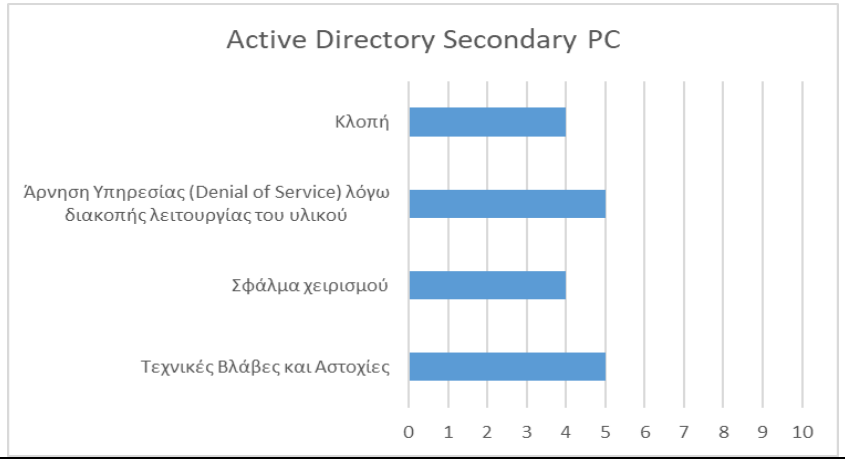
Πίνακας 7**: Η κλίμακα του επιπέδου επικινδυνότητας της μεθοδολογίας** CRAMM

4.2.2. **Αναλυτικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** CRAMM- **Επικινδυνότητα**



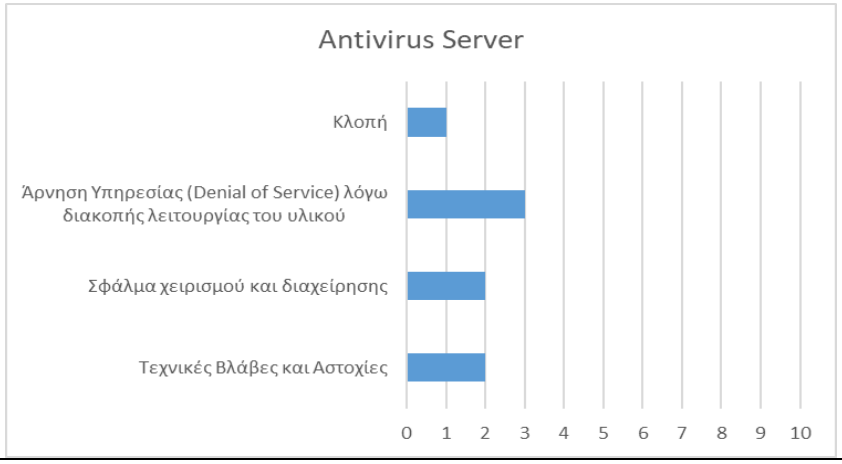
Διάγραμμα 2: Active Directory Primary PC/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active Directory Primary PC, δηλαδή ο κύριος server που έχει εγκατεστημένο το Active Directory. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας και στις Τεχνικές Βλάβες και Αστοχίες.



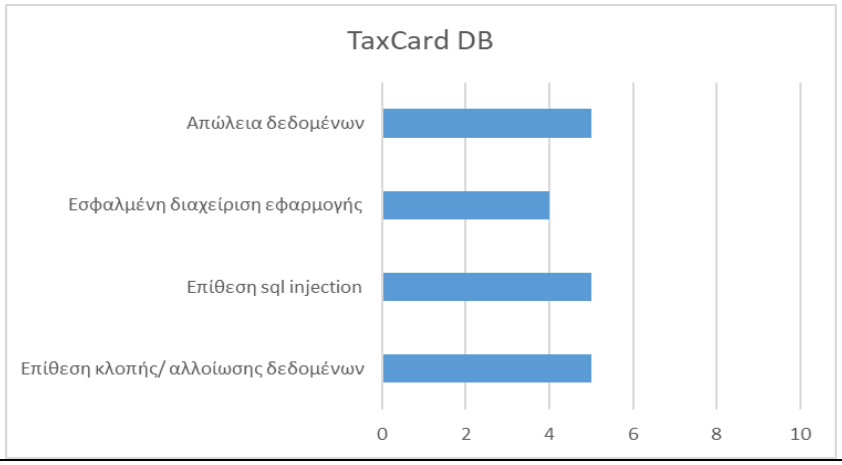
Διάγραμμα 3: Active Directory Secondary PC/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active Directory Secondary PC, δηλαδή ο κύριος server που έχει εγκατεστημένο το Active Directory. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας και στις Τεχνικές Βλάβες και Αστοχίες.



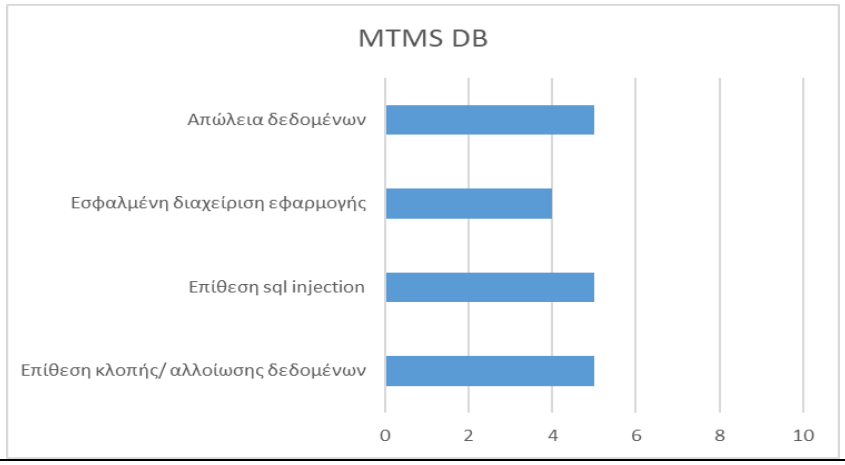
Διάγραμμα 4: Antivirus Server/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus Server, δηλαδή ο server που έχει εγκατεστημένο πρόγραμμα antivirus για την προστασία του πληροφοριακού συστήματος από κακόβουλα λογισμικά ή ιούς που μπορεί να εισέλθουν στο σύστημα. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



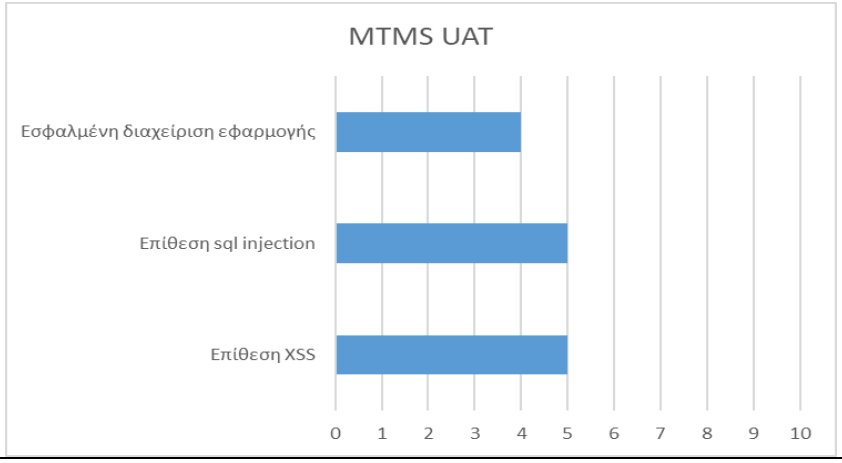
Διάγραμμα 5: TaxCard DB/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού TaxCard DB, δηλαδή την βάση δεδομένων (Data Base) που περιέχει τους πελάτες του χρηματοπιστωτικού ιδρύματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Απώλεια Δεδομένων την επίθεση SQL injection και την Επίθεση κλοπής/ αλλοίωσης δεδομένων.



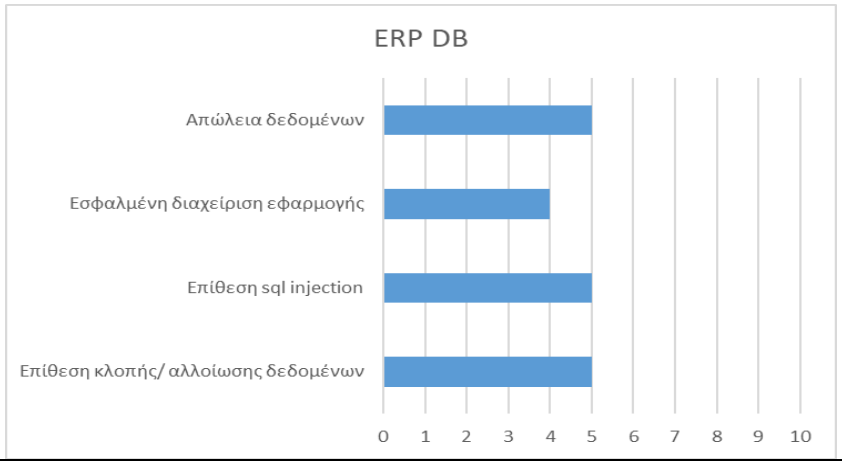
Διάγραμμα 6: MTMS DB/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS DB, δηλαδή την βάση δεδομένων (Data Base) που περιέχει πολλαπλά επίπεδα (Multi-Tier Management System) με σκοπό την ταυτοποίηση των πελατών του χρηματοπιστωτικού ιδρύματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Απώλεια Δεδομένων την Επίθεση SQL injection και την Επίθεση κλοπής/ αλλοίωσης δεδομένων.



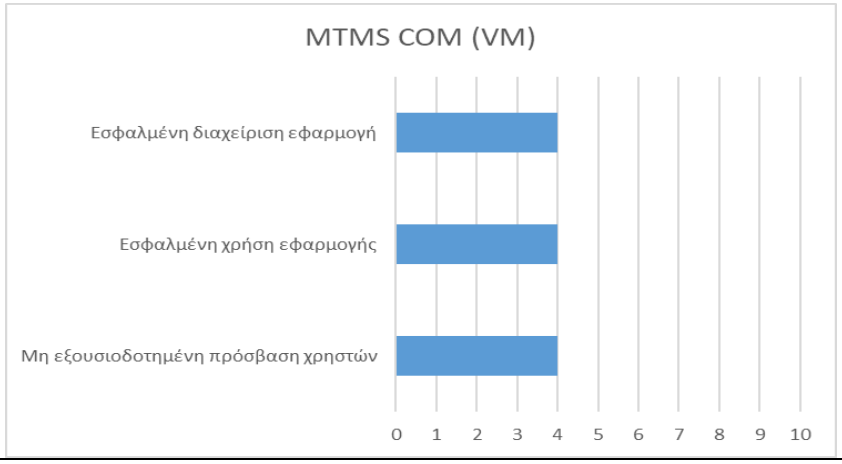
Διάγραμμα 7: MTMS UAT/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS UAT, δηλαδή το λογισμικό Multi-Tier Management System User acceptance testing που χρησιμοποιείται με σκοπό τον έλεγχο της εφικτότητας των απαιτήσεων των πελατών του χρηματοπιστωτικού ιδρύματος σε πραγματικό χρόνο σενάρια. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Επίθεση SQL injection και την επίθεση XSS (Cross-site Scripting).



Διάγραμμα 8: ERP DB/ risk CRAMM

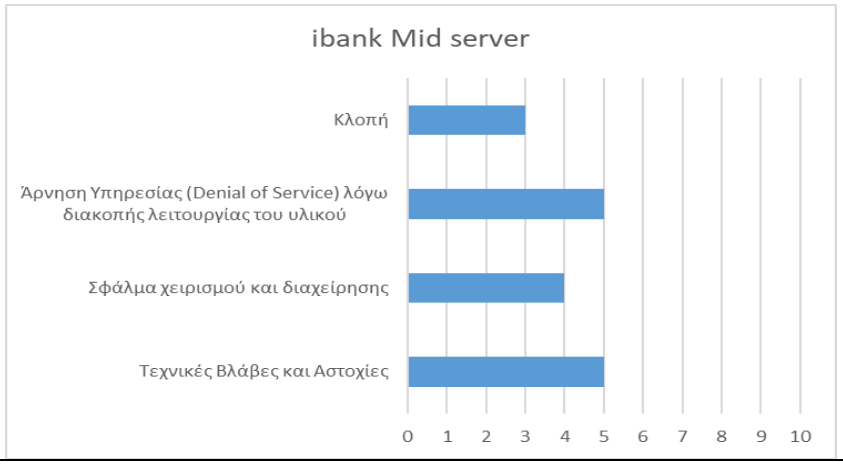
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ERP DB, δηλαδή την βάση δεδομένων (Data Base) του συστήματα ενδοεπιχειρησιακού σχεδιασμού (enterprise resource planning, ERP) με σκοπό να διευκολύνουν τη ροή των πληροφοριών μεταξύ όλων των επιχειρησιακών λειτουργιών μέσα στα όρια της οργάνωσης και να καταφέρουν τις συνδέσεις προς τα έξω με τα ενδιαφερόμενα μέρη. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Απώλεια Δεδομένων την Επίθεση SQL injection και την Επίθεση κλοπής/ αλλοίωσης δεδομένων.



Διάγραμμα 9: MTMS COM (VM)/ risk CRAMM

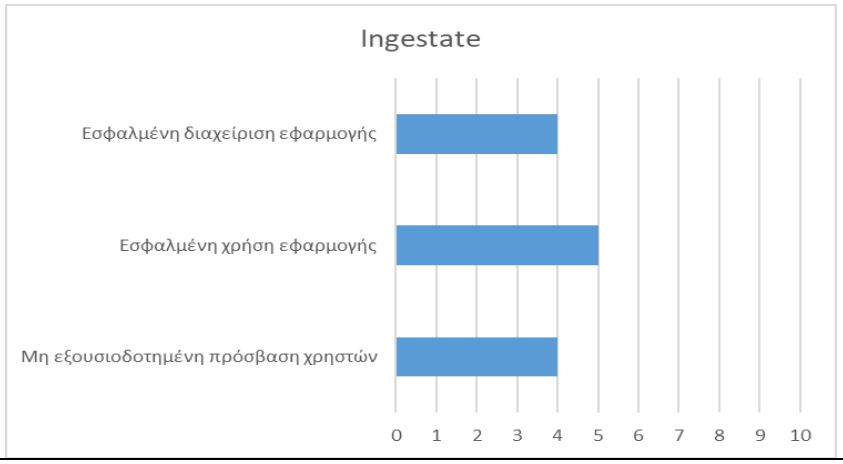
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS COM (VM), δηλαδή το εικονικό μηχάνημα (Virtual Machine) του MTMS συστήματος που είναι υπεύθυνο για την παρακολούθηση και έλεγχο της ομαλής επικοινωνίας μεταξύ των πολλαπλών επιπέδων. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι

στην Εσφαλμένη διαχείριση της εφαρμογής, την Εσφαλμένη χρήση της εφαρμογής και την Μη εξουσιοδοτούμενη πρόσβαση χρηστών.



Διάγραμμα 10: ibank Mid Server/ risk CRAMM

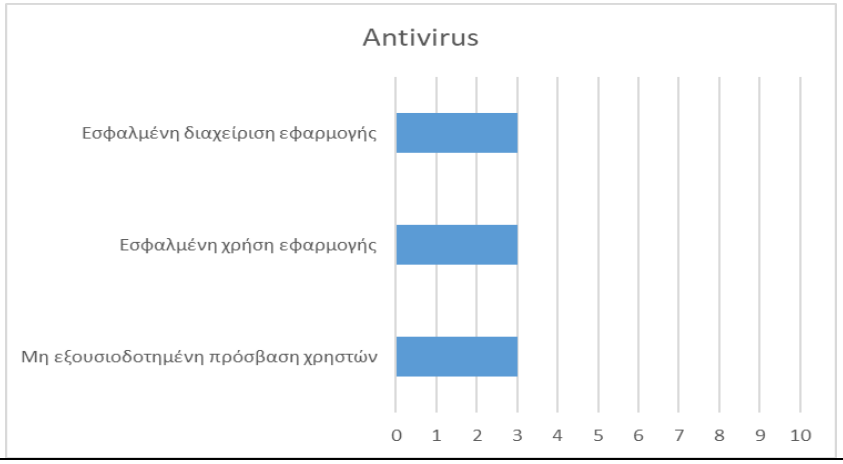
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ibank Mid Server, δηλαδή ο ενδιάμεσος server που έχει εγκατεστημένο το πρόγραμμα των διαδικτυακών εφαρμογών (ibank) του χρηματοπιστωτικού ιδρύματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας και στις Τεχνικές Βλάβες και Αστοχίες.



Διάγραμμα 11: Ingestate/ risk CRAMM

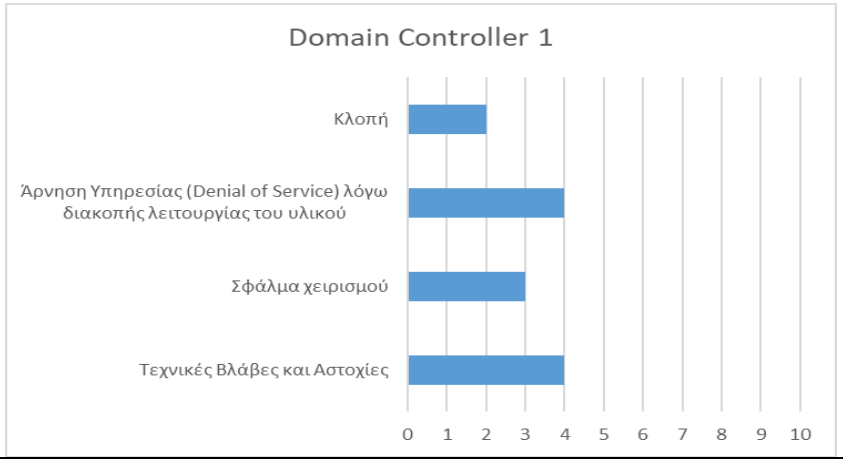
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Ingestate, δηλαδή η πλατφόρμα που δίνει την δυνατότητα στου διαχειριστές του συστήματος να έχουν τον έλεγχο του συνόλου των τερματικών του συστήματος καθώς και του λογισμικού που έχουν

αυτά. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη χρήση εφαρμογής



Διάγραμμα 12: Antivirus/ risk CRAMM

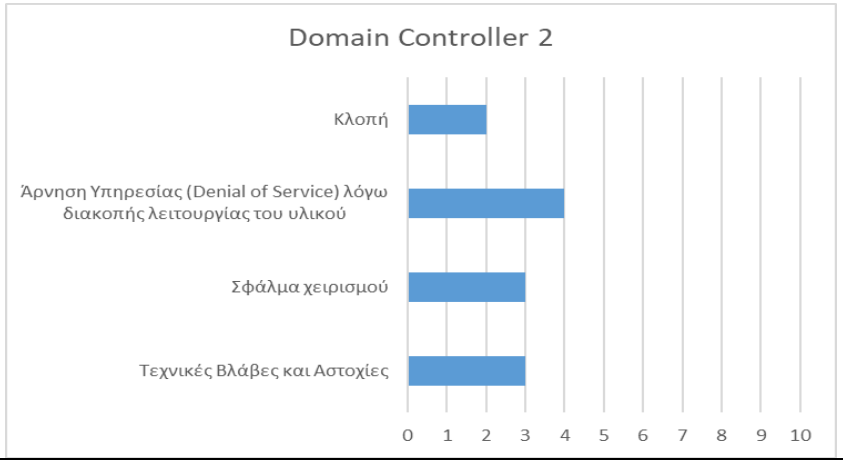
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus, δηλαδή το πρόγραμμα antivirus για την προστασία του πληροφοριακού συστήματος από κακόβουλα λογισμικά ή ιούς που μπορεί να εισέλθουν στο σύστημα. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής, Εσφαλμένη χρήση εφαρμογής και την Μη εξουσιοδοτούμενη πρόσβαση χρηστών.



Διάγραμμα 13: Domain Controller 1/ risk CRAMM

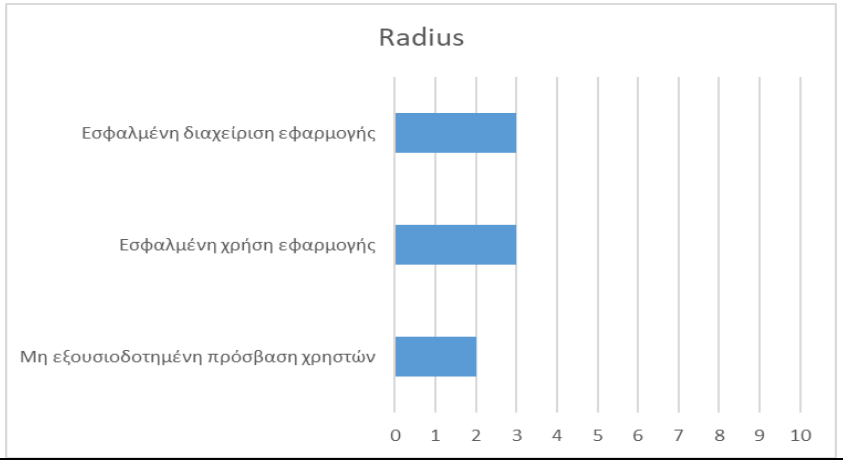
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Domain Controller 1, δηλαδή ο κύριος ελεγκτής του IT τομέα. Συγκεκριμένα, το αγαθό αυτό

έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας και στις Τεχνικές Βλάβες και Αστοχίες.



Διάγραμμα 14: Domain Controller 2/ risk CRAMM

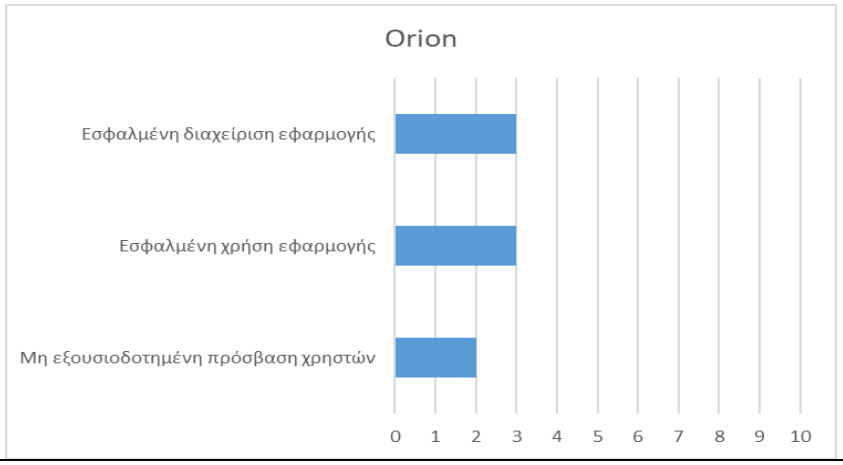
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Domain Controller 2, δηλαδή ο δευτερεύων (σε περίπτωση απώλειας του κύριου) ελεγκτής του IT τομέα. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας.



Διάγραμμα 15: Radius/ risk CRAMM

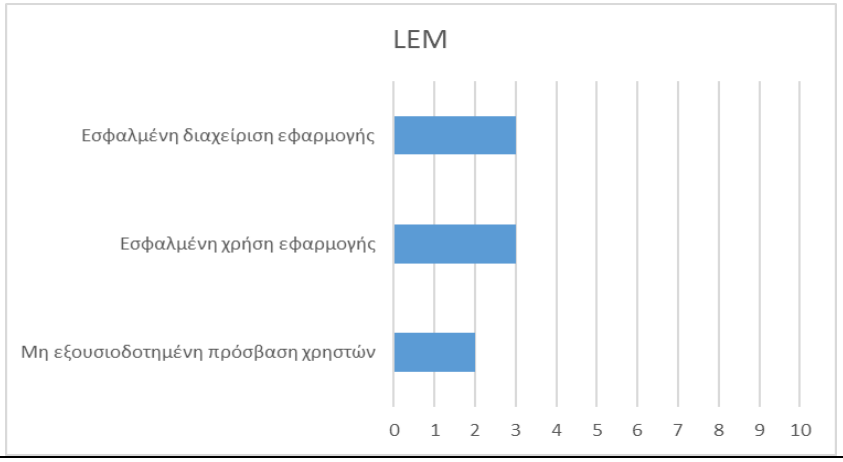
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού RADIUS, δηλαδή ένα λογισμικό που είναι υπεύθυνο για την υπηρεσία απομακρυσμένης επαλήθευσης ταυτότητας από απόσταση (RADIUS) που παρέχει διαχείριση κεντρικού ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής για χρήστες που συνδέουν και χρησιμοποιούν μια υπηρεσία

δικτύου. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής και Εσφαλμένη χρήση εφαρμογής.



Διάγραμμα 16: Orion/ risk CRAMM

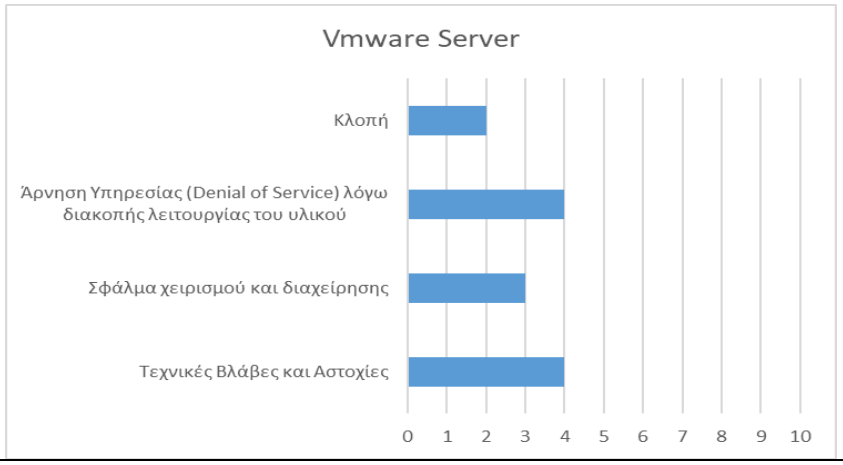
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ORION, δηλαδή ένα Java EE (Enterprise Edition) application server. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής και Εσφαλμένη χρήση εφαρμογής.



Διάγραμμα 17: LEM/ risk CRAMM

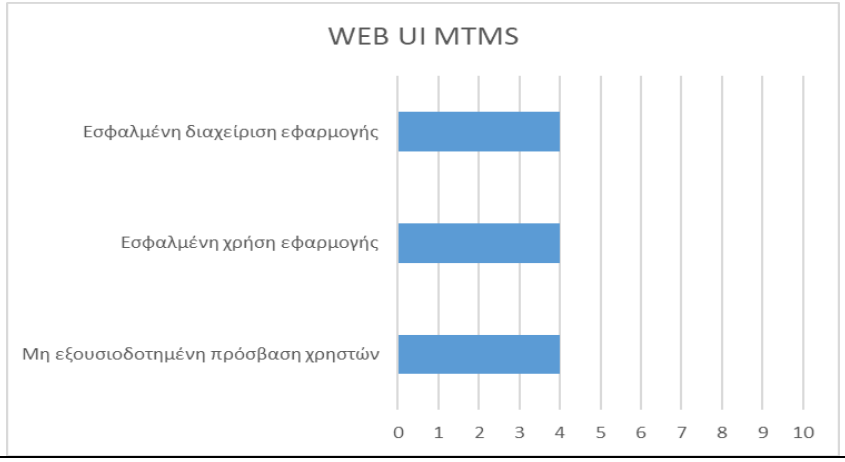
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού LEM (Log & Event Manager), δηλαδή ένα λογισμικό διαχείρισης ημερολογίου (log) για ασφάλεια, συμμόρφωση και αντιμετώπιση προβλημάτων του συστήματος. Συγκεκριμένα, το αγαθό αυτό

έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής και Εσφαλμένη χρήση εφαρμογής.



Διάγραμμα 18: VMware Server/ risk CRAMM

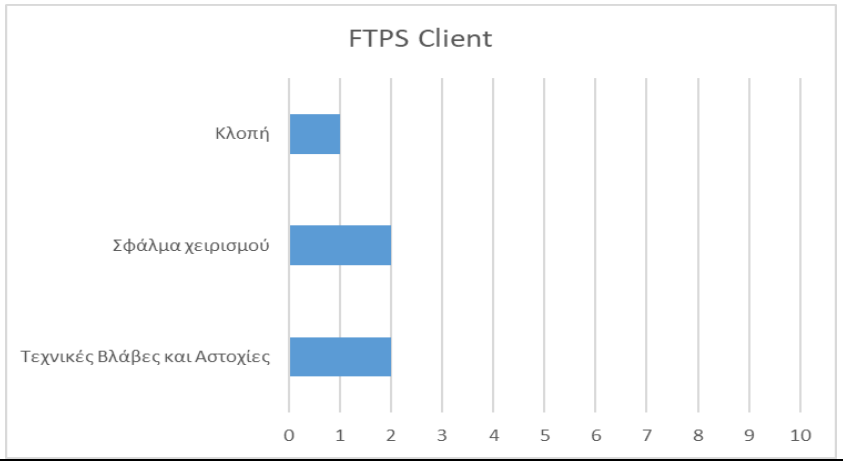
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active VMware server, δηλαδή ο εικονικό μηχάνημα που έχει λειτουργεί ως βοηθητικός sever στις για την υλοποίηση διατραπεζικών συναλλαγών. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας και στις Τεχνικές Βλάβες και Αστοχίες.



Διάγραμμα 19: WEB UI MTMS/ risk CRAMM

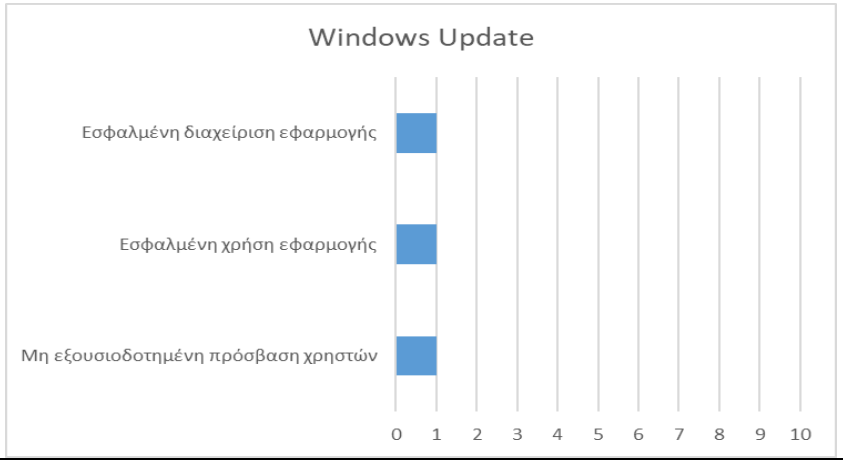
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού WEB UI MTMS, δηλαδή το λογισμικό Web User Interface του Multi-Tier Management System που χρησιμοποιείται με σκοπό το την διεπαφή των χρηστών του συστήματος με το MTMS.

Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής, Εσφαλμένη χρήση εφαρμογής και την Μη εξουσιοδοτημένη πρόσβαση χρηστών.



Διάγραμμα 20: FTPS Client/ risk CRAMM

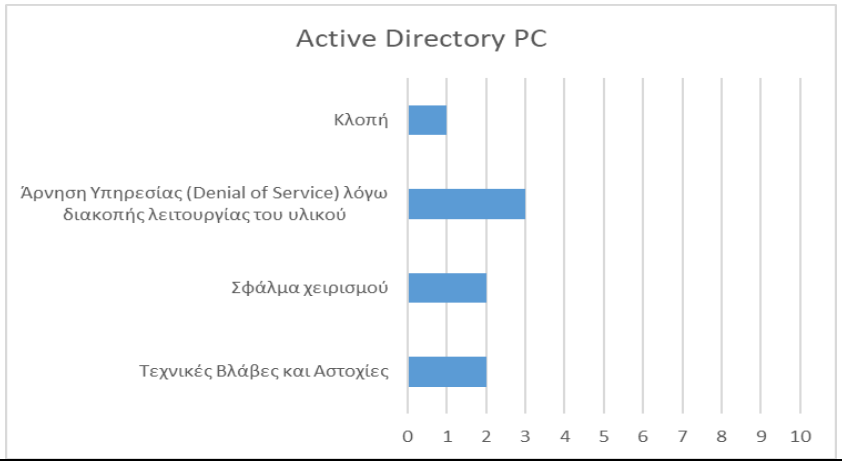
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού FTPS Client, δηλαδή το λογισμικό που χρησιμοποιείται με σκοπό το την διεπαφή ενός χρήστη του συστήματος με τον FTPS Server. Συγκεκριμένα, το αγαθό αυτό έχει μικρό βαθμό επικινδυνότητας απέναντι στο Σφάλμα χειρισμού και στις Τεχνικές Βλάβες και Αστοχίες.



Διάγραμμα 21: Windows Update/ risk CRAMM

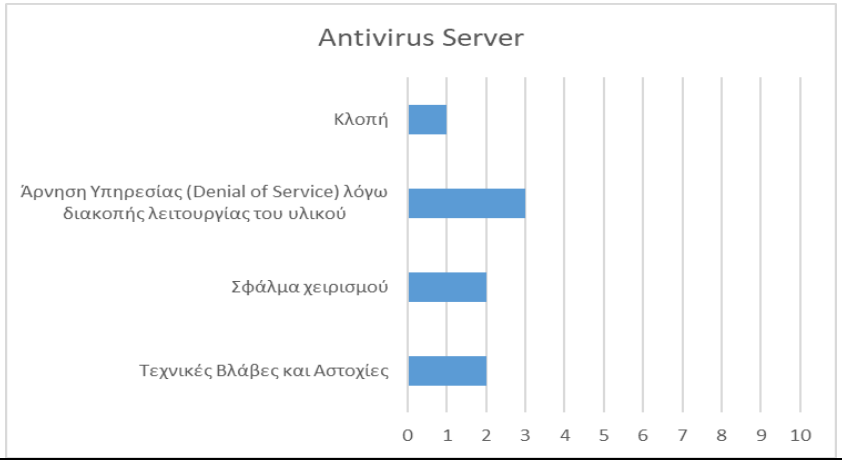
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμούWindows Update, δηλαδή το λογισμικό που χρησιμοποιείται με σκοπό τον έλεγχο και την εκτέλεση ενημερώσεων των Windows μηχανημάτων του συστήματος. Συγκεκριμένα, το αγαθό αυτό

έχει πολύ μικρό βαθμό επικινδυνότητας απέναντι στην Εσφαλμένη διαχείριση εφαρμογής, Εσφαλμένη χρήση εφαρμογής και την Μη εξουσιοδοτημένη πρόσβαση χρηστών.



Διάγραμμα 22: Active Directory Pc/ risk CRAMM

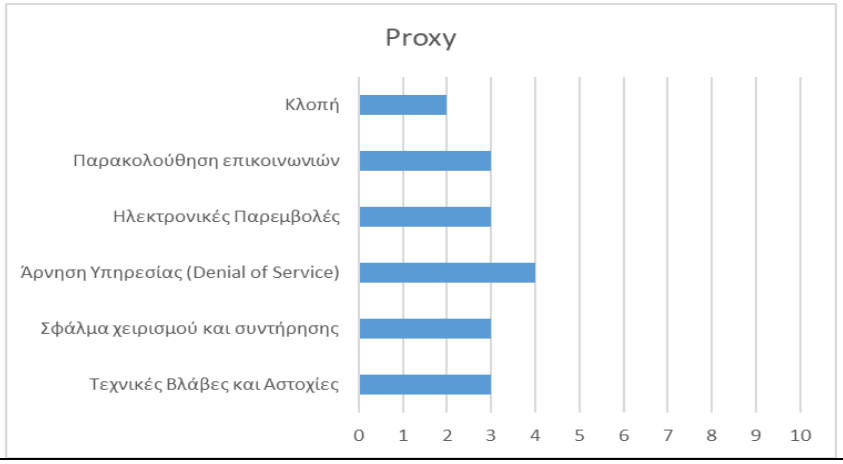
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active Directory PC, δηλαδή ένας τρίτος server σε άλλη ζώνη του τομέα που έχει εγκατεστημένο το Active Directory. Συγκεκριμένα, το αγαθό αυτό έχει μικρό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας.



Διάγραμμα 23: Antivirus Server/ risk CRAMM

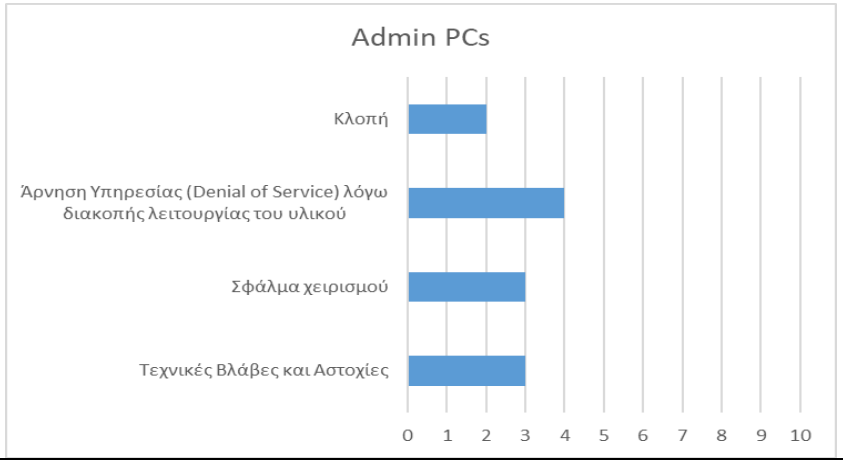
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus Server, δηλαδή ο δεύτερος server σε άλλη ζώνη του τομέα που έχει εγκατεστημένο πρόγραμμα antivirus για την προστασία του πληροφοριακού συστήματος από κακόβουλα

λογισμικά ή ιούς που μπορεί να εισέλθουν στο σύστημα. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



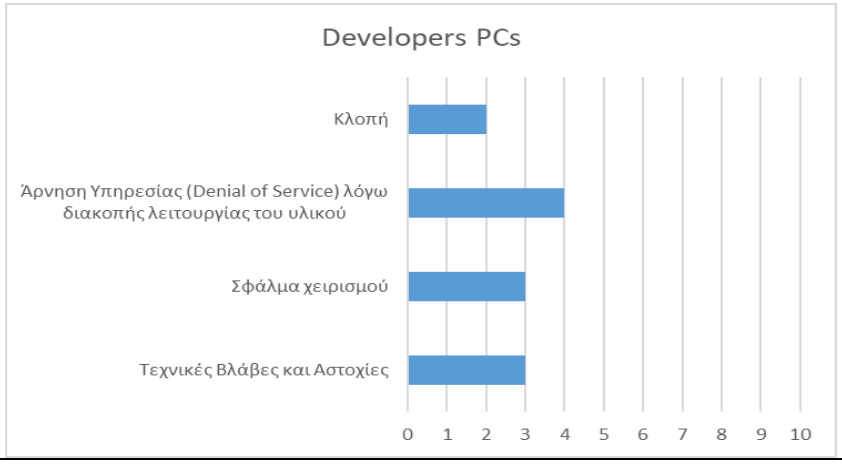
Διάγραμμα 24: Proxy/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Proxy server, δηλαδή ο server που σκοπό έχει να λειτουργεί ως διαμεσολαβητής μεταξύ των διαφόρων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



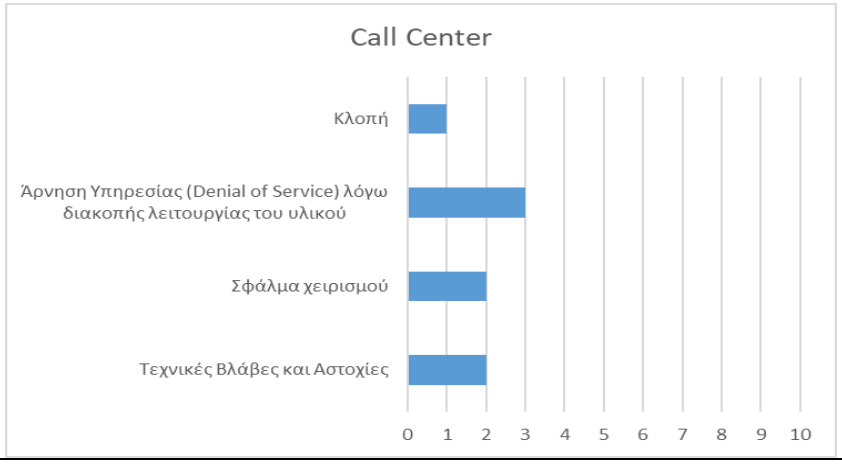
Διάγραμμα 25: Admin PCs/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Admin PCs, δηλαδή τα τερματικά που χρησιμοποιούνται για την διαχείριση του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



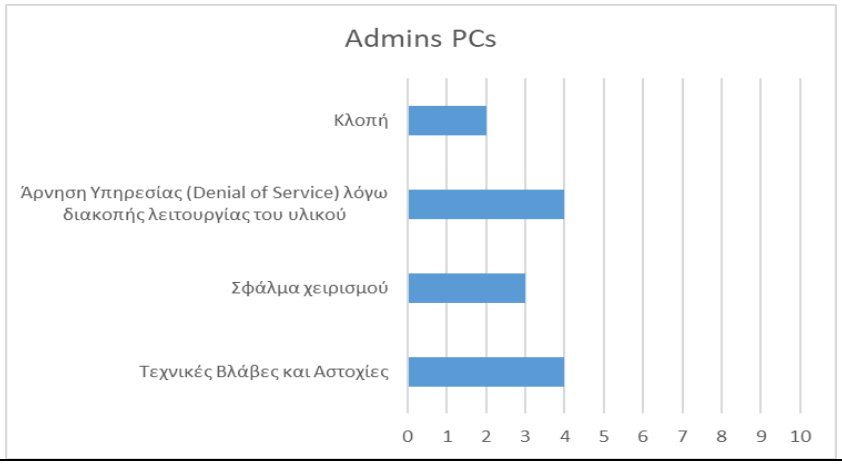
Διάγραμμα 26: Developers PCs/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Developers PCs, δηλαδή τα τερματικά που χρησιμοποιούνται για την ανάπτυξη και τροποποίηση του IT κομματιού του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



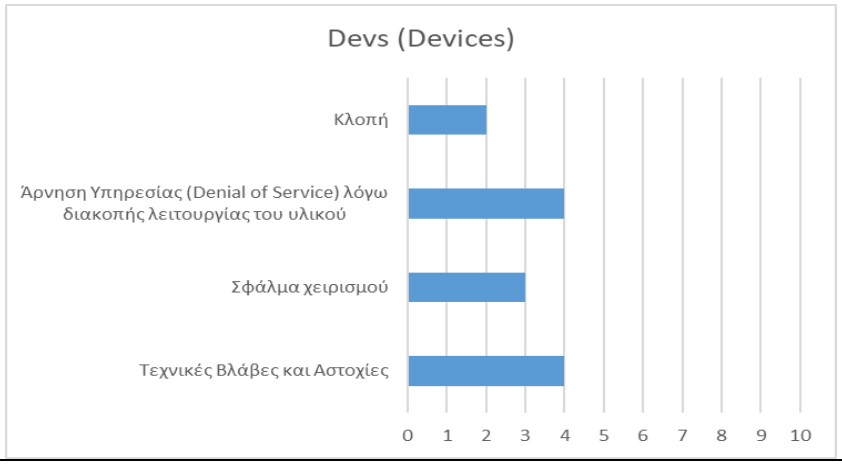
Διάγραμμα 27: Call Center/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Call Center, δηλαδή τα τερματικά και το τηλεφωνικό κέντρο που χρησιμοποιούνται για την διεπικοινωνία μεταξύ των χρηστών του συστήματος καθώς και των πελατών του τραπεζικού συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μέτριο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



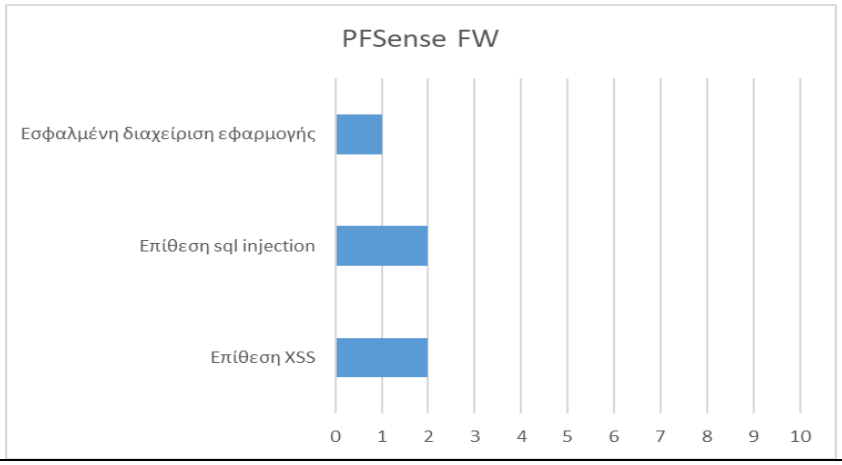
Διάγραμμα 28: Admins PCs/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Admins PCs, δηλαδή μια δεύτερη ομάδα τερματικών που χρησιμοποιούνται για την διαχείριση του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



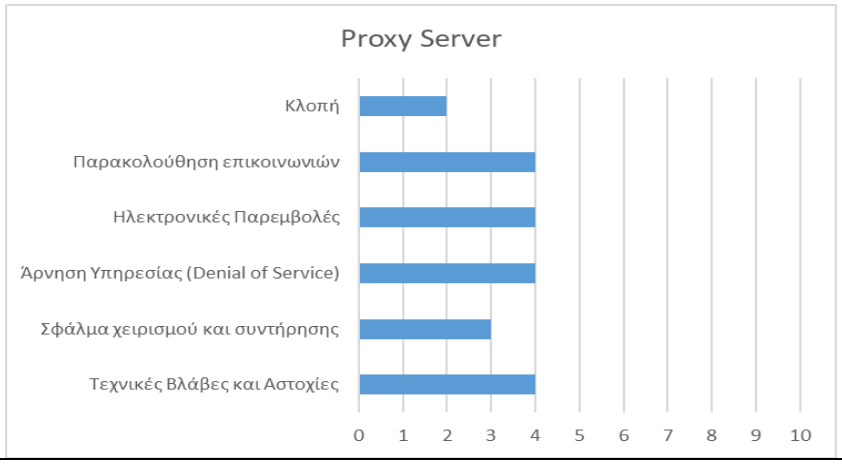
Διάγραμμα 29: Devs (Devices) / risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Devs (Devices), δηλαδή τα περιφερειακά και λοιπές μονάδες εισόδου και εξόδου χρησιμοποιούνται για την ομαλή λειτουργία του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



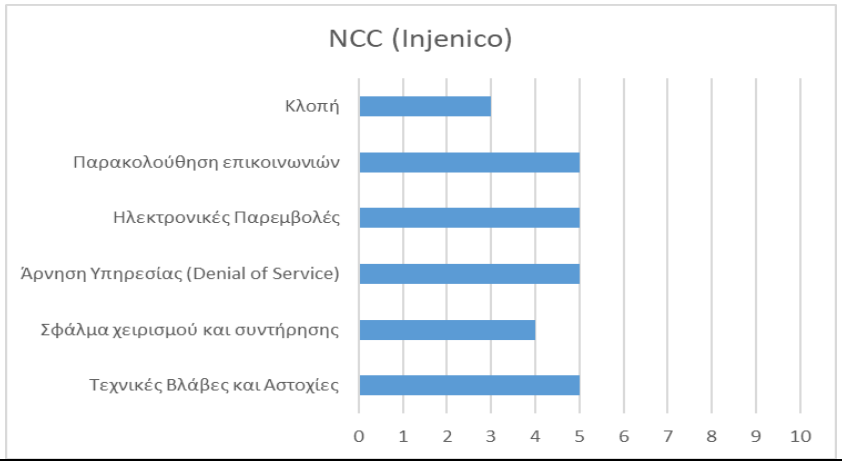
Διάγραμμα 30: PFSense FW/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού PFSense FW, δηλαδή το "τείχος" προστασίας (Firewall) που έχει ως σκοπό το "φιλτράρισμα", έλεγχο των εισόδων και εξόδων μεταξύ των διαφόρων servers του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μικρό βαθμό επικινδυνότητας απέναντι στην Επίθεση SQL injection και την Επίθεση XSS.



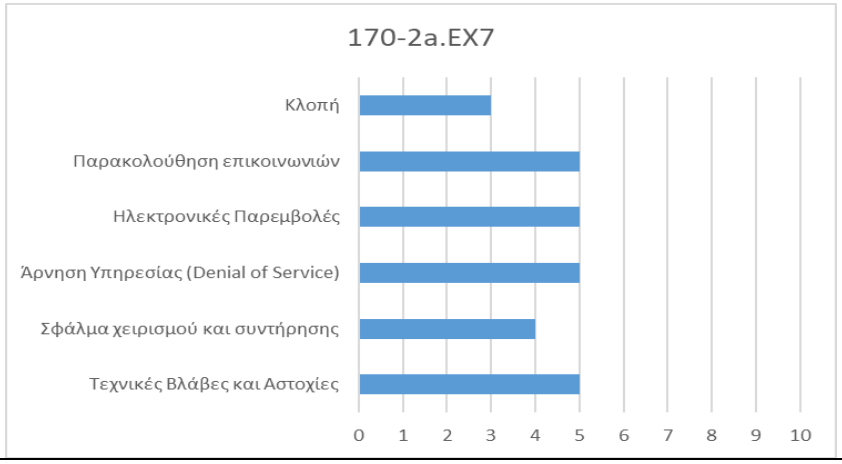
Διάγραμμα 31: Proxy Server/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Proxy server, δηλαδή ένας δεύτερος server που λειτουργεί ως διαμεσολαβητής μεταξύ των διαφόρων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



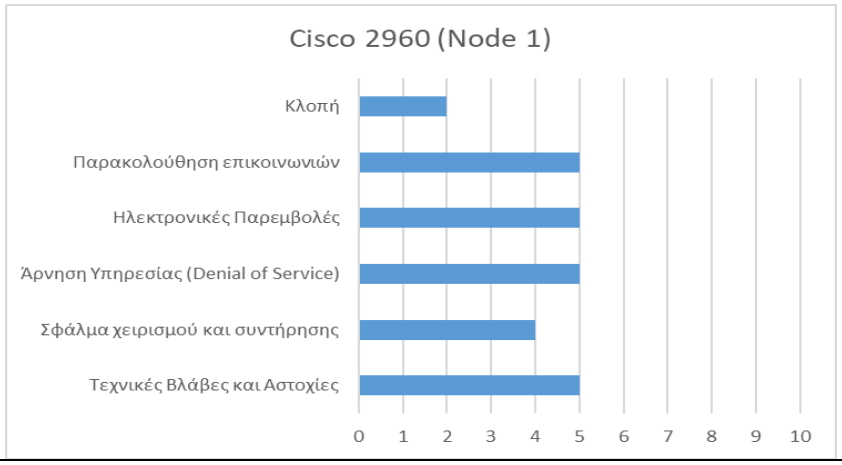
Διάγραμμα 32: NCC (Injenico)/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού NCC (Injenico), δηλαδή ο ελεγκτής (controller) που σκοπό έχει να παρακολουθεί και δρομολογεί τις συναλλαγές των πελατών μεταξύ των κατάλληλων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



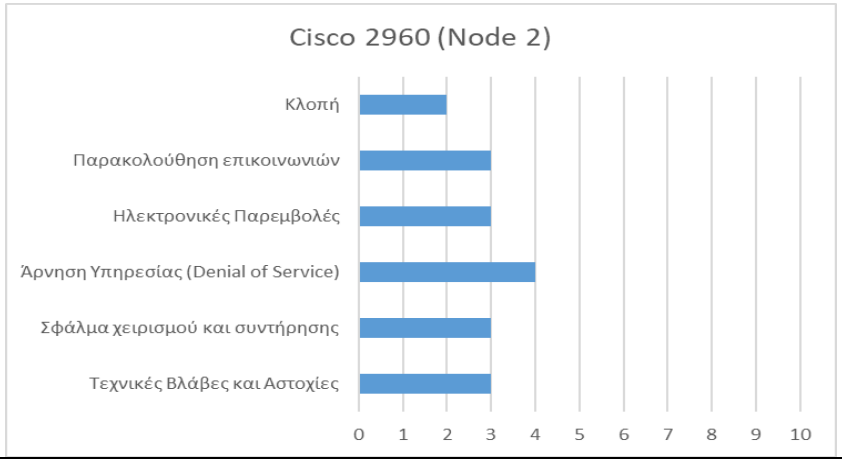
Διάγραμμα 33: 170-2a.EX7/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 170-2a.EX7, δηλαδή ο δρομολογητής/ ελεγκτής (switch) που σκοπό έχει να δρομολογεί/ ελέγχει την επικοινωνία των τερματικών και των περιφερειακών συσκευών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



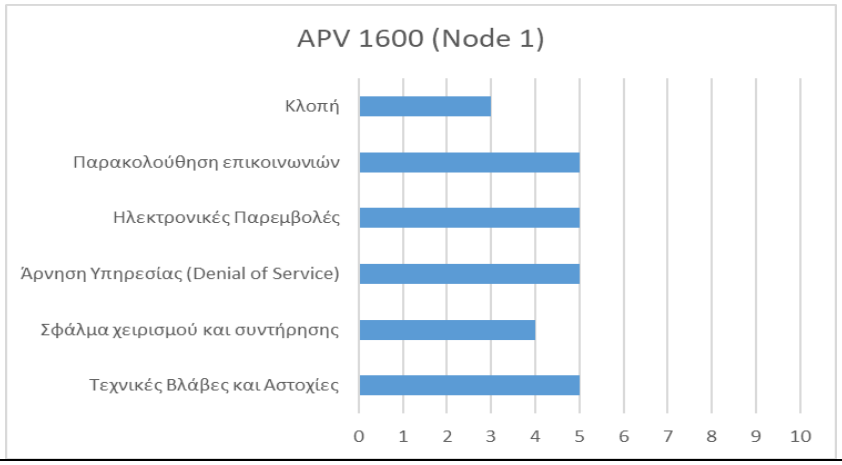
Διάγραμμα 34: Cisco 2960 (Node 1) / risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960 (Node 1), δηλαδή ο κόμβος που σκοπό έχει να δρομολογεί σημαντικές πληροφορίες μεταξύ διαφόρων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



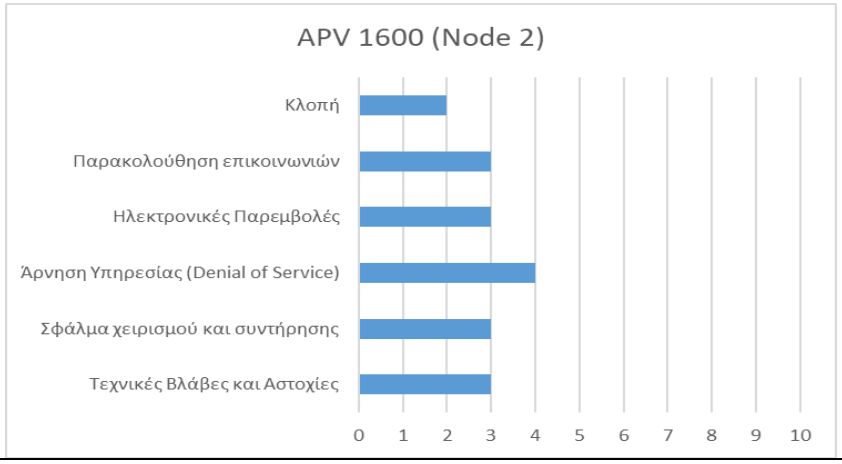
Διάγραμμα 35: Cisco 2960 (Node 2) / risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960 (Node 2), δηλαδή ο κόμβος που σκοπό έχει να δρομολογεί δευτερεύουσας σημασίας πληροφορίες μεταξύ διαφόρων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



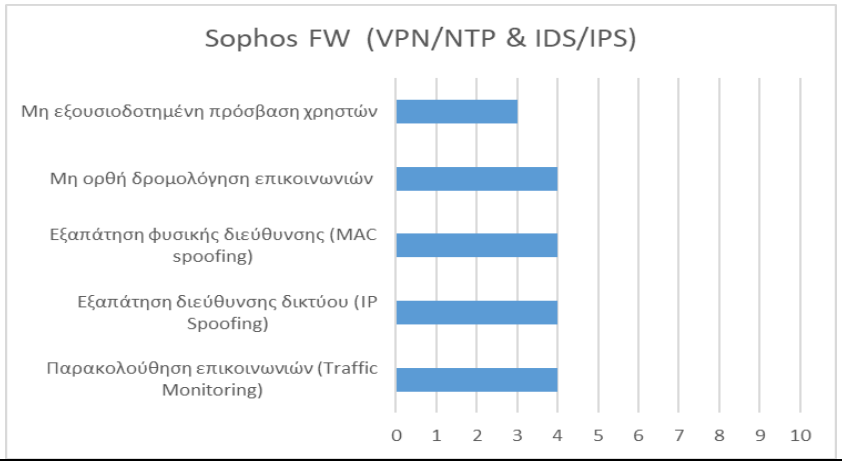
Διάγραμμα 36: APV 1600 (Node 1) / risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 1), δηλαδή ο ελεγκτής/ κόμβος των εφαρμογών του συστήματος (Application Delivery Controllers) που σκοπό έχει να ελέγχει την λειτουργεία των σημαντικών εφαρμογών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



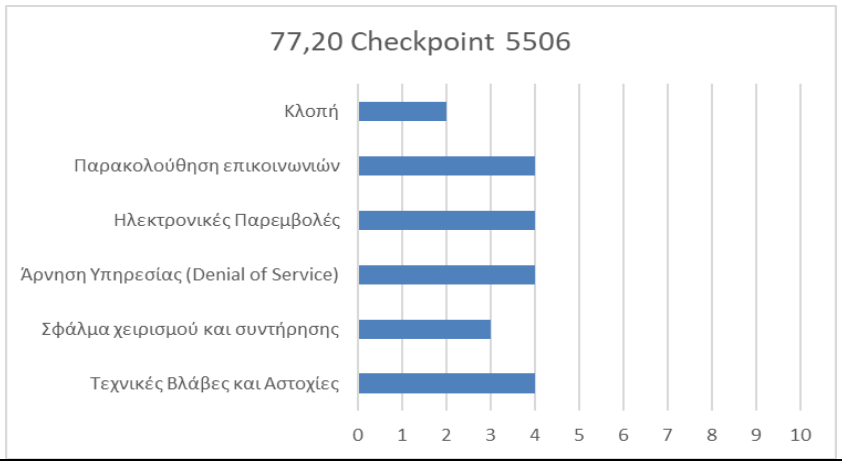
Διάγραμμα 37: APV 1600 (Node 2) / risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 2), δηλαδή ο ελεγκτής/ κόμβος των εφαρμογών του συστήματος (Application Delivery Controllers) που σκοπό έχει να ελέγχει την λειτουργεία των δευτερευουσών εφαρμογών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μεγάλο βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



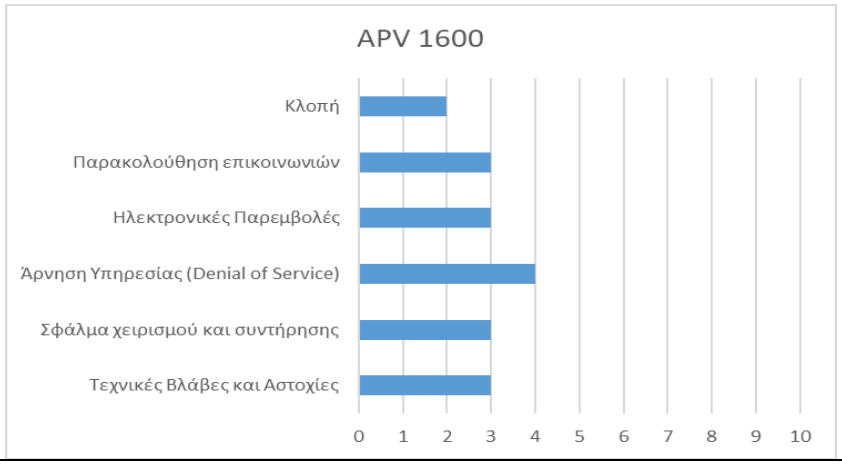
Διάγραμμα 38: SOFOS FW/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού PFSense FW, δηλαδή το δικτυακό "τείχος" προστασίας (Firewall) που έχει ως σκοπό το "φιλτράρισμα", έλεγχο του δικτυακού κομματιού του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Μη ορθή δρομολόγηση επικοινωνιών, Εξαπάτηση φυσικής διεύθυνσης (MAC spoofing), Εξαπάτηση διεύθυνσης δικτύου (IP spoofing) και την Παρακολούθηση επικοινωνιών (Traffic Monitoring).



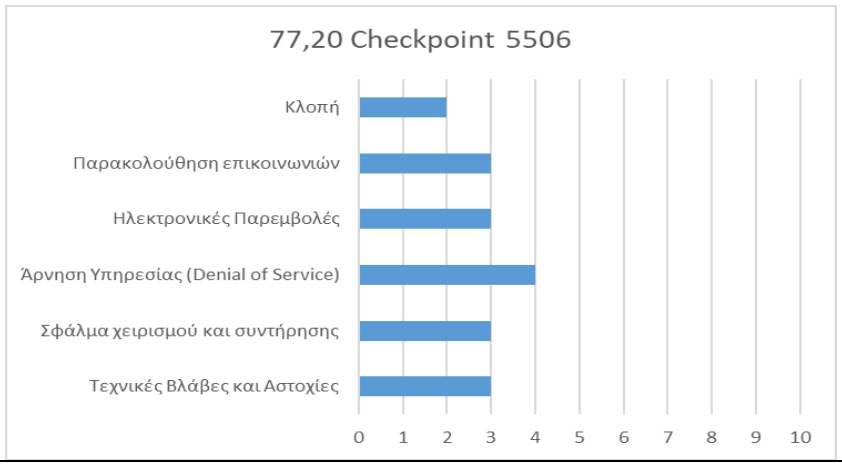
Διάγραμμα 39: 77,20 Checkpoint 5506/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 77,20 Checkpoint 5506, δηλαδή ο το μηχάνημα και η πλατφόρμα λογισμικού που σκοπό έχει να ελέγχει την ασφάλεια επικοινωνιών μεταξύ εφαρμογών του συστήματος.Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες.



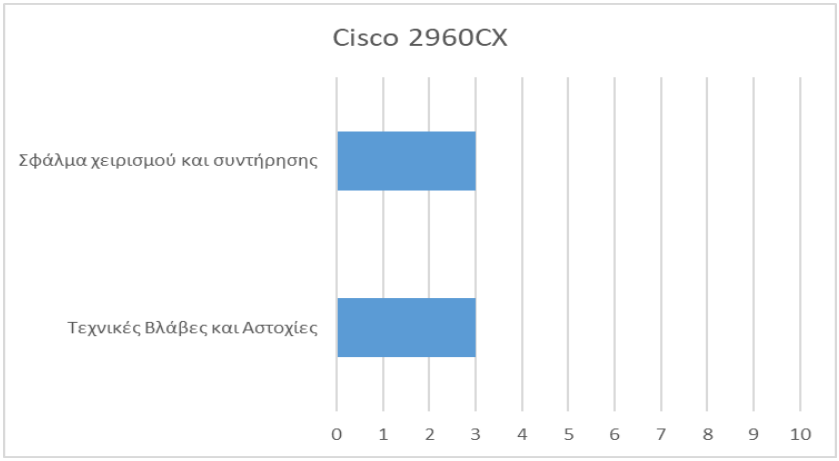
Διάγραμμα 40: APV 1600/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 2), δηλαδή ο ελεγκτής/ κόμβος των εφαρμογών του συστήματος (Application Delivery Controllers), που σε περίπτωση βλάβης του πρωτεύοντος συστήματος σκοπό έχει να ελέγχει την λειτουργία των εφαρμογών του συστήματος σε περίπτωση απώλειας του του πρωτεύοντος συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.



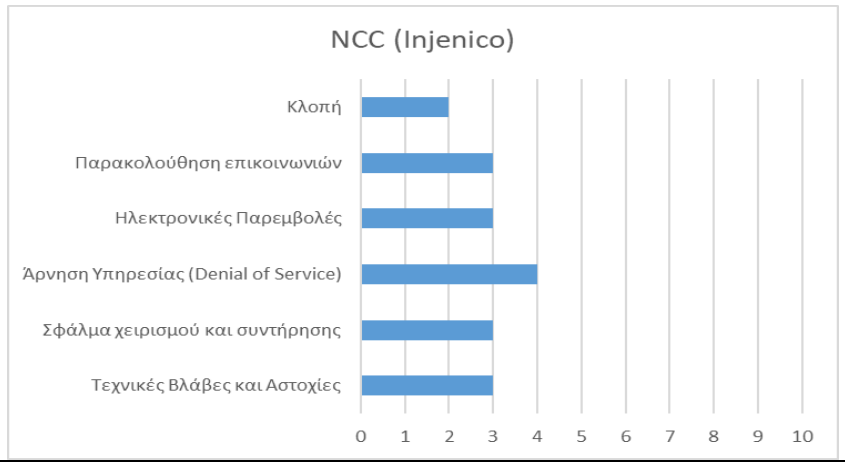
Διάγραμμα 41: 77,20 Checkpoint 5506/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 77,20 Checkpoint 5506, δηλαδή ο το μηχάνημα και η πλατφόρμα λογισμικού, που σε περίπτωση βλάβης του πρωτεύοντος συστήματος σκοπό έχει να ελέγχει την ασφάλεια επικοινωνιών μεταξύ εφαρμογών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Παρακολούθηση Επικοινωνιών, στις Ηλεκτρονικές Παρεμβολές, Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού και στις Τεχνικές Βλάβες και Αστοχίες



Διάγραμμα 42: Cisco 2960X/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960CX, δηλαδή ο κόμβος, που σε περίπτωση βλάβης του πρωτεύοντος συστήματος σκοπό έχει να δρομολογεί σημαντικές πληροφορίες μεταξύ διαφόρων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει μικρό βαθμό επικινδυνότητας απέναντι στο Σφάλμα χειρισμού και συντήρησης και στις Τεχνικές Βλάβες και Αστοχίες.



Διάγραμμα 43: NCC (Injenico)/ risk CRAMM

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού NCC (Injenico), δηλαδή ο ελεγκτής (controller), που σε περίπτωση βλάβης του πρωτεύοντος συστήματος σκοπό έχει να παρακολουθεί και δρομολογεί τις συναλλαγές των πελατών μεταξύ των κατάλληλων ζωνών του συστήματος. Συγκεκριμένα, το αγαθό αυτό έχει σημαντικό βαθμό επικινδυνότητας απέναντι στην Άρνηση Υπηρεσίας λόγω διακοπής λειτουργίας του υλικού.

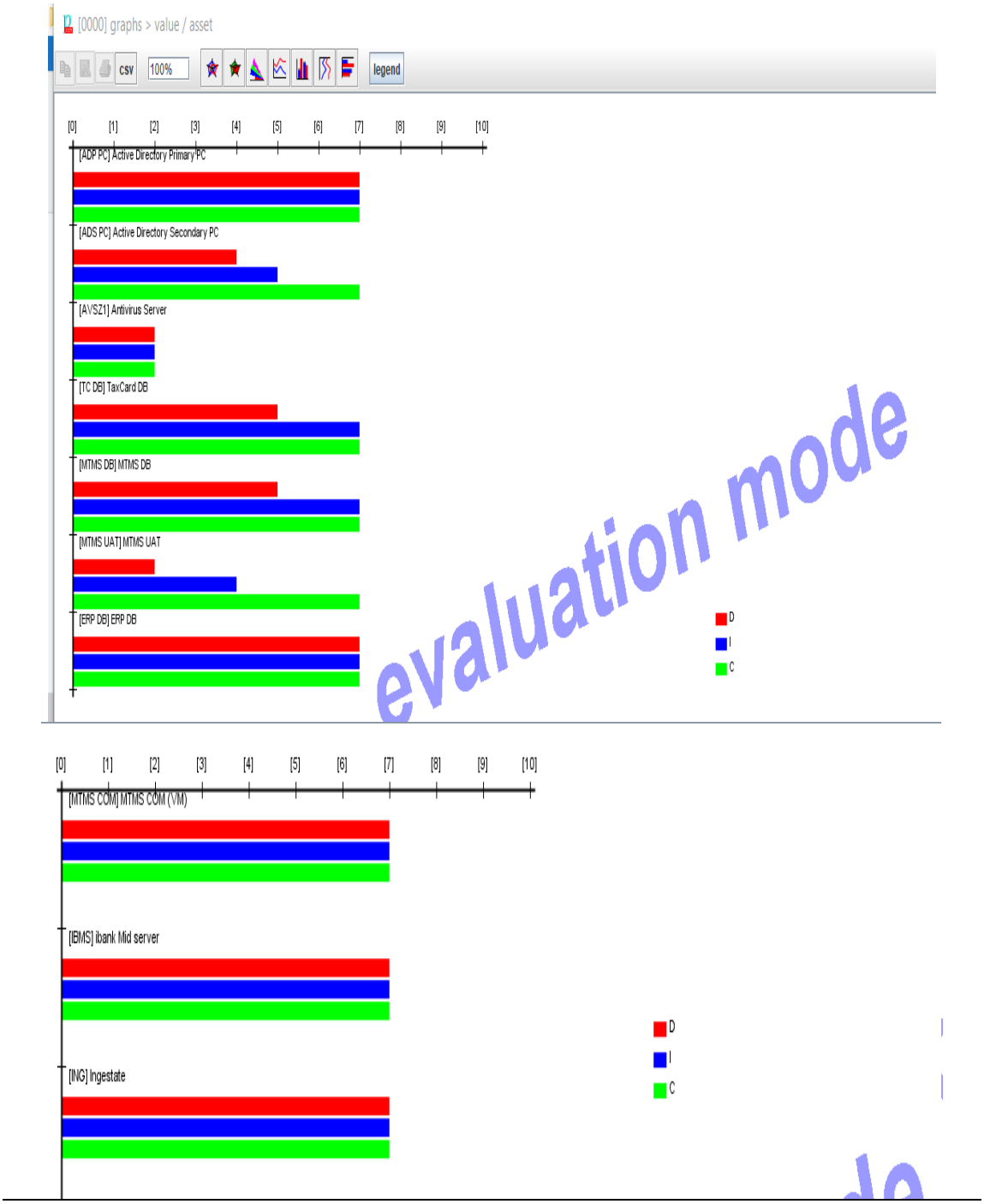
4.3 **ΠΡΟΣΟΜΟΙΩΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ** MAGERIT

Μετά από εκτέλεση των απαιτούμενων προπαρασκευαστικών βημάτων που ορίζει η μεθοδολογία MAGERIT, από το εργαλείο PILAR που χρησιμοποιήθηκε προέκυψαν τα παρακάτω αποτελέσματα που αφορούν την αξιολόγηση των αγαθών του σεναρίου ως προς τον βαθμό επίπτωσης (impact) στους τρείς άξονες της Διαθεσιμότητας (Availability-A), Εμπιστευτικότητας (Confidentiality-C) και Ακεραιότητας (Integrity-I).

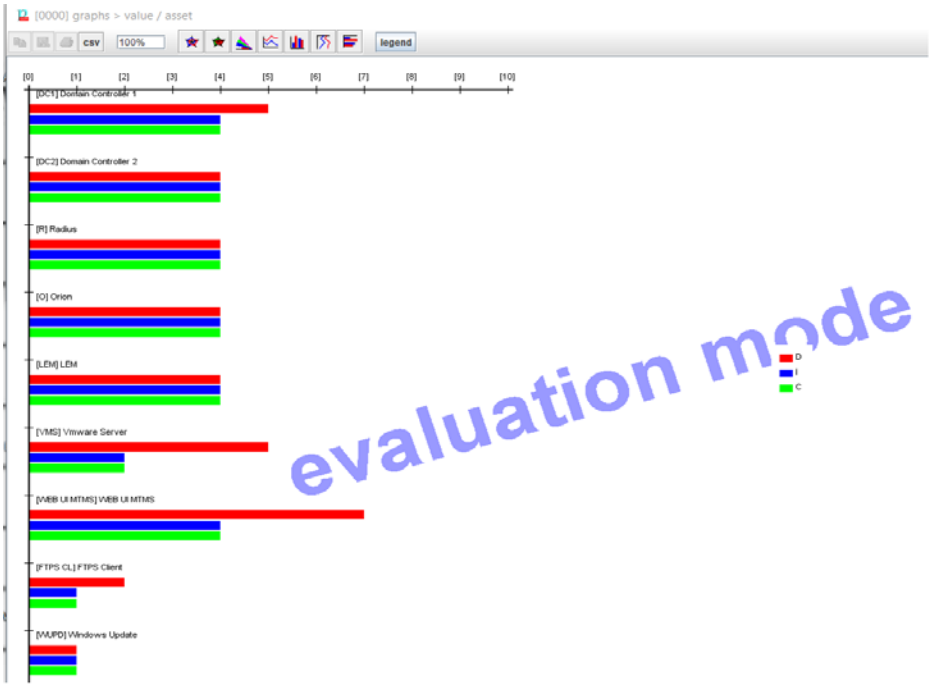
Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επίπτωσης όπως αυτό έχει οριστεί από την MAGERIT με την εννοιολογική της περιγραφή.

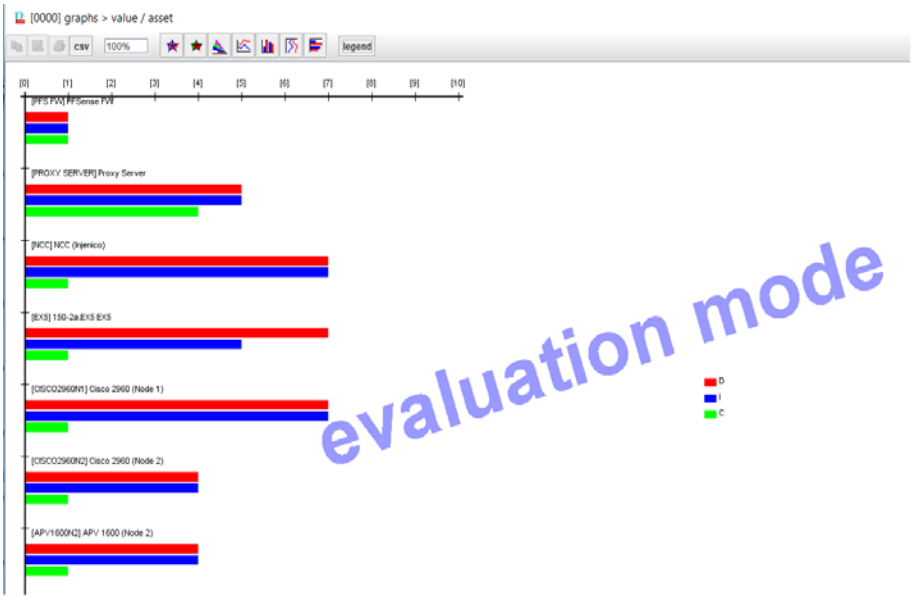
Επίπεδο Επίπτωσης	**Περιγραφή**
1	**Πολύ μικρή επίπτωση**
2	**Μικρή επίπτωση**
3	**Μέτρια επίπτωση**
4	Σημαντική επίπτωση
5	**Μεγάλη επίπτωση**
6	Πολύ μεγάλη επίπτωση
7	**Κρίσιμη επίπτωση**

Πίνακας 8: **Η κλίμακα του επιπέδου επίπτωσης (**impact**) της μεθοδολογίας** MAGERIT

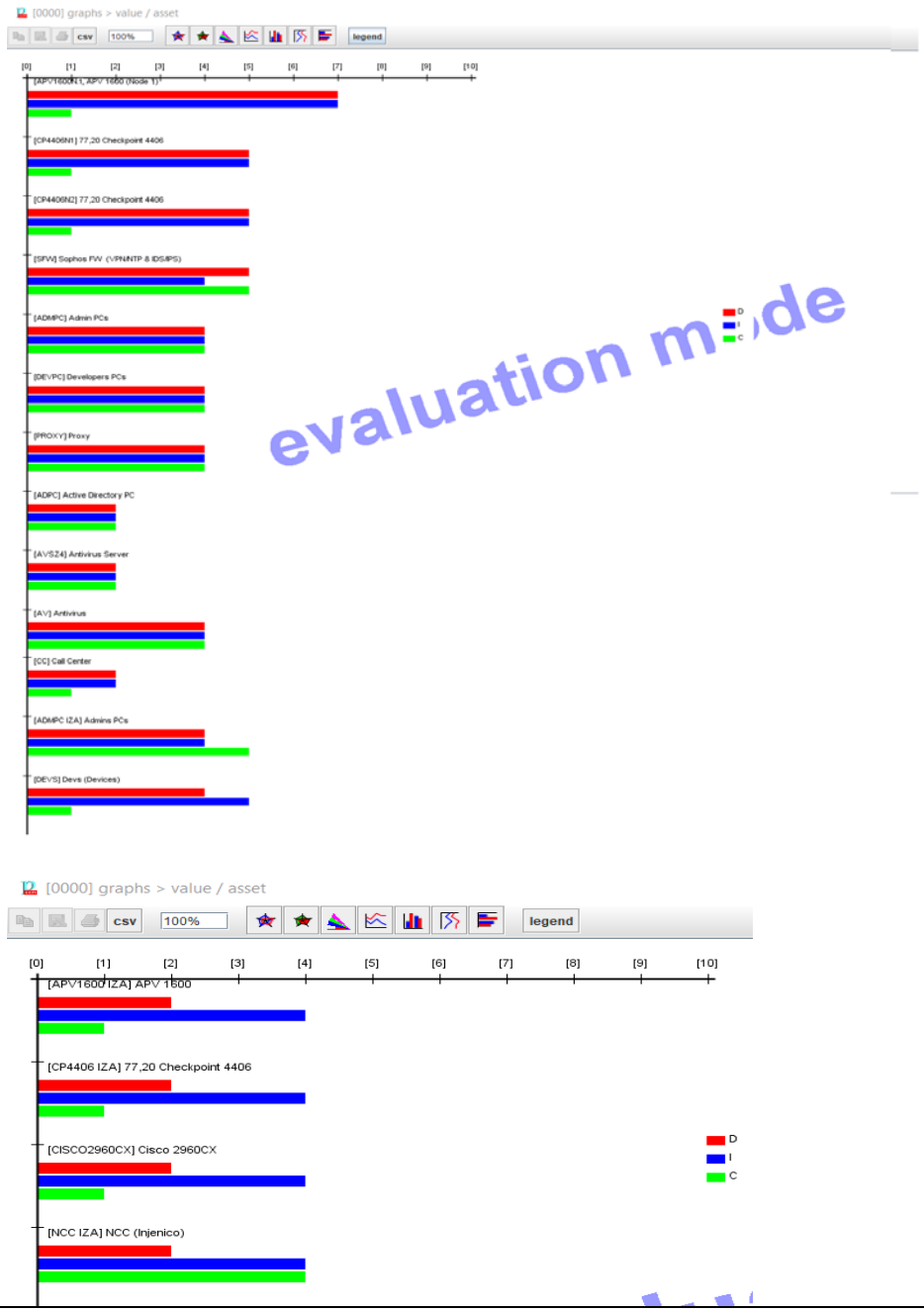


Διάγραμμα 44**: Το επίπεδο επίπτωσης (**impact**) ανά αγαθό ως προς** A, I **και** C, MAGERIT (1-3)





Διάγραμμα 45**: Το επίπεδο επίπτωσης (**impact**) ανά αγαθό ως προς** A, I **και** C, MAGERIT (2-3)



Διάγραμμα 46**: Το επίπεδο επίπτωσης (**impact**) ανά αγαθό ως προς** A, I **και** C, MAGERIT (3-3)

4.3.1. **Γενικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** MAGERIT - **Επίπτωση**

Μετά από μελέτη του ανωτέρω σχήματος προκύπτει ότι ως προς τον άξονα της Διαθεσιμότητας (Availability-A) τα αγαθά που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι τα Active Directory Primary PC, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, NCC (Injenico), Web UI MTMS, Cisco 2960 (Node 1), 170.2a.EX7 και το APV 1600 (Node1). Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα TaxCard DB, MTMS DB, Domain Controller 1, VMware Server, Proxy Server, τα δυο 77,20 Checkpoint 5506 και το Sophos FW. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality-C) κρίσιμο επίπεδο επίπτωσης παρουσιάζουν τα αγαθά Active Directory Primary PC, Active Directory Secondary PC, TaxCard DB, MTMS DB, MTMS COM (VM), MTMS UAT, ERP DB, ibank Mid Server και Ingestate. Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα Admins PCs και Sophos FW. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Τέλος, ως προς τον άξονα της Ακεραιότητας (Integrity-I) κρίσιμο επίπεδο επίπτωσης παρουσιάζουν τα αγαθά τα Active Directory Primary PC, TaxCard DB, MTMS DB, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, NCC (Injenico), Cisco 2960 (Node 1) και το APV 1600 (Node1). Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν τα Active Directory Secondary PC, 170.2a.EX7, Devs (Devices) και τα δυο 77,20 Checkpoint 5506. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Στην συνέχεια, γίνεται παράθεση και σχολιασμός των αποτελεσμάτων του επιπέδου επικινδυνότητας κάθε αγαθού συναρτήσει των κινδύνων που πρόκειται να αντιμετωπίσει κατά την λειτουργία του.

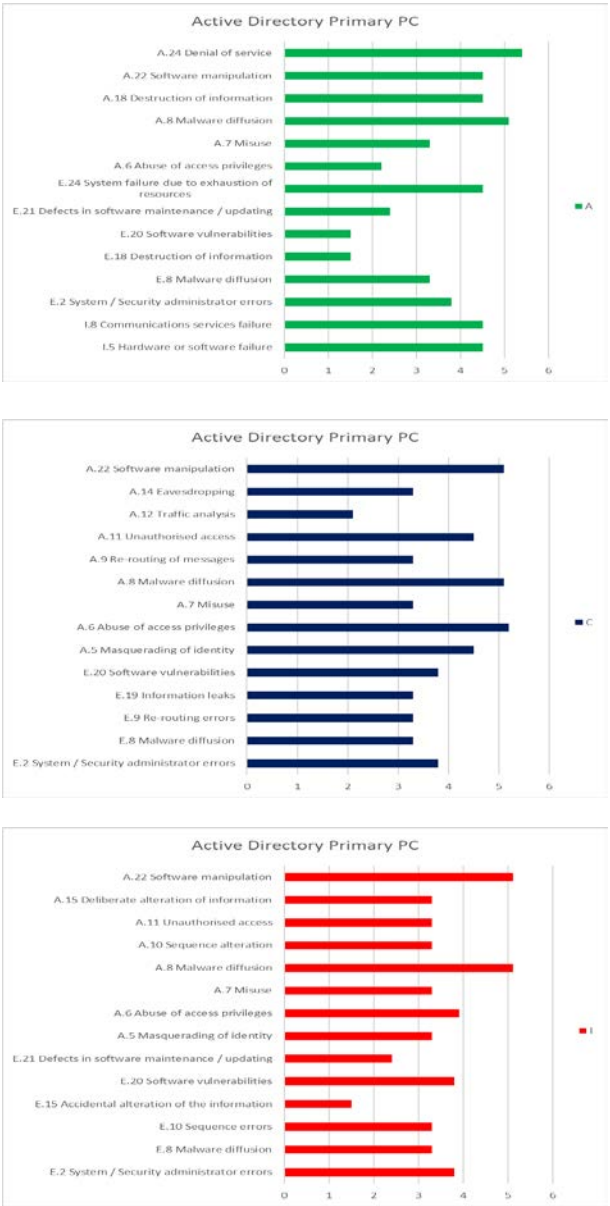
Η MAGERIT ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την τιμή της επίπτωσης (impact) κάθε αγαθού ξεχωριστά για κάθε απειλή ως προς και τους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα). Συνεπώς η επικινδυνότητα που προκύπτει για κάθε απειλή κάθε αγαθού παρουσιάζεται σε τρεις (3) μπάρες μια για κάθε άξονα μελέτης.

Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από την MAGERIT με την εννοιολογική της περιγραφή.

Επίπεδο Επικινδυνότητας	Περιγραφή
{0}	Πολύ μικρός κίνδυνος
{1}	Μικρός κίνδυνος
{2}	Μέτριος κίνδυνος
{3}	Μεγάλος κίνδυνος
{4}	Πολύ μεγάλος κίνδυνος
{5}	Κρίσιμος κίνδυνος
{6}	Πολύ κρίσιμος κίνδυνος
{7}	Εξαιρετικά κρίσιμος κίνδυνος

Πίνακας 9**: Η κλίμακα του επιπέδου επικινδυνότητας της μεθοδολογίας** MAGERIT

4.3.2. **Αναλυτικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** MAGERIT - **Επικινδυνότητα**



Διάγραμμα 47: **Διάγραμμα** 48: Active Directory Primary PC/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active Directory Primary PC. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο

επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

Διάγραμμα 49: Active Directory Secondary PC/ risk (A, C, I) MAGERIT

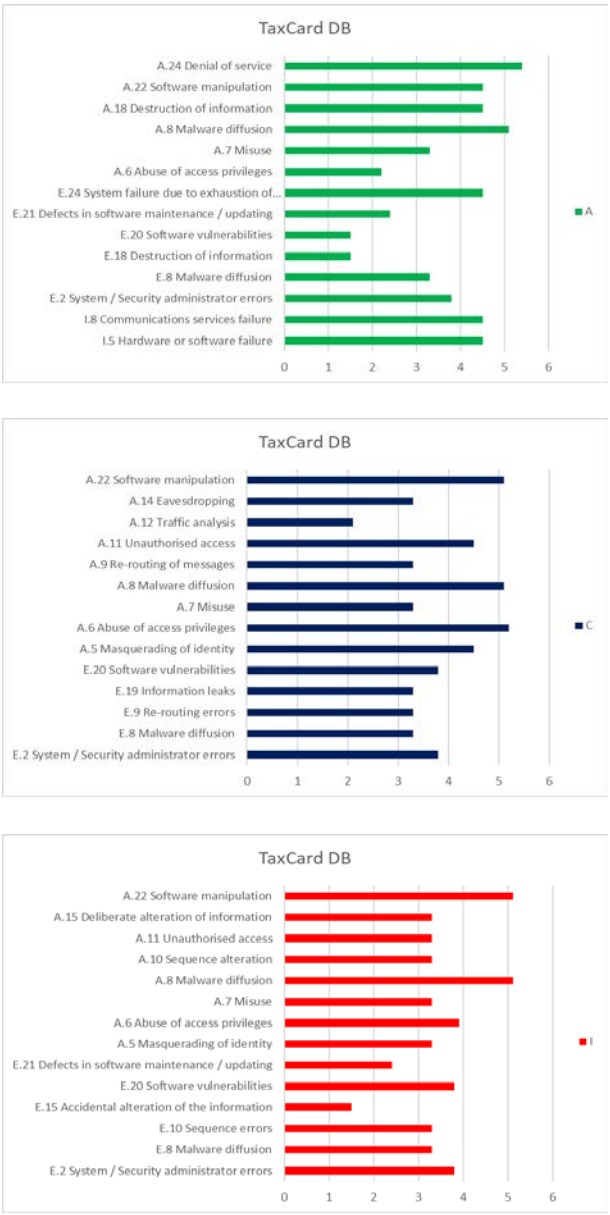
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του

οργανισμού Active Directory Secondary PC. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

Διάγραμμα 50: Antivirus Server/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus Server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας

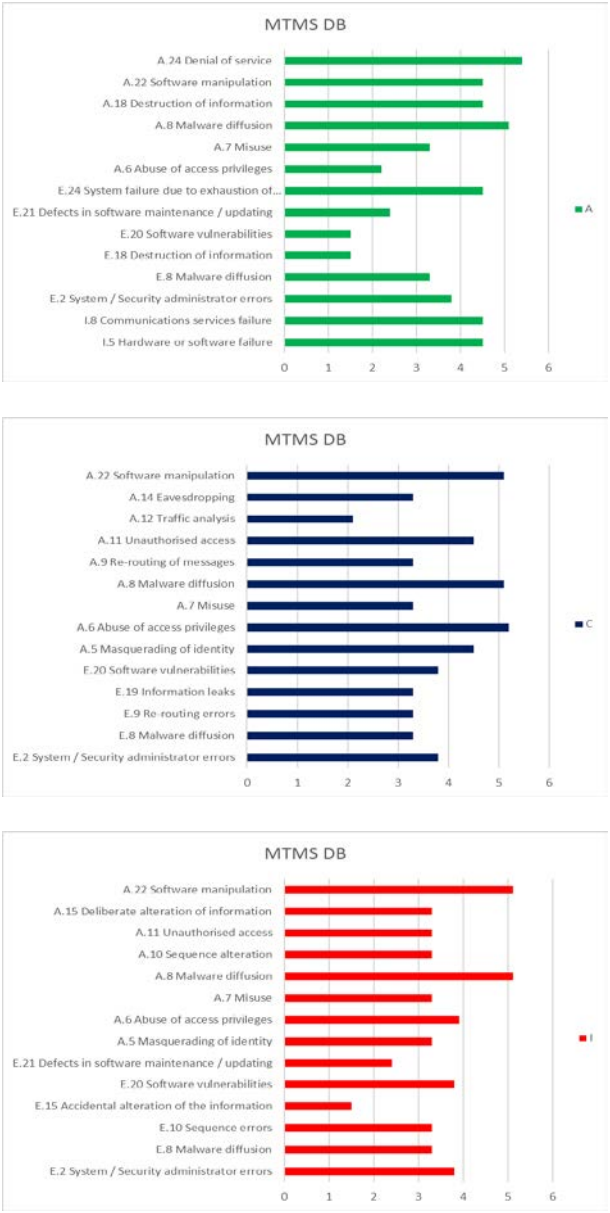
απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



Διάγραμμα 51: TaxCard DB/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού TaxCard DB. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι

σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



Διάγραμμα 52: MTMS DB/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε

Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

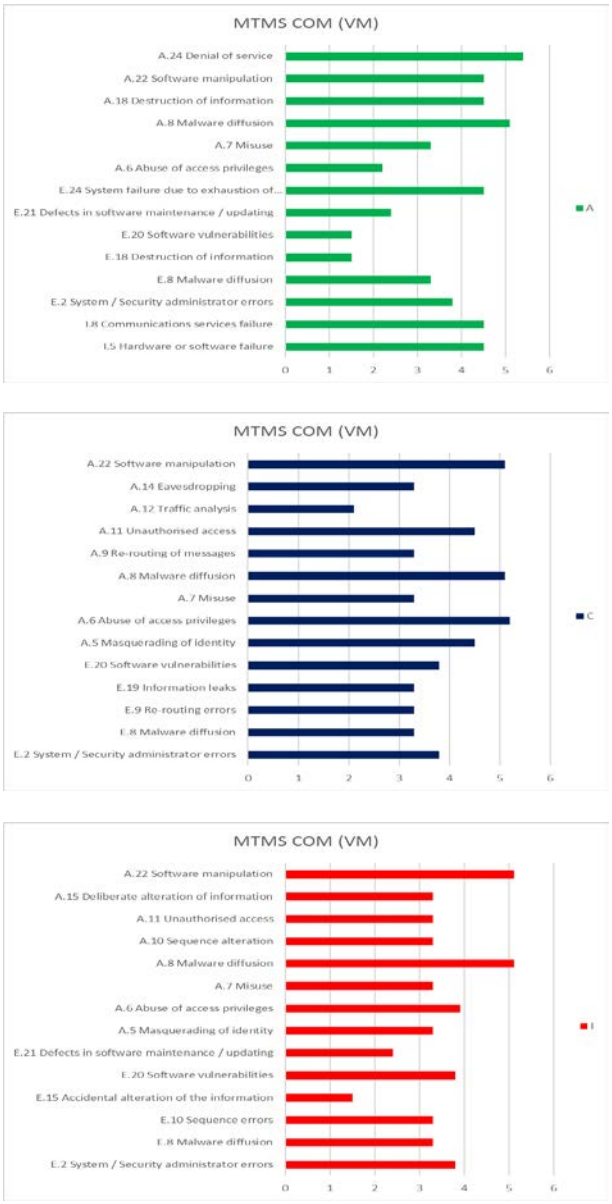
Διάγραμμα 53: MTMS UAT/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS UAT. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι

σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

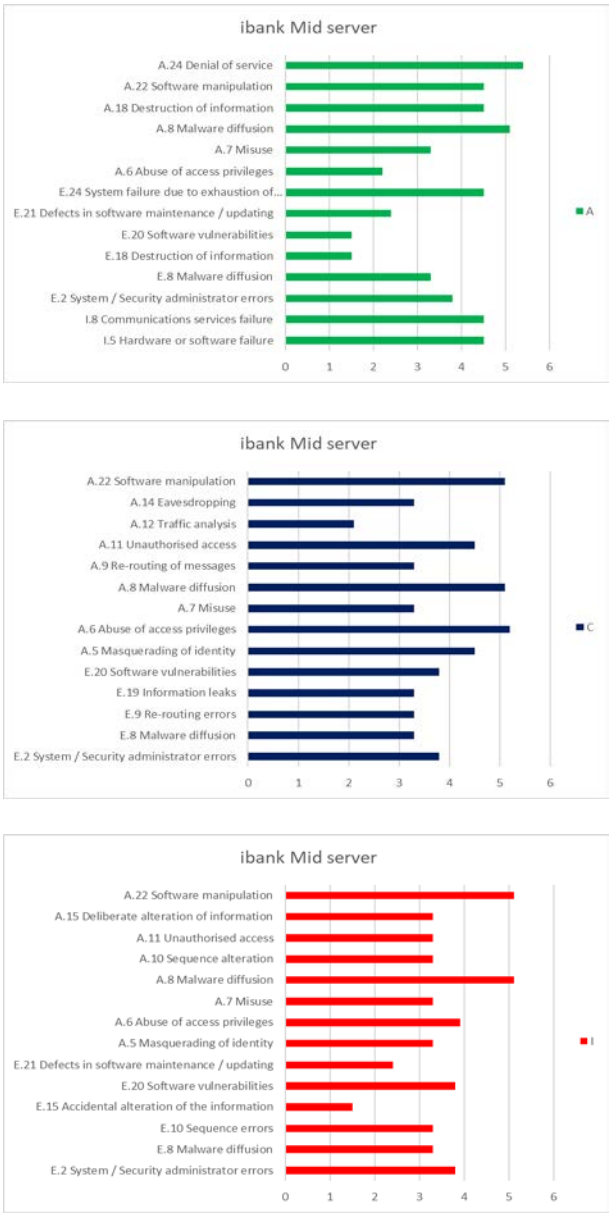
Διάγραμμα 54: ERP DB/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ERP DB. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



Διάγραμμα 55: MTMS COM (VM)/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού MTMS COM (VM). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

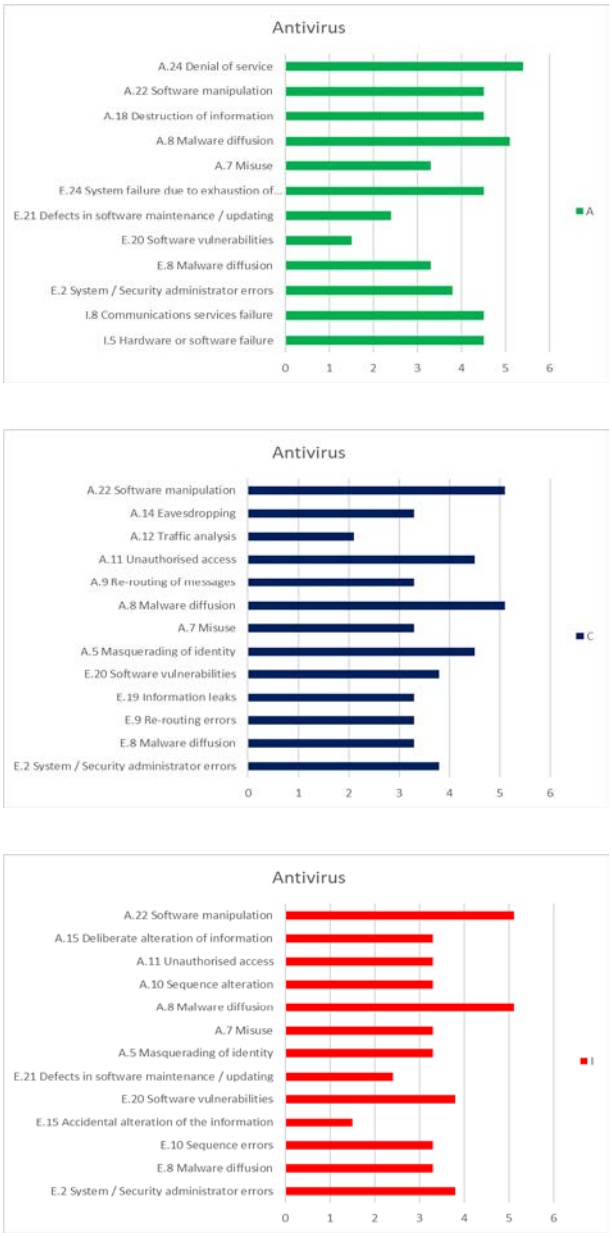


Διάγραμμα 56: ibank Mid Server/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ibank Mid Server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

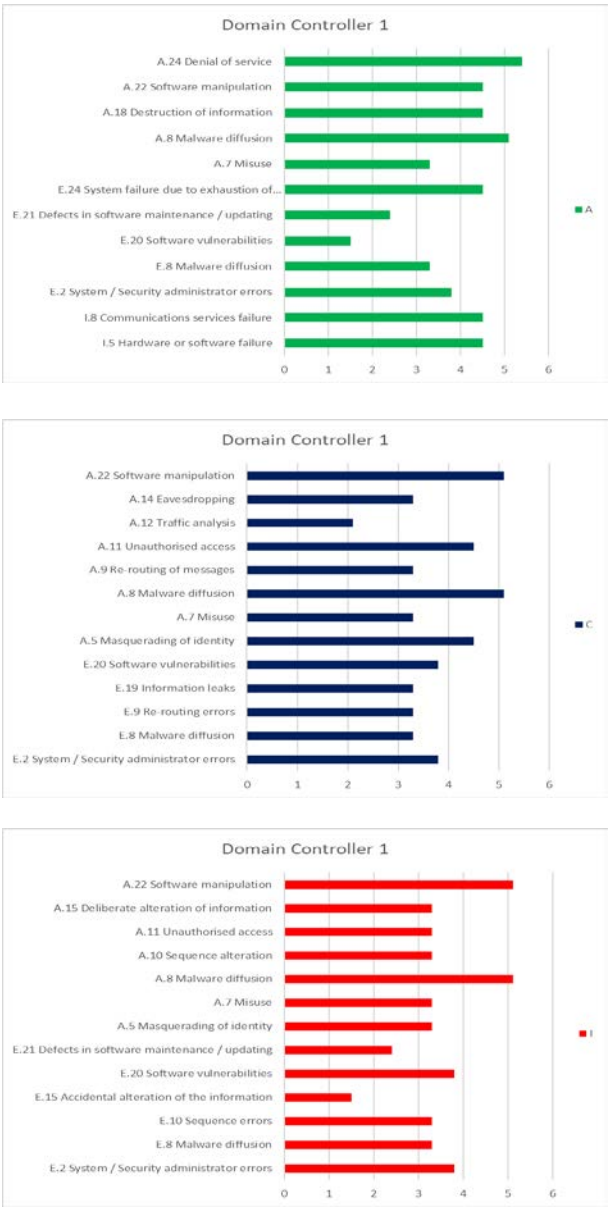
Διάγραμμα 57: Ingestate/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Ingestate. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



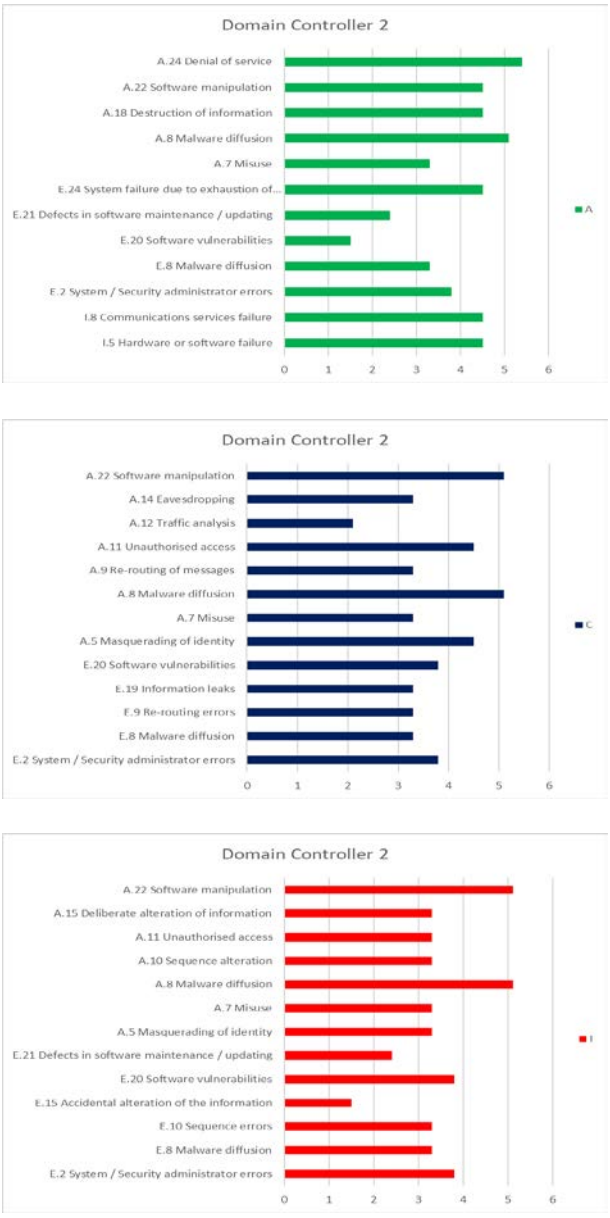
Διάγραμμα 58: Antivirus/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



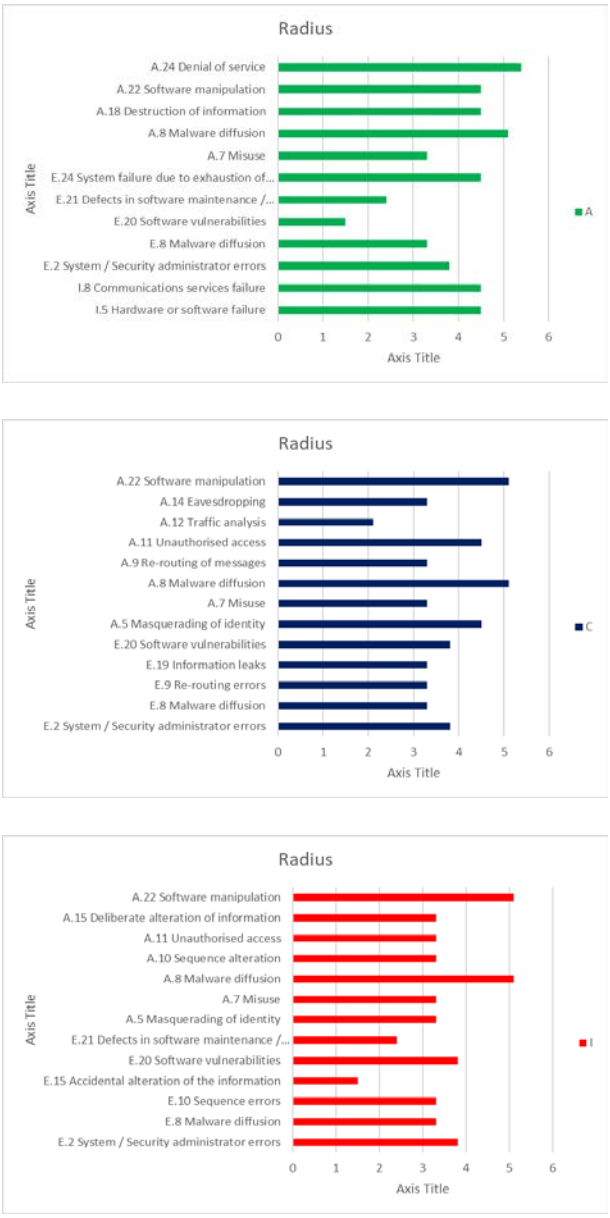
Διάγραμμα 59: Domain Controller 1/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Domain Controller 1. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



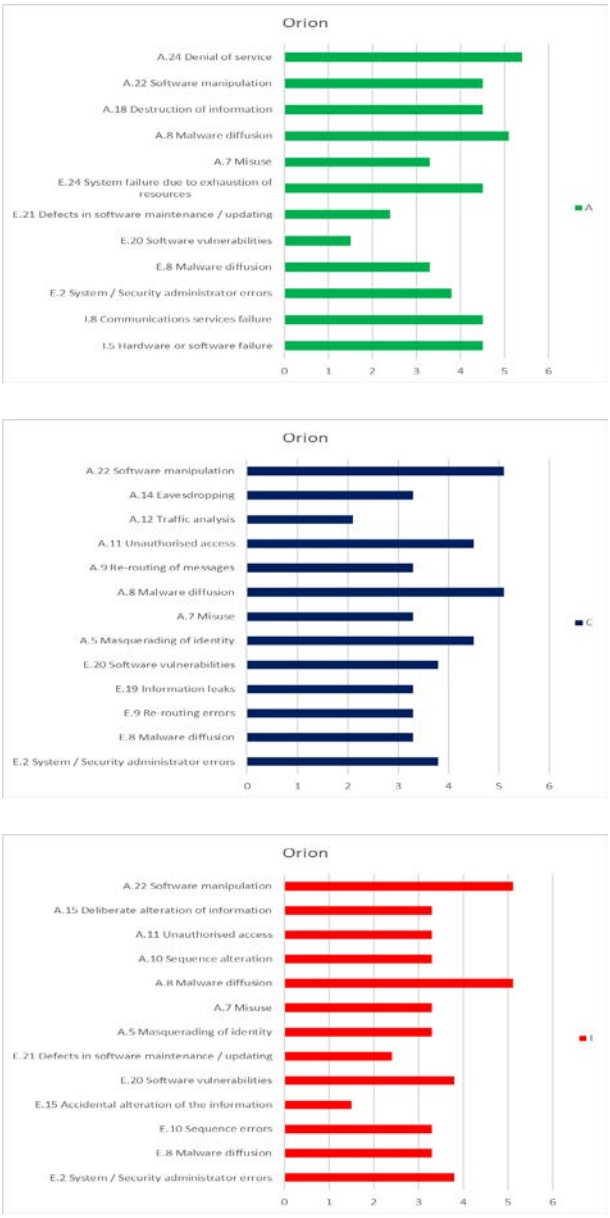
Διάγραμμα 60: Domain Controller 2/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Domain Controller 2. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



Διάγραμμα 61: Radius/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού RADIUS. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



Διάγραμμα 62: Orion/ risk (A, C, I) MAGERIT

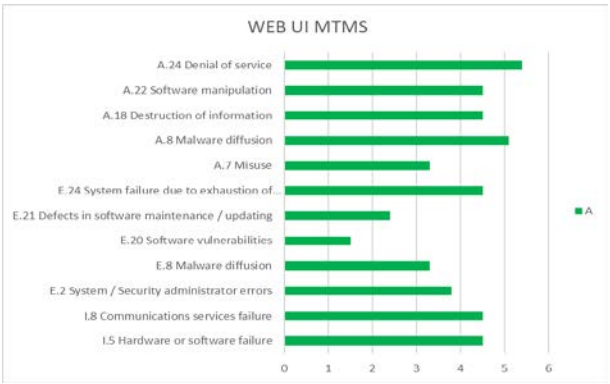
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού ORION. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

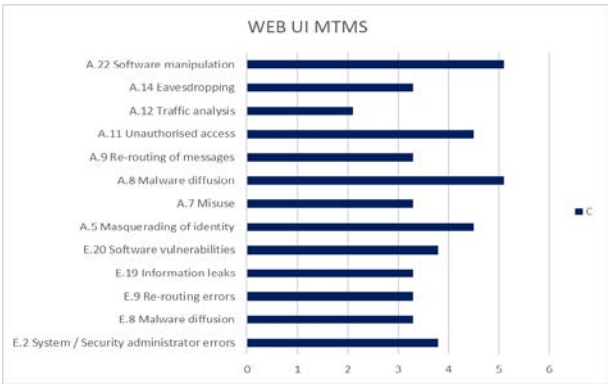
Διάγραμμα 63: LEM/ risk (A, C, I) MAGERIT

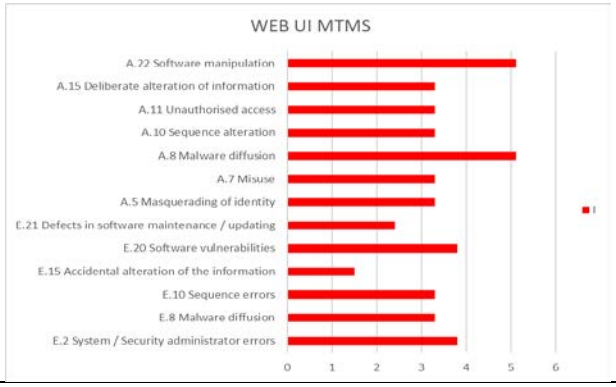
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού LEM (Log & Event Manager). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

Διάγραμμα 64: VMware Server/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active VMware server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).





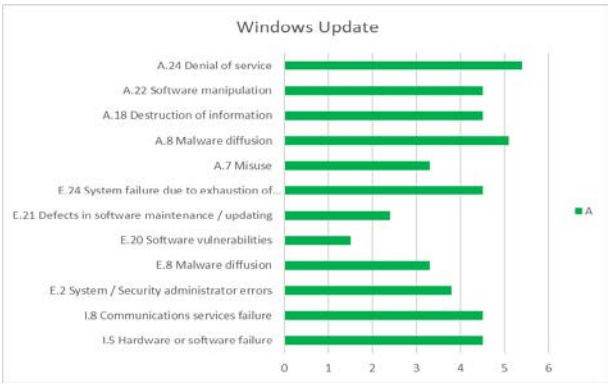


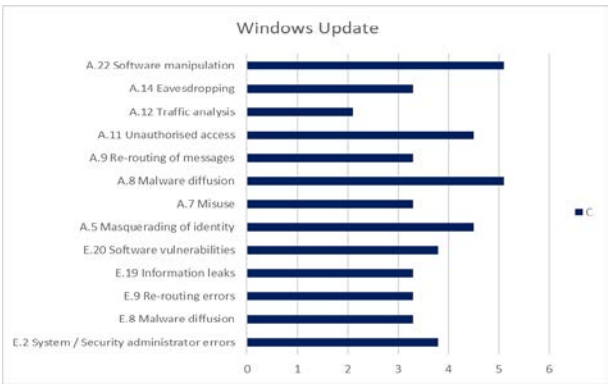
Διάγραμμα 65: WEB UI MTMS/ risk (A, C, I) MAGERIT

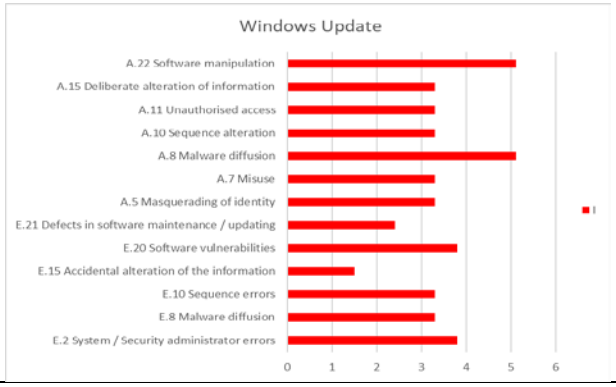
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού WEB UI MTMS. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

Διάγραμμα 66: FTPS Client/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού FTPS Client. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).

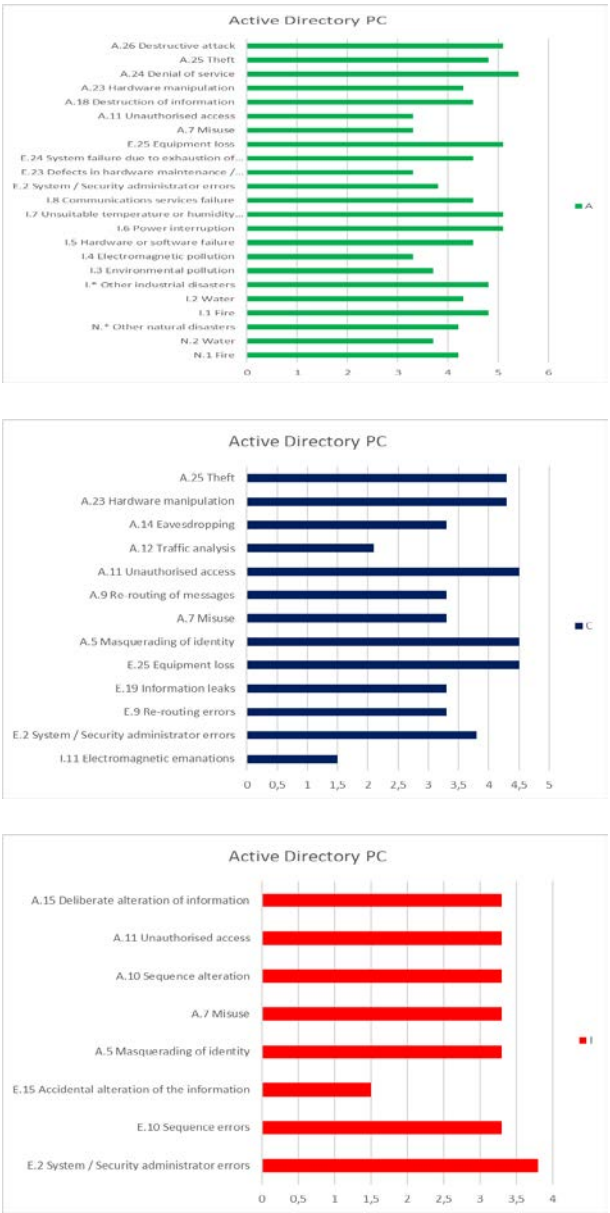






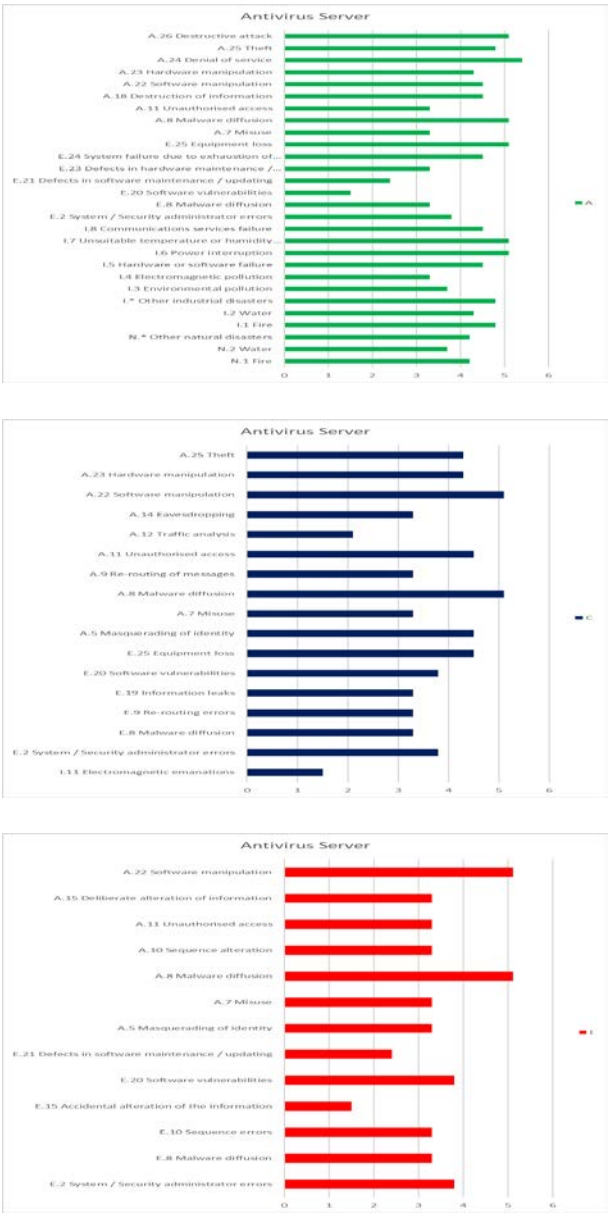
Διάγραμμα 67: Windows Update/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Windows Update. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Denial of service (A), Malware diffusion (A, C, I), Abuse of access privileges (C) και Software manipulation (C, I).



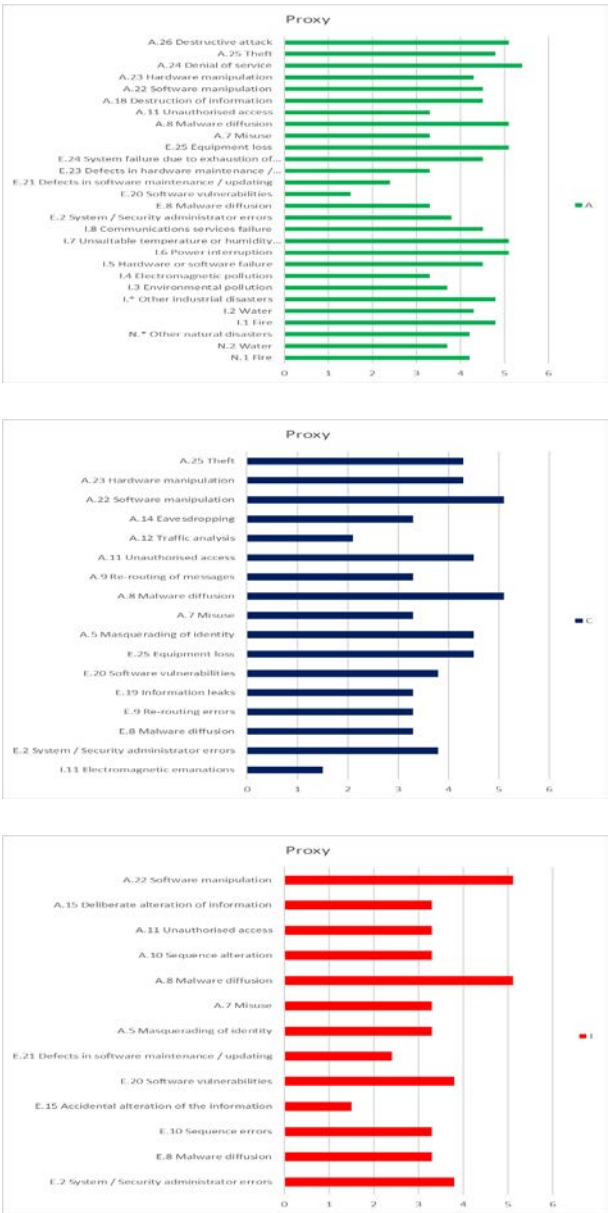
Διάγραμμα 68: Active Directory PC/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Active Directory PC. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



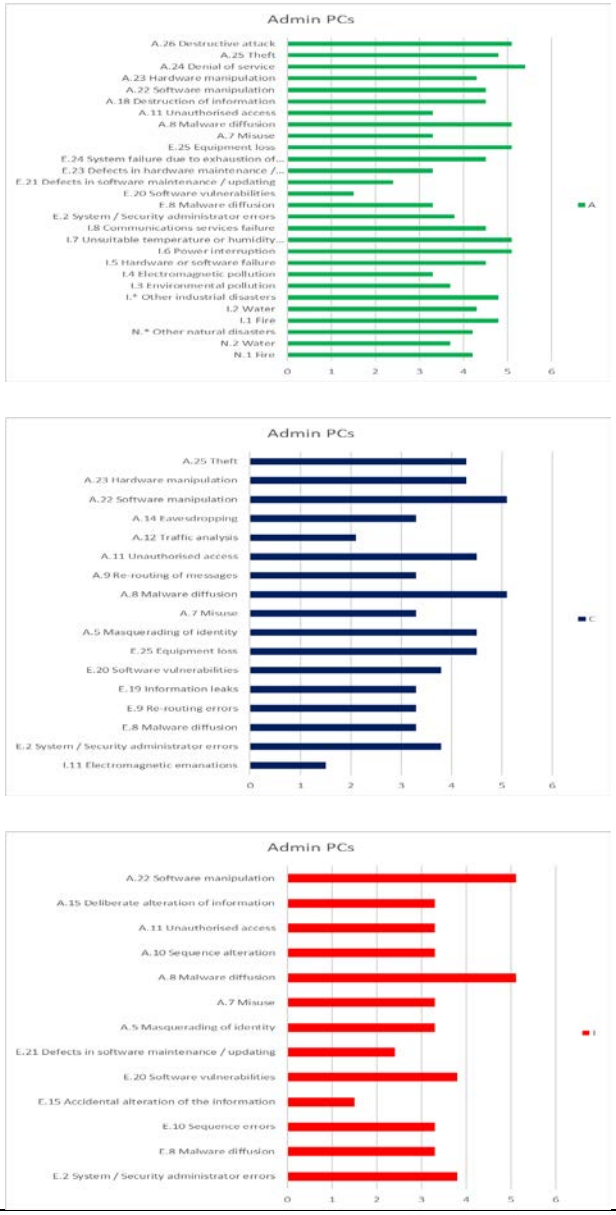
Διάγραμμα 69: Antivirus Server/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Antivirus Server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



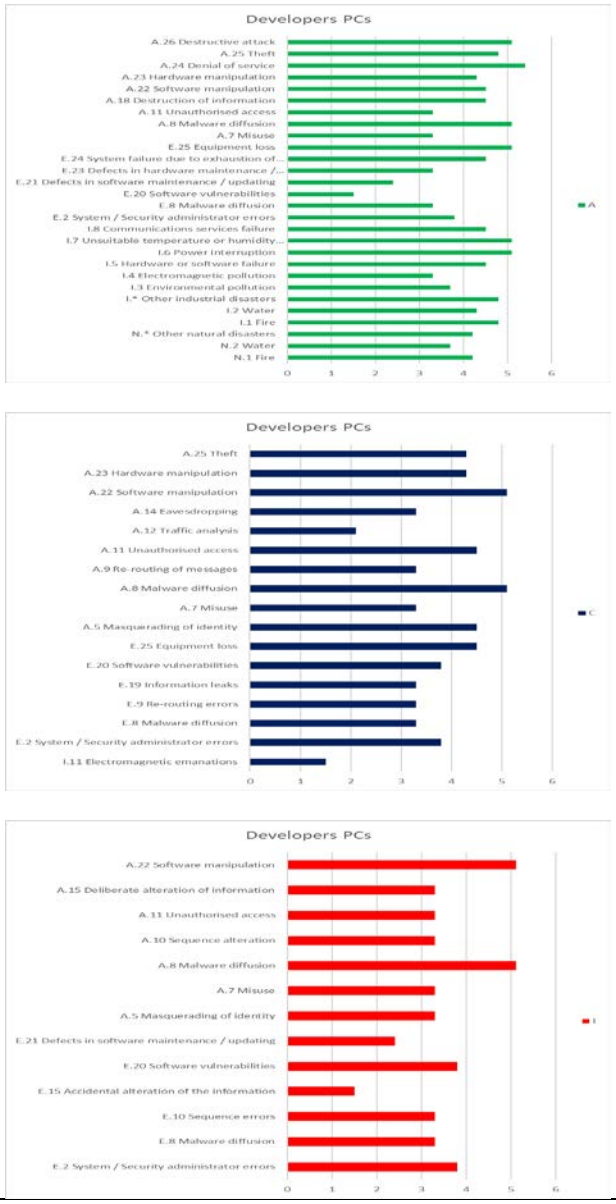
Διάγραμμα 70: Proxy/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Proxy server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



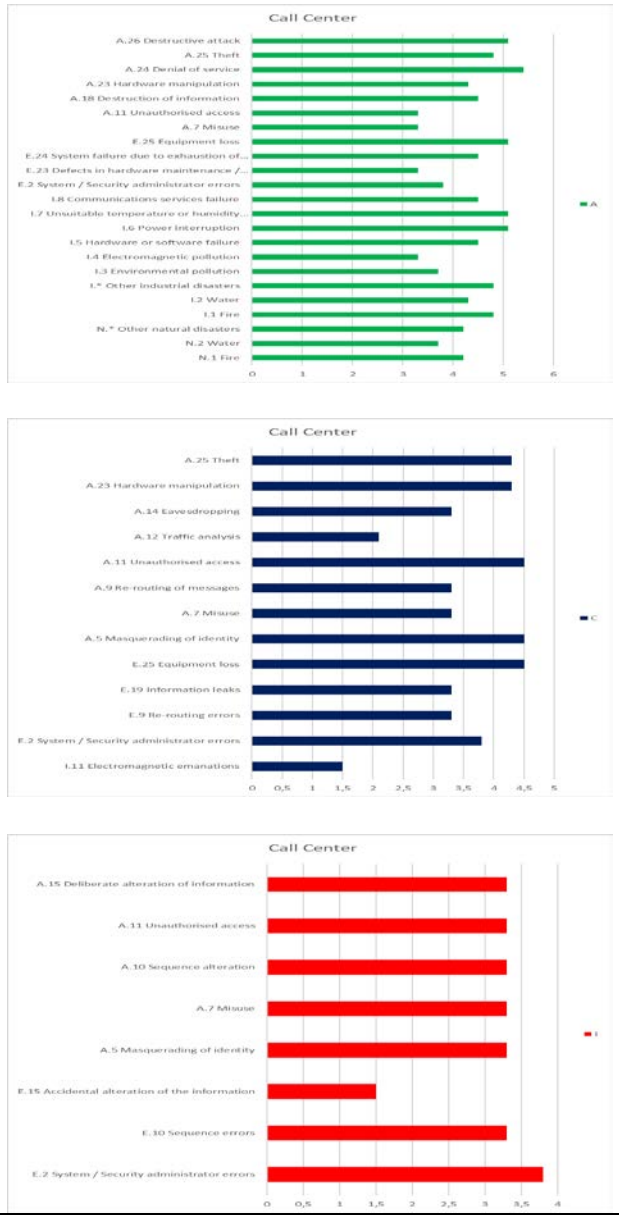
Διάγραμμα 71: Admin PCs/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Admin PCs. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



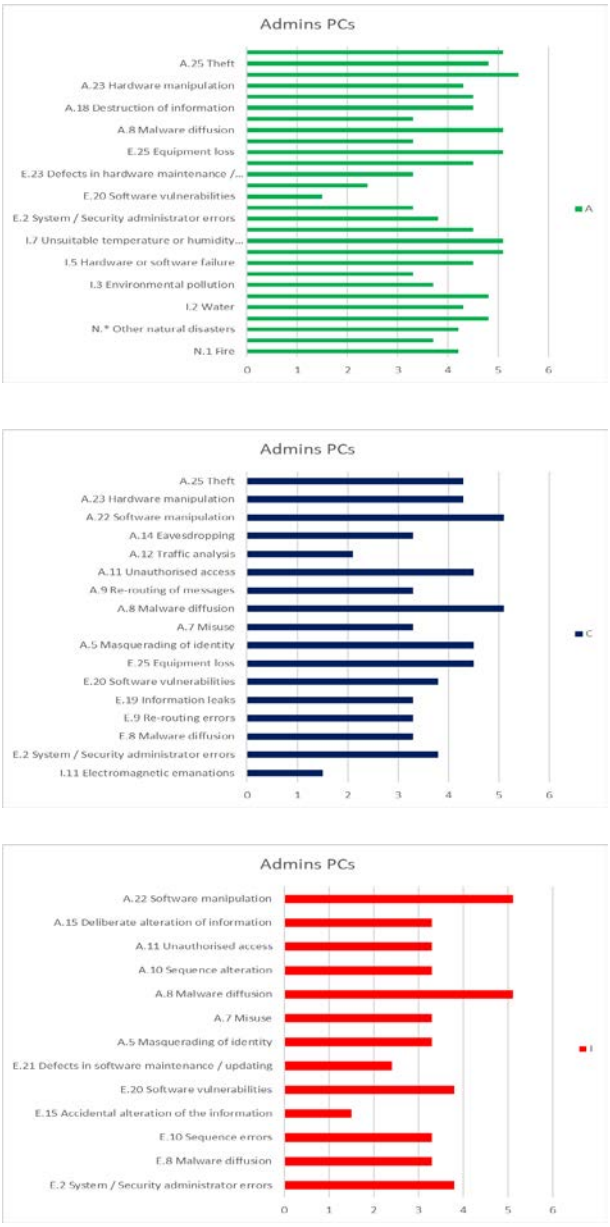
Διάγραμμα 72: Developers PCs/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Developers PCs. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



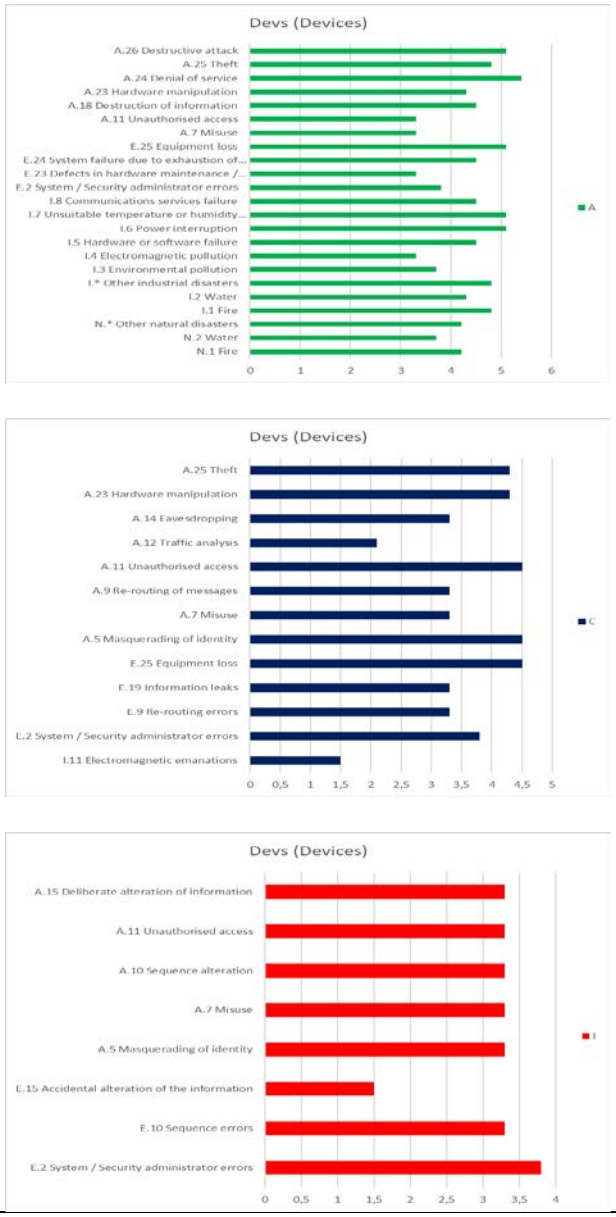
Διάγραμμα 73: Call Center/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Call Center. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



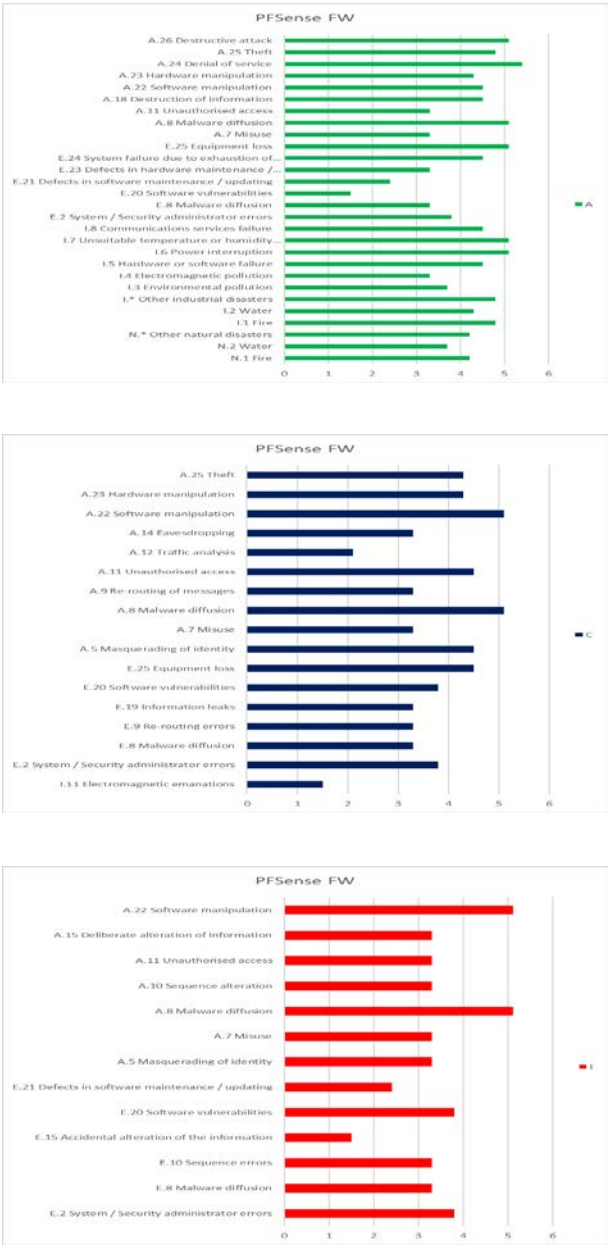
Διάγραμμα 74: Admins PCs/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Admin PCs. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



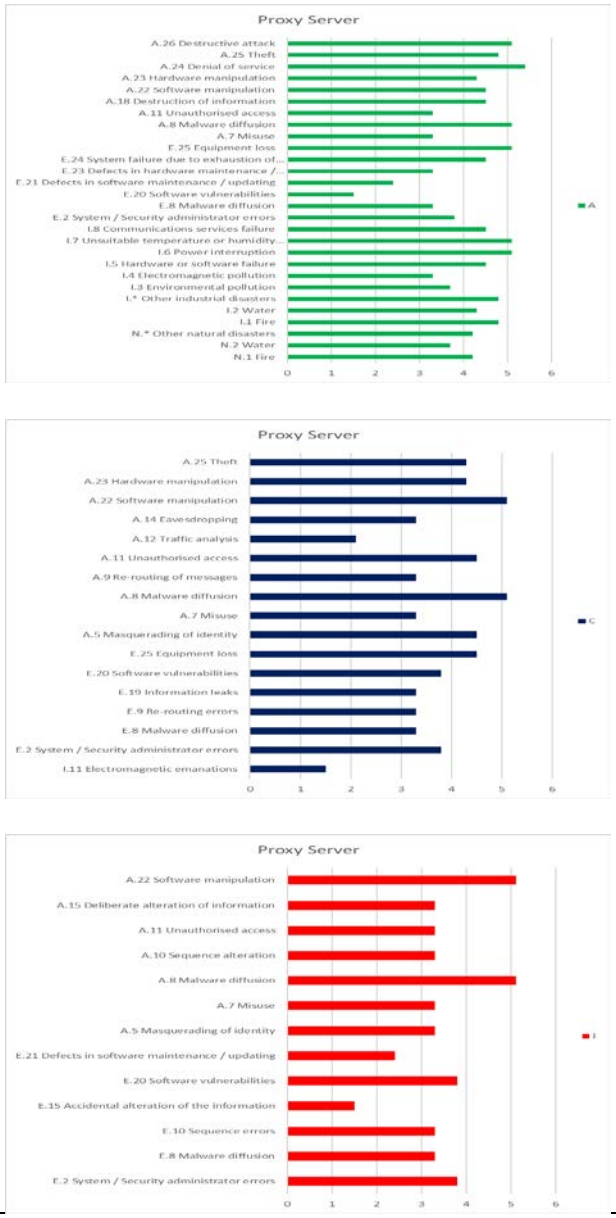
Διάγραμμα 75: Devs (Devices) / risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Devs (Devices. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



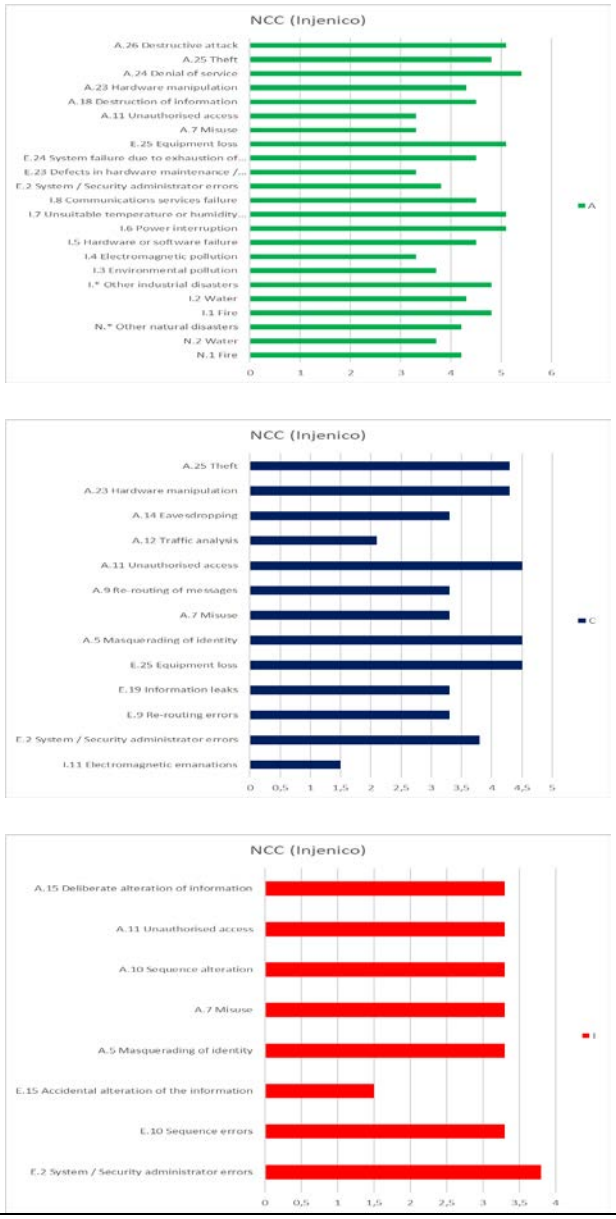
Διάγραμμα 76: PFSense FW/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού PFSense FW. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



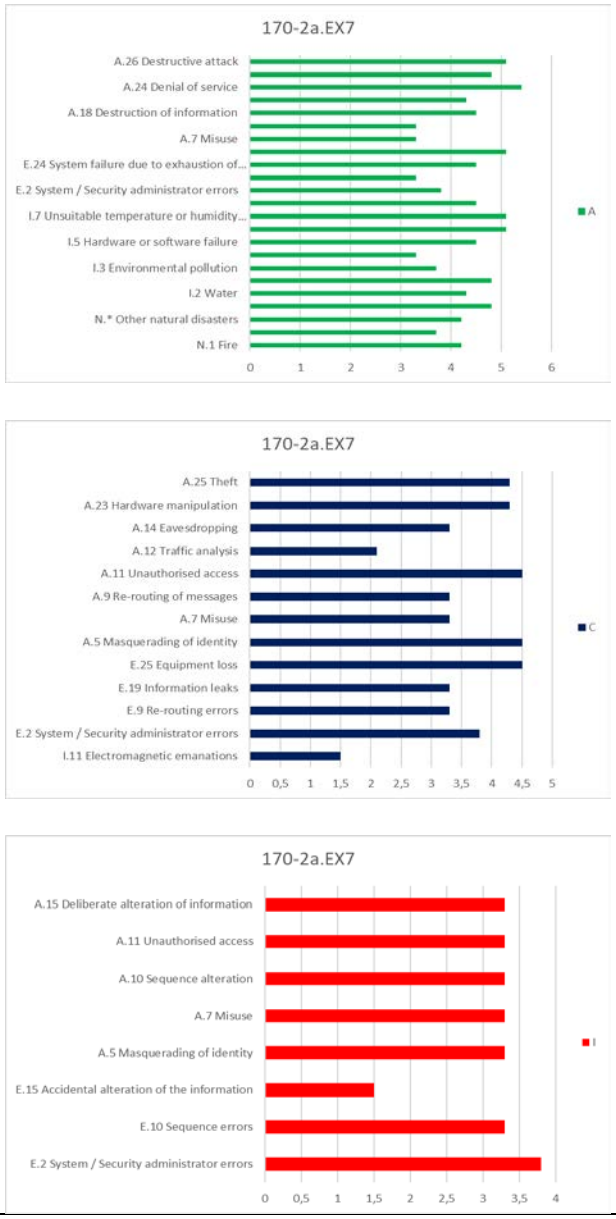
Διάγραμμα 77: Proxy Server/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Proxy server. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, I, C), Unsuitable humidity or temperature conditions (A), Power Interruption (A), Equipment Loss (A), Software manipulation (C, I).



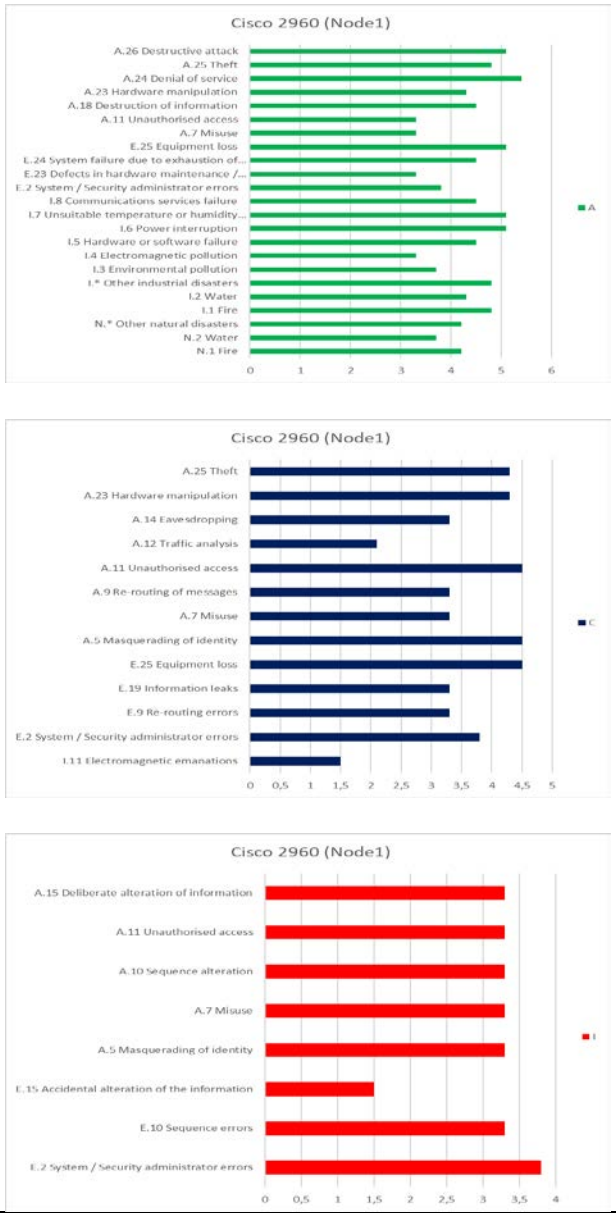
Διάγραμμα 78: NCC (Injenico)/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού NCC (Injenico). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



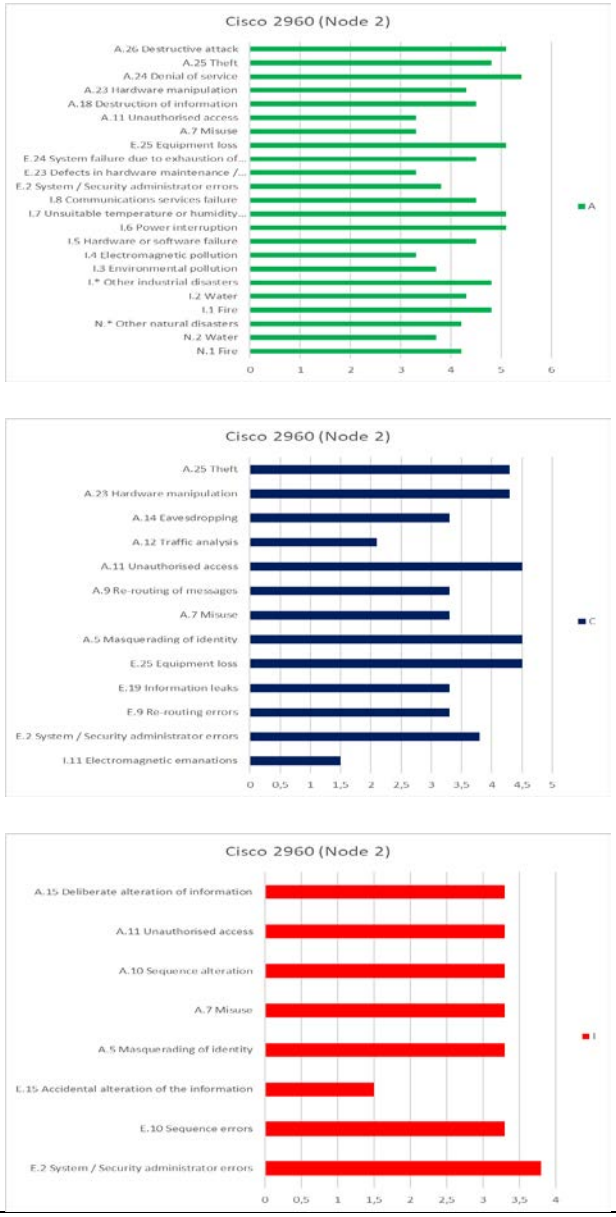
Διάγραμμα 79: 170-2a.EX7/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 170-2a.EX7. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



Διάγραμμα 80: Cisco 2960 (Node 1)/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960 (Node 1). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



Διάγραμμα 81: Cisco 2960 (Node 2)/ risk (A, C, I) MAGERIT

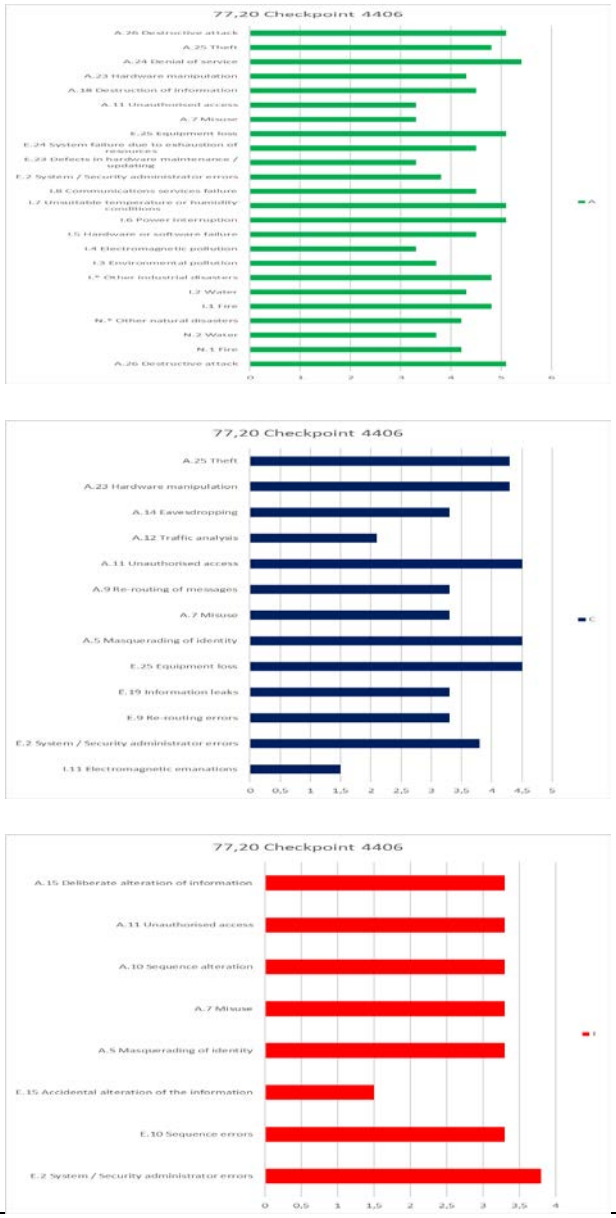
Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960 (Node 2). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

Διάγραμμα 82: APV 1600 (Node 1) / risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 1). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

Διάγραμμα 83: APV 1600 (Node 2) / risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 2). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Malware diffusion (A, C, I), System failure due to exhaustion of resources (A), Equipment Loss (A), Unsuitable temperature or humidity conditions (A), Power interruption (A) και Software manipulation (C, I).

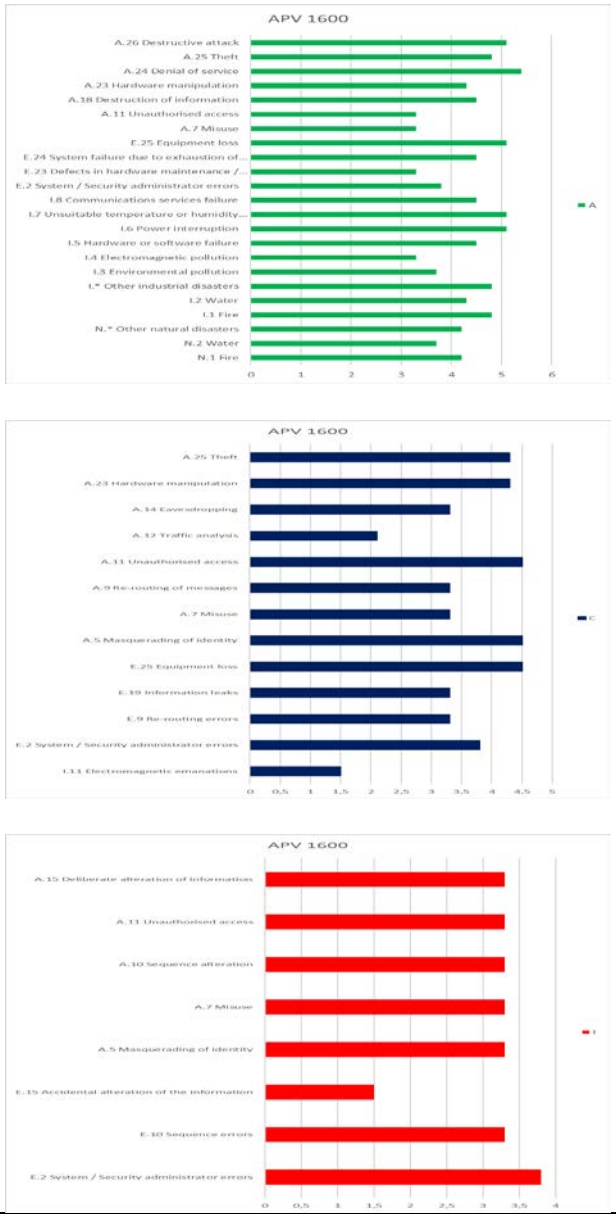


Διάγραμμα 84: 77,20 Checkpoint 5506/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 77,20 Checkpoint 5506. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

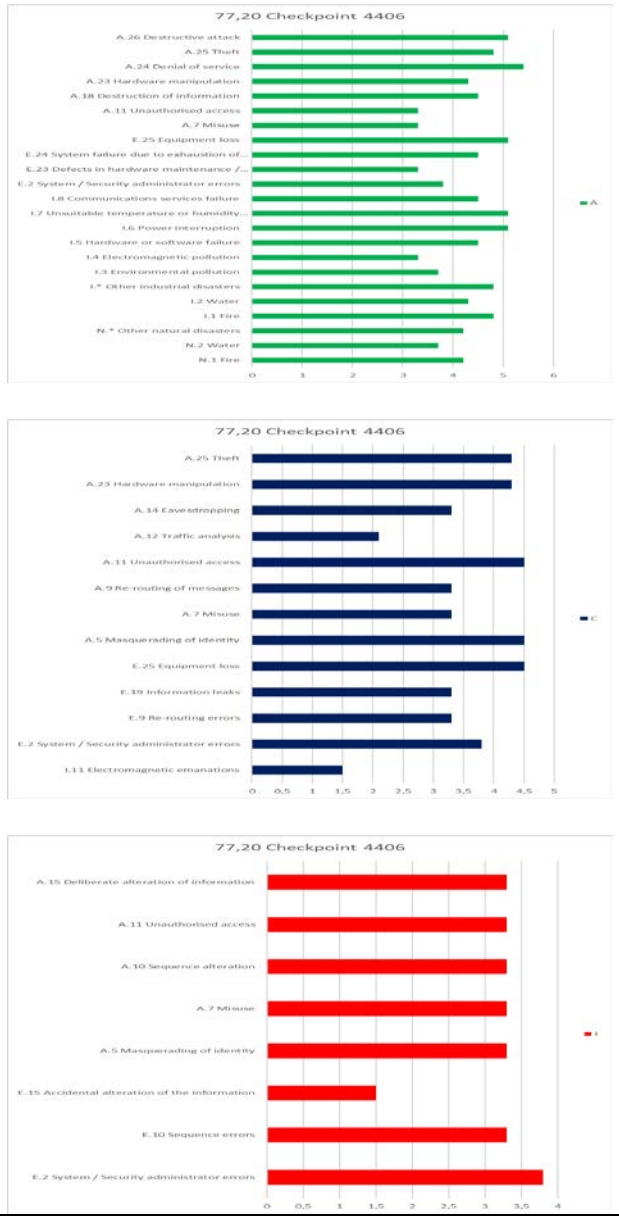
Διάγραμμα 85: SOFOS FW/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού PFSense FW. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



Διάγραμμα 86: APV 1600/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού APV 1600 (Node 2). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

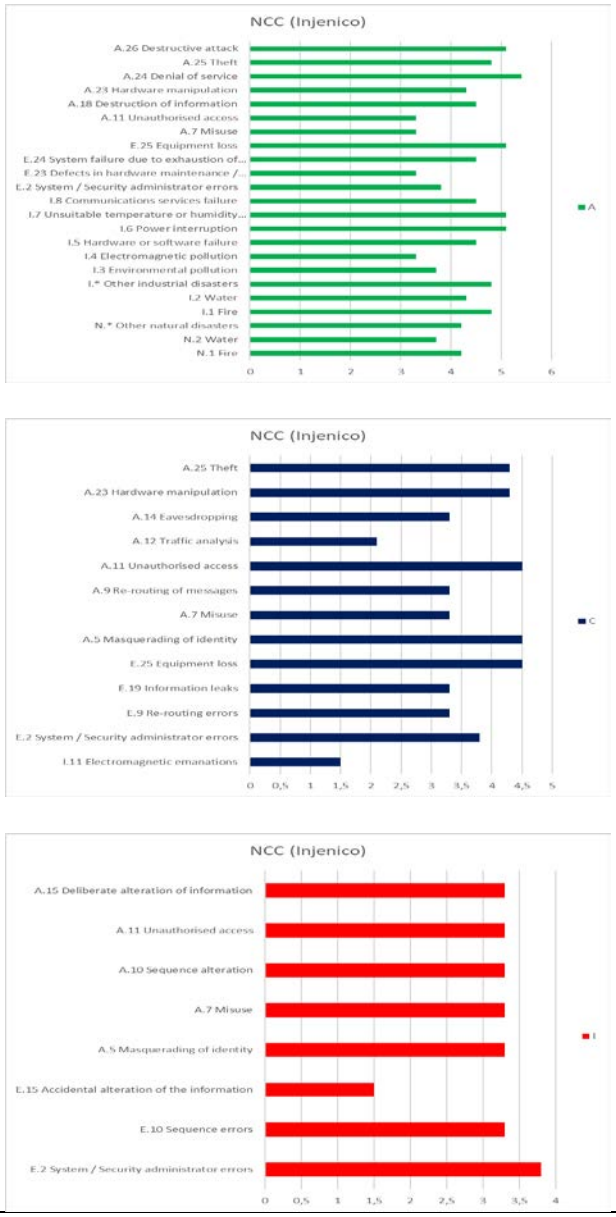


Διάγραμμα 87: 77,20 Checkpoint 5506/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού 77,20 Checkpoint 5506. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

Διάγραμμα 88: Cisco 2960X/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού Cisco 2960CX. Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).



Διάγραμμα 89: NCC (Injenico)/ risk (A, C, I) MAGERIT

Το παραπάνω διάγραμμα αποτυπώνει τον βαθμό επικινδυνότητας που χαρακτηρίζει το αγαθό του οργανισμού NCC (Injenico). Συγκεκριμένα, το αγαθό αυτό έχει κρίσιμο επίπεδο επικινδυνότητας απέναντι σε Destructive attack (A), Denial of Service (A), Equipment loss (A), Unsuitable humidity or temperature conditions (A), Power Interruption (A), ενώ, έχει μεγάλο επίπεδο επικινδυνότητας απέναντι σε Theft (C), Hardware manipulation (C), Unauthorised access (C), Masquerading identity και Equipment loss (C).

4.4. **ΠΡΟΣΟΜΟΙΩΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ** MEHARI

Μετά από εκτέλεση των απαιτούμενων προπαρασκευαστικών βημάτων που ορίζει η μεθοδολογία MEHARI, από το εργαλείο (ειδικά διαμορφωμένο υπολογιστικό φύλλο MS Excel) που χρησιμοποιήθηκε προέκυψαν τα παρακάτω αποτελέσματα που αφορούν την αξιολόγηση των αγαθών του σεναρίου ως προς τον βαθμό επίπτωσης (impact) στους τρείς άξονες της Διαθεσιμότητας (Availability-A), Εμπιστευτικότητας (Confidentiality-C) και Ακεραιότητας (Integrity-I).

Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από την MEHARI με την εννοιολογική της περιγραφή

Επίπεδο Επίπτωσης	Περιγραφή
1	**Μικρή επίπτωση**
2	Μέτρια επίπτωση
3	**Μεγάλη επίπτωση**
4	Κρίσιμη επίπτωση

Πίνακας 10**: Η κλίμακα του επιπέδου επίπτωσης (**impact**) της μεθοδολογίας** MEHARI

Διάγραμμα 90: **Το επίπεδο επίπτωσης (**impact**) των υποκατηγοριών της κατηγορίας** Data and information **αγαθών ως προς** A, I **και** C, MEHARI

Διάγραμμα 91**: Το επίπεδο επίπτωσης (**impact**) των υποκατηγοριών της κατηγορίας** Services **αγαθών ως προς** A, I **και** C, MEHARI

4.4.1. **Γενικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** MEHARI - **Επίπτωση**

Μετά από μελέτη των ανωτέρω σχημάτων προκύπτει ότι ως προς τον άξονα της Διαθεσιμότητας (Availability-A) η υποκατηγορία των αγαθών που κατατάσσονται στα Data and Information που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι η Data files and data bases accessed by applications. Τα υπόλοιπα αγαθά ανήκουν σε υποκατηγορίες που έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality-C) κρίσιμο επίπεδο επίπτωσης παρουσιάζει η υποκατηγορία των αγαθών Data files and data bases accessed by applications. Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν οι Shared office files and data, Personal office files (on user work stations and equipment), Written or printed information and data kept by users and personal archives, Listings or printed documents, Exchanged messages-screen views-data individually sensitive, electronic mailing, (Post) Mails and faxes, Patrimonial archives or documents used as proofs, IT related Archives, Data and information published on public or internal sites Τα υπόλοιπα αγαθά ανήκουν σε υποκατηγορίες που έχουν μέτριο και μικρό επίπεδο επίπτωσης. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Τέλος, ως προς τον άξονα της Ακεραιότητας (Integrity-I) κρίσιμο επίπεδο επίπτωσης παρουσιάζει η υποκατηγορία των αγαθών Data files and data bases accessed by applications. Ενώ, μεγάλο βαθμό επίπτωσης παρουσιάζουν οι Shared office files and data, Personal office files (on user work stations and equipment), Exchanged messages-screen views-data individually sensitive, electronic

mailing, (Post) Mails and faxes, IT related Archives, Data and information published on public or internal sites Τα υπόλοιπα αγαθά ανήκουν σε υποκατηγορίες που έχουν μέτριο και μικρό επίπεδο επίπτωσης. Τα υπόλοιπα αγαθά έχουν μέτριο και μικρό επίπεδο επίπτωσης.

Κατά αντίστοιχο τρόπο προκύπτει ότι ως προς τον άξονα της Διαθεσιμότητας (Availability-A) οι υποκατηγορίες των αγαθών που κατατάσσονται στα Services που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι οι User workspace and environment, Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), "Users' disposal of Equipment (workstations, local printers, peripherals, specific interfaces, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.). Ενώ, μεγάλο επίπεδο επίπτωσης παρουσιάζει η υποκατηγορία Web editing Service (internal or public).

Ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality-C) κρίσιμο επίπεδο επίπτωσης (impact) είναι η υποκατηγορία Services provided by applications.

Τέλος, ως προς τον άξονα της Ακεραιότητας (Integrity-I) πολύ μεγάλο επίπεδο επίπτωσης (impact) είναι οι Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), "Users' disposal of Equipments (workstations, local printers, peripherals, specific interfaces, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.). Ενώ, μεγάλο επίπεδο επίπτωσης παρουσιάζει η υποκατηγορία Web editing Service (internal or public).

Στην συνέχεια, γίνεται παράθεση και σχολιασμός των αποτελεσμάτων του επιπέδου επικινδυνότητας (risk) κάθε αγαθού συναρτήσει των κινδύνων που πρόκειται να αντιμετωπίσει κατά την λειτουργία του.

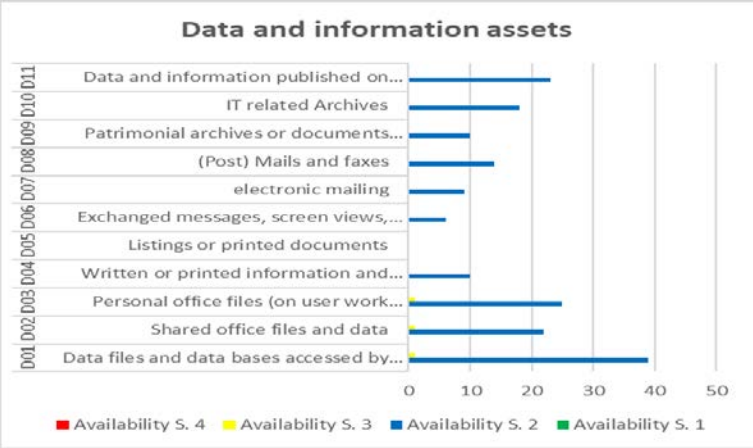
Η MEHARI ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την κατηγορία/είδος τους και υπολογίζει την επικινδυνότητα σύμφωνα με τις απειλές που πλήττουν την κάθε υποκατηγορία αυτών και στους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα). Λόγω της ιδιαιτερότητας αυτής καθώς και της χρήσης από το εργαλείο της MEHARI βιβλιοθηκών με μεγάλο πλήθος απειλών ανά υποκατηγορία αγαθών, θα γίνει παρουσίαση του πλήθους των απειλών ανά υποκατηγορία αγαθών ανά επίπεδο επικινδυνότητας.

Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από την MEHARI με την εννοιολογική της περιγραφή.

Επίπεδο Επικινδυνότητας	Περιγραφή
1	Μικρός κίνδυνος
2	Μέτριος κίνδυνος
3	Μεγάλος κίνδυνος
4	Πολύ μεγάλος κίνδυνος

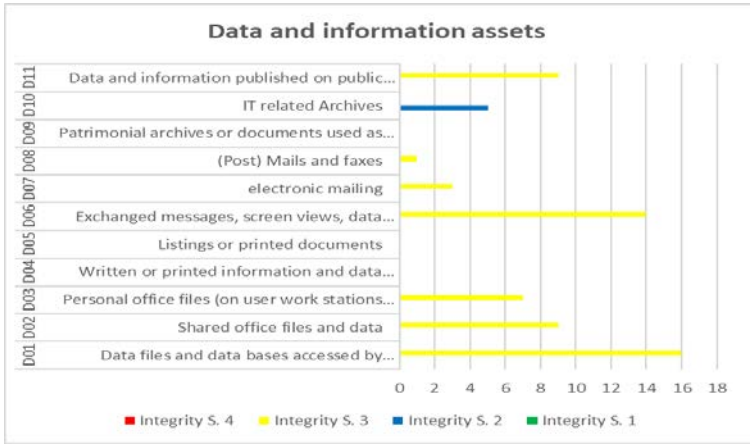
Πίνακας 11: Η κλίμακα του επιπέδου επικινδυνότητας της μεθοδολογίας MEHARI

4.4.2. **Αναλυτικός σχολιασμός αποτελεσμάτων της μεθοδολογίας** MEHARI - **Επικινδυνότητα**



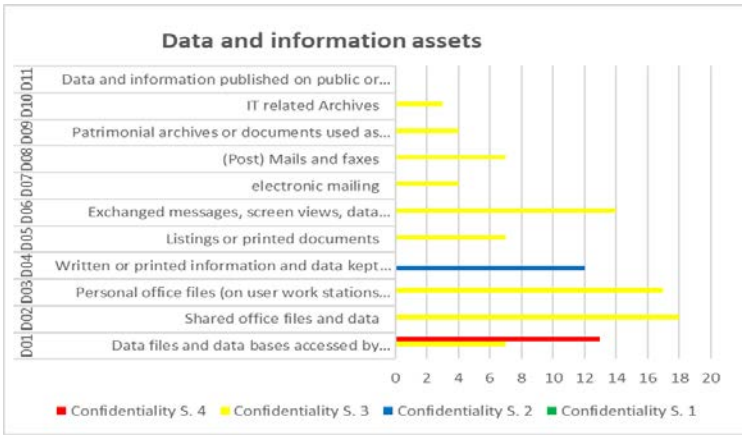
Διάγραμμα 92: Data and information assets/ risk (A) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Διαθεσιμότητας (Availability) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Data and Information. Συγκεκριμένα, στις υποκατηγορίες Data files and data bases accessed by applications, Shared office files and data, Personal office files (on user work stations and equipment) υπάρχει από μία απειλή με μεγάλο επίπεδο επικινδυνότητας, ακόμα αξίζει να σημειωθεί ότι στην υποκατηγορία Data files and data bases accessed by applications υπάρχουν 39 απειλές με μέτριο επίπεδο επικινδυνότητας ενώ οι Shared office files and data, Personal office files (on user work stations and equipment), Data and information published on public or internal sites έχουν και αυτές πάνω από 20 απειλές με μέτριο επίπεδο επικινδυνότητας.



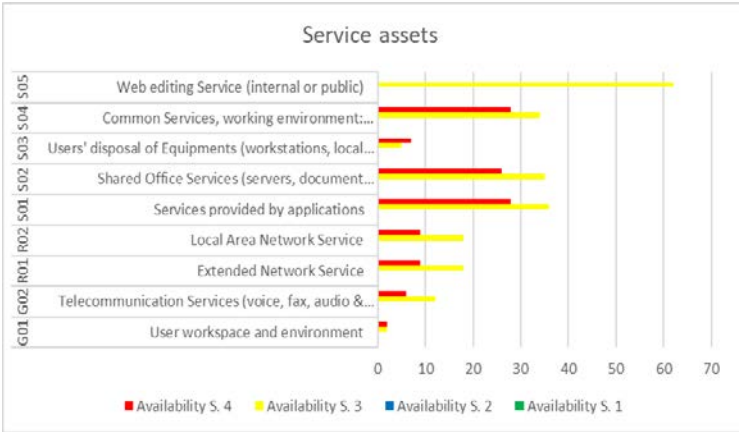
Διάγραμμα 93: Data and information assets/ risk (I) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Ακεραιότητας (Integrity) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Data and Information. Συγκεκριμένα, στις υποκατηγορίες Data files and data bases accessed by applications και Exchanged messages-screen views-data individually sensitive υπάρχουν 16 και 12 απειλές με μεγάλο επίπεδο επικινδυνότητας, ενώ, οι Shared office files and data, Personal office files (on user work stations and equipment), Data and information published on public or internal sites έχουν και αυτές πάνω από 6 απειλές με μεγάλο επίπεδο επικινδυνότητας.



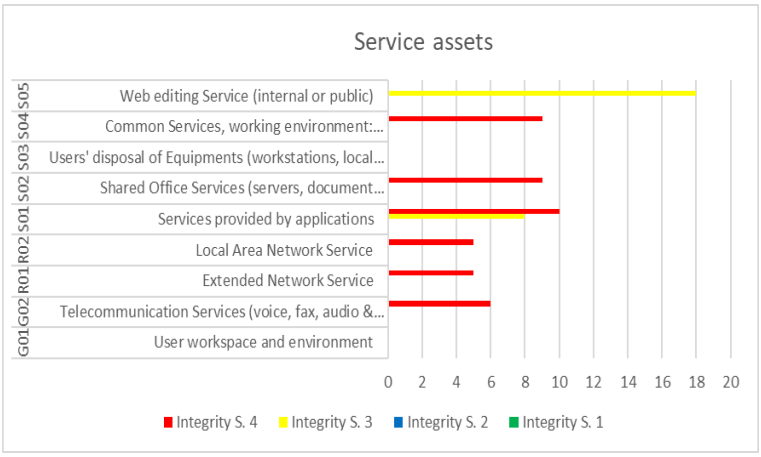
Διάγραμμα 94: Data and information assets/ risk (C) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Data and Information. Συγκεκριμένα, στην υποκατηγορία Data files and data bases accessed by applications υπάρχουν 13 απειλές με πολύ μεγάλο επίπεδο επικινδυνότητας και 18 με μεγάλο επίπεδο επικινδυνότητας, ενώ, οι Shared office files and data, Personal office files (on user work stations and equipment's Exchanged messages-screen views-data individually sensitive έχουν και αυτές πάνω από 14 απειλές με μεγάλο επίπεδο επικινδυνότητας.



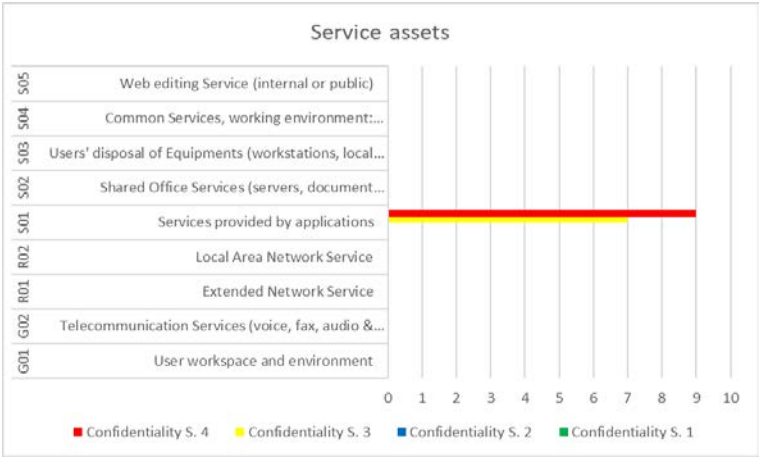
Διάγραμμα 95: Services assets/ risk (A) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Διαθεσιμότητας (Availability) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Services. Συγκεκριμένα, στις υποκατηγορίες User workspace and environment, Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), "Users' disposal of Equipment (workstations, local printers, peripherals, specific interfaces, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.) υπάρχουν από 2 έως 28 απειλές με πολύ μεγάλο επίπεδο επικινδυνότητας, ενώ, οι Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.), Web editing Service (internal or public) έχουν πάνω από 30 απειλές με μεγάλο επίπεδο επικινδυνότητας με την Web editing Service (internal or public) να έχει πάνω από 60.



Διάγραμμα 96: Services assets/ risk (I) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Ακεραιότητας (Integrity) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Services. Συγκεκριμένα, στις υποκατηγορίες Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.) υπάρχουν από 3 έως 9 απειλές με πολύ μεγάλο επίπεδο επικινδυνότητας, ενώ, οι Services provided by applications, Web editing Service (internal or public) έχουν 18 και 8 απειλές αντίστοιχα με μεγάλο επίπεδο επικινδυνότητας.



Διάγραμμα 97: Services assets/ risk (C) MEHARI

Το παραπάνω διάγραμμα αποτυπώνει ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality) το πλήθος των απειλών ανά υποκατηγορία και ανά επίπεδο επικινδυνότητας των αγαθών που ανήκουν στην κατηγορία Services. Συγκεκριμένα, στην υποκατηγορία Services provided by applications υπάρχουν 9 απειλές με πολύ μεγάλο επίπεδο επικινδυνότητας και 7 απειλές με μεγάλο επίπεδο επικινδυνότητας.

4.5. ΕΡΓΑΣΤΗΡΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΡΟΣΟΜΟΙΩΣΗΣ

4.5.1. Επίπτωση

Παρακάτω θα γίνει σύγκριση των αποτελεσμάτων του επίπεδου επίπτωσης μεταξύ των τριών μεθοδολογιών (CRAMM, MAGERIT, MEHARI) της προσομοίωσης για το επιλεγμένο σενάριο. Η σύγκριση για την εξαγωγή κατάλληλων συμπερασμάτων θα γίνει για κάθε έναν από τους τρείς άξονες μελέτης (Διαθεσιμότητα, Εμπιστευτικότητα, Ακεραιότητα).

4.5.1.1. Διαθεσιμότητα (Availability)

Από τον σχολιασμό της επίπτωσης, για κάθε μια μεθοδολογία ως προς τον άξονα της Διαθεσιμότητας (Availability-A), τα κοινά αγαθά που παρατηρείται πως παρουσιάζουν τόσο στην CRAMM όσο και στην MAGERIT κρίσιμο επίπεδο επίπτωσης (impact) είναι τα εξής οκτώ (8): Active Directory Primary PC, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, NCC (Injenico), Cisco 2960 (Node 1) και το APV 1600 (Node1), με την MAGERIT να περιλαμβάνει στα αγαθά κρίσιμου επιπέδου δύο (2) ακόμα (Web UI MTMS, 170.2a.EX7).

Όσον αφορά την MEHARI μεθοδολογία, στον σχολιασμό της επίπτωσης ως προς την Διαθεσιμότητα προκύπτει ότι η υποκατηγορία των αγαθών, τα οποία κατατάσσονται στα Data and Information, που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι η Data files and data bases accessed by applications. Μετά από μελέτη του υπολογιστικού φύλλου (MS Excel) που χρησιμοποιείται ως εργαλείο εκπόνησης της προσομοίωσης διαπιστώνεται πως στην κατηγορία αυτή τα αποτελέσματα

ταυτίζονται με αυτά της MAGERIT μεθοδολογίας, ενώ, για τις υποκατηγορίες των αγαθών που κατατάσσονται στα Services που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης [User workspace and environment, Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), "Users' disposal of Equipment (workstations, local printers, peripherals, specific interfaces, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.)] προστίθενται στην λίστα και τα εξής εννέα (9) αγαθά (Active Directory Secondary PC, TaxCard DB, MTMS DB, Proxy, Admin PCs, Developers PCs, Proxy Server, Call Center, Admins PCs).

4.5.1.2. Εμπιστευτικότητα (Confidentiality)

Από τον σχολιασμό της επίπτωσης, για κάθε μια μεθοδολογία ως προς τον άξονα της Εμπιστευτικότητας (Confidentiality-C), τα κοινά αγαθά που παρατηρείται πως παρουσιάζουν τόσο στην CRAMM όσο και στην MAGERIT κρίσιμο επίπεδο επίπτωσης (impact) είναι τα εξής εννέα (9): Active Directory Primary PC, Active Directory Secondary PC, TaxCard DB, MTMS DB, MTMS COM (VM), MTMS UAT, ERP DB, ibank Mid Server και Ingestate, με τις δύο μεθοδολογίες να ταυτίζονται απόλυτα.

Όσον αφορά την MEHARI μεθοδολογία, στον σχολιασμό της επίπτωσης ως προς την Εμπιστευτικότητα προκύπτει ότι η υποκατηγορία των αγαθών, τα οποία κατατάσσονται στα Data and Information, που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι η Data files and data bases accessed by applications. Μετά από μελέτη του υπολογιστικού φύλλου (MS Excel) που χρησιμοποιείται ως εργαλείο εκπόνησης της προσομοίωσης διαπιστώνεται πως στην κατηγορία αυτή τα αποτελέσματα ταυτίζονται με αυτά των CRAMM και MAGERIT μεθοδολογιών, ενώ, για την υποκατηγορία των αγαθών που κατατάσσονται στα Services που παρουσιάζει κρίσιμο επίπεδο επίπτωσης Services provided by applications προστίθενται στην λίστα και τα εξής δύο (2) αγαθά (Proxy και Proxy Server).

4.5.1.3. Ακεραιότητα (Integrity)

Από τον σχολιασμό της επίπτωσης, για κάθε μια μεθοδολογία ως προς τον άξονα της Ακεραιότητας (Integrity-I), τα κοινά αγαθά που παρατηρείται πως παρουσιάζουν τόσο στην CRAMM όσο και στην MAGERIT κρίσιμο επίπεδο επίπτωσης (impact) είναι τα εξής οκτώ (8): Active Directory Primary PC, ERP DB, MTMS COM (VM), ibank Mid Server, Ingestate, NCC (Injenico), Cisco 2960 (Node 1) και το APV 1600 (Node1), με την CRAMM να περιλαμβάνει στα αγαθά κρίσιμου επιπέδου δύο (2) ακόμα (Web UI MTMS, 170.2a.EX7) και την MAGERIT επίσης δύο (2) ακόμα (TaxCard DB, MTMS DB).

Όσον αφορά την MEHARI μεθοδολογία, στον σχολιασμό της επίπτωσης ως προς την Διαθεσιμότητα προκύπτει ότι η υποκατηγορία των αγαθών, τα οποία κατατάσσονται στα Data and Information, που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης (impact) είναι η Data files and data bases accessed by applications. Μετά από μελέτη του υπολογιστικού φύλλου (MS Excel) που χρησιμοποιείται ως εργαλείο εκπόνησης της προσομοίωσης διαπιστώνεται πως στην κατηγορία αυτή τα αποτελέσματα ταυτίζονται με αυτά της MAGERIT μεθοδολογίας, ενώ, για τις υποκατηγορίες των αγαθών που κατατάσσονται στα Services που παρουσιάζουν κρίσιμο επίπεδο επίπτωσης [Telecommunication Services (voice, fax, audio & videoconferencing, etc.), Extended Network Service, Local Area Network Service, Services provided by applications, Shared Office Services (servers, document management, shared printers, etc.), "Users' disposal of Equipment (workstations, local printers, peripherals, specific interfaces, etc.), Common Services και working environment (messaging, archiving, print, editing, etc.)]

προστίθενται στην λίστα και τα εξής τέσσερα (4) αγαθά (Web UI MTMS, Proxy, Proxy Server και Call Center).

4.5.2. **Επικινδυνότητα**

Στην προσπάθεια να γίνει σύγκριση του επιπέδου επικινδυνότητας του επιλεγμένου σεναρίου όπως αυτό προκύπτει από κάθε μια από τις μεθοδολογίες CRAMM, MAGERIT και MEHARI μπορεί κανείς να συμπεράνει πως τα αποτελέσματα διαφέρουν σε μορφή, πλήθος και ποικιλία.

Όσον αφορά την CRAMM ως μεθοδολογία αυτό οφείλεται επειδή στην φάση υπολογισμού της επικινδυνότητας αυτή μελετά τα αγαθά λαμβάνοντας υπόψιν μόνο την μέγιστη τιμή της επίπτωσης (impact) μεταξύ των τριών (3) αξόνων (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα) για κάθε απειλή που πλήττει το αγαθό, ενώ οι βιβλιοθήκες των απειλών προκύπτει, από σύγκριση με αυτές των άλλων μεθοδολογιών, ότι είναι σημαντικά περιορισμένη σε πλήθος και ποικιλία. Συνεπώς τα αποτελέσματα της δεν προσφέρονται για διεξοδική ανάλυση επικινδυνότητας ανά άξονα μελέτης αλλά παρέχουν μια συνολική εκτίμηση του επιπέδου επικινδυνότητας κάθε αγαθού του οργανισμού υπό μελέτη.

Από την πλευρά της, η MAGERIT ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την τιμή της επίπτωσης (impact) κάθε αγαθού ξεχωριστά για κάθε απειλή ως προς και τους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα), ενώ οι βιβλιοθήκες των απειλών προκύπτει, από σύγκριση με αυτές των άλλων μεθοδολογιών, ότι είναι κατάλληλες τόσο σε πλήθος όσο και σε ποικιλία ώστε να καλύπτουν όσο το δυνατό περισσότερα σενάρια κινδύνων που μπορεί να κληθεί να αντιμετωπίσει ο υπό μελέτη οργανισμός. Συνεπώς τα αποτελέσματα της προσφέρονται για διεξοδική ανάλυση επικινδυνότητας ανά άξονα μελέτης και παρέχουν μια ικανοποιητική εκτίμηση του επιπέδου επικινδυνότητας κάθε αγαθού του οργανισμού υπό μελέτη.

Τέλος, η MEHARI ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την κατηγορία/είδος τους και υπολογίζει την επικινδυνότητα σύμφωνα με τις απειλές που πλήττουν την κάθε υποκατηγορία αυτών και στους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα). Αυτή η ιδιαιτερότητα της MEHARI σε συνδυασμό με τις άκρως εκτενείς και λεπτομερείς βιβλιοθήκες απειλών την καθιστούν σε πάρα πολύ μεγάλο βαθμό αναλυτική αλλά ταυτόχρονα πολύπλοκη και κατ’ επέκταση δύσκολή στην μελέτη για μη έμπειρους χρήστες.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι οργανισμοί, που αποτελούν κρίσιμές υποδομές, λειτουργούν σε ένα περιβάλλον υψηλής πολυπλοκότητας και διασύνδεσης. Αυτή η λειτουργικότητα εδράζεται σαφώς στα πληροφοριακά συστήματα που διαθέτουν. Η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος. Σε συστήματα που περιέχουν ευαίσθητα δεδομένα οι επιπτώσεις δεν είναι μόνο οικονομικής αλλά και ζωτικής σημασίας, καθιστώντας την ασφάλεια των πληροφοριακών συστημάτων ακρογωνιαίο λίθο για τη σύγχρονη κοινωνία.

Οι οργανισμοί χρησιμοποιούν την ανάλυση επικινδυνότητας για να καθορίσουν την έκταση των πιθανών απειλών και τους κινδύνους που σχετίζονται με ένα πληροφοριακό σύστημα. Η έννοια της επικινδυνότητας υποκαθιστά τον αόριστο στόχο της επίτευξης της ασφάλειας με τον εφικτό και μετρήσιμο στόχο του περιορισμού της επικινδυνότητας εντός αποδεκτών ορίων. Το αποτέλεσμα αυτής της διεργασίας συντελεί στην αναγνώριση των κατάλληλων ελέγχων για την πρόληψη και τον περιορισμό των κινδύνων και στην καλύτερη κατανόηση των εσωτερικών διαδικασιών του οργανισμού. Για την αξιολόγηση/αποτίμηση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων εφαρμόζονται τεχνικές ανάλυσης επικινδυνότητας. Η ανάλυση επικινδυνότητας εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών, όσο και στην αποτίμηση των απειλών και τρωτοτήτων. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων, τη συστηματικότητα των μεθόδων ανάλυσης επικινδυνότητας και την «αντικειμενικότητα» των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.

Στην παρούσα μεταπτυχιακή διατριβή, ο υπό μελέτη οργανισμός (χρηματοπιστωτικό ίδρυμα και ειδικότερα το κομμάτι του IT που εμπλέκεται στην εκτέλεση διατραπεζικών συναλλαγών) αποτελεί μέρος κρίσιμης υποδομής. Ο συγκεκριμένος οργανισμός επιλέχθηκε με στόχο να βρεθεί η καταλληλότερη μεθοδολογία για την υλοποίηση ανάλυσης επικινδυνότητας σε αυτόν, όπως απαιτείται από τα διεθνή πρότυπα τα οποία διέπουν την λειτουργία αυτού. Με κύριο στόχο της μελέτης του συγκεκριμένου σεναρίου να είναι η σύγκριση της ανάλυσης επικινδυνότητας των τριών μεθοδολογιών (CRAMM, MAGERIT, MEHARI), και όχι η σύγκριση και των προτεινόμενων αντιμέτρων των μεθοδολογιών, προκύπτει ότι δεν μπορεί κανείς να ξεχωρίσει κάποια μεθοδολογία μόνο από τα πρωτογενή της αποτελέσματα. Κάθε μεθοδολογία έχει τις ιδιαιτερότητες της, τα δυνατά της και αδύναμά της σημεία, τομείς που επικεντρώνεται και τομείς που η ανάλυση της κρίνεται λιγότερο λεπτομερής.

Συνεπώς κάθε αναλυτής επικινδυνότητας ενός οργανισμού, που αποτελεί μέρος μια κρίσιμής υποδομής, πρέπει να επιστρατεύσει, με οδηγό την κριτική και συνδυαστική σκέψη, την εμπειρία και τη γνώση που προκύπτει από μελέτες όπως η παρούσα, που αφορούν τα ιδιαίτερα χαρακτηριστικά κάθε μεθοδολογίας πριν κάνει την επιλογή της μεθοδολογίας ή του συνδυασμού μεθοδολογιών ανάλυσης επικινδυνότητας που θα χρησιμοποιήσει.

Για τον συγκεκριμένο οργανισμό προτείνεται η χρήση της μεθοδολογίας MAGERIT, η οποία βάσει των αναγκών και των απαιτήσεων του οργανισμού είναι η πιο κοντινή μεθοδολογία που μπορεί να εφαρμοστεί. Η MAGERIT ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την τιμή της επίπτωσης (impact) κάθε αγαθού ξεχωριστά για κάθε απειλή ως προς και τους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα), ενώ οι βιβλιοθήκες των απειλών προκύπτει, από σύγκριση με αυτές των άλλων μεθοδολογιών, ότι είναι κατάλληλες τόσο σε πλήθος, όσο και σε ποικιλία ώστε να καλύπτουν όσο το δυνατό περισσότερα σενάρια κινδύνων που μπορεί να κληθεί να αντιμετωπίσει ο υπό μελέτη οργανισμός.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission under Contract TREN/C1/185/200. 2010. Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.

[2] Alberts C., Dorofee A. (2001). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method Implementation Guide, v2.0. Software Engineering Institute, Carnegie Mellon University, http://www.cert.org/octave/.

[3] Balmat J., Lafont F., Maifret R., Pessel N., (2009). "MAritime RISk Assessment (MARISA), a fuz-zy approach to define an individual ship risk factor", Ocean Engineering, Vol. 36, No. 15-16, pp. 1278-1286

[4] Bourguignon, F., Ferreira, F. and Leite, P. (2002). Ex-ante evaluation of conditional cash transfer programs: the case of Bolsa Escola. Policy Research Working Paper 2916. World Bank, Policy Research Department, Washington D.C

[5] Browne, M. W., & Cudeck, R. (1989). Single sample cross-validation indices for covariance structures. Multivariate Behavioral Research, 24(4), 445-455.

[6] Bryman, A. (2012). Social research methods. Oxford university press.

[7] BSI Standard 100-1 (2005). Information Security Management Systems (ISMS) www.bsi.bund.de.

[8] BSI Standard 100-2. (2005). IT - Grundszchutz methodology. (www.bsi.bund.de)

[9] BSI Standard 100-3. (2005). Risk analysis based on IT–Grundszchutz (www.bsi.bund.de)

[10] Burgess, P. (2006). Social values and the logic of threat: the European Programme for Critical Infrastructures Protection (EPCIP). In Critical Infrastructure Protection Conference, Utrecht (Vol. 8). Bush, G. W. (2003). Homeland Security Presidential Directive (HSPD-7): Critical infrastructure identification, prioritization, and protection. Washington, DC: White House.

[11] Campbell, P. L., & Stamp, J. E. (2004). A classification scheme for risk assessment methods. United States. Department of Energy.

[12] Carr, M. J., Konda, S. L., Monarch, I. A., Ulrich, F. C., & Walker, C. F. (1993). T axonomy-Based Risk Identification. SEI Technical Report SEI-93-TR-O06, Pittsburgh, PA: Software Engineering Institute.

[13] Champlain J., Auditing Information Systems, Second Edition, Editura Wiley USA, 2003.

[14] Chevalier, Judith, and Glenn Ellison, 1997, "Risk Taking by Mutual Funds as a Response to Incentives," Journal of Political Economy 105, 1167-1200.

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

[16] Congressional Budget Office. (1983). Public works infrastructures: Policy considerations for the 1980s., Government Printing Office.

[17] Craft, R. (1998). An Open Framework for Risk Management, Proceedings of the 21st National Information Systems Security Conference, Arlington, USA.

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

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

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

[21] Downs B., (2007). "The Maritime Security Risk Analysis Model", in USCG Proc. of the Marine Safety and Security Council, (http://www.uscg.mil/proceedings/)

[22] Ebios (2010). Expression of Needs and Identification of Security Objectives Premier Ministre Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil. (www.ssi.gouv.fr)

[23] El Fray, I. (2012). A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. In Computer Information Systems and Industrial Management (pp. 428-442). Springer Berlin Heidelberg. J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). Report to the President's Commission on Critical Infrastructure Protection (No. CMU/SEI-97-SR-00333). Carnegie-Mellon University, Pittsburgh.

[24] Elachgar H., Regragui B. (2012). Information Security, new approach, Conf. Innovative Computing Technology (INTECH), IEEE

[25] ENISA Report, (2011). "Analysis of cyber security aspects in the maritime sector", http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector/cyber-security-aspects-in-the-maritime-sector-1, last accessed March 4, 2014.

[26] ENISA. (2006). Inventory of Risk Management/Risk Assessment methods and tools. Last accessed 16 October 2014 http://www.enisa.europa.eu/rmra/rm_home.htm

[27] Froot, Kenneth A., and Jeremy C. Stein, 1998, "Risk Management, Capital Budgeting, and Capital Structure Policy for Financial Institutions: An Integrated Approach," Journal of Financial Economics 47, 55-82.

[28] Georgios Makrodimitris, Nineta Polemi, and Christos Douligeris, Security Risk Assessment Challenges in Port Information Technology Systems University of Piraeus, Department of Informatics, 80, Karaoli & Dimitriou St., 185 34 Piraeus, Greece

[29] Humphreys, E. (2011). Information security management system standards. Datenschutz und Datensicherheit-DuD, 35(1), 7-11.

[30] Insight Consulting, CRAMM User Guide (2005). Issue 5.1, United Kingdom

[31] ISAMM-Information Security Assessment & Monitoring Method (2002) http://www.telindus.com

[32] ISO/IEC 13335: 1998. Information Technology-Guidelines for the management of IT Security-Part 3: Techniques for the management of IT Security. International Organization for Standardization.

[33] ISO/IEC 27001:2005. Information technology-security techniques-information security management systems-requirements. International Organization for Standardization.

[34] ISO/IEC:27002 (2005). Information technology - Security techniques - Code of practice for information security management, http://www.iso.org

[35] ISO/IEC:27005 (2008). Information Technology - Security Techniques - Information Security Risk Management, http://www.iso.org

[36] Johnson, H. Thomas, 1991, "Managing by Remote Control: Recent Management Accounting Practice in Historical Perspective," in Peter Temin, ed., Inside the Business Enterprise. Chicago: University of Chicago Press for NBER.

[37] Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk analysis, 1(1), 11-27.

[38] Karolak, D. W., & Karolak, N. (1995). Software engineering risk management: A just-in-time approach. IEEE Computer Society Press.

[39] Kitchenham, B., Linkman, S., & Law, D. (1997). DESMET: a methodology for evaluating software engineering methods and tools. Computing & Control Engineering Journal, 8(3), 120-126.

[40] Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering & System Safety, 93(12), 1781-1787.

[41] Kurowski, S., Zibuschka, J., Roßnagel, H., & Engelbach, W. (2012). A Survey of Interoperability Concepts for Security Systems in Public Transport. Mobility in a Globalised World, 6, 91. Landoll, D. J., & Landoll, D. (2005). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC Press.

[42] Lichtenstein, S. (1996). Internet acceptable usage policy. Computer Audit Update, 1996(12), 10-21.

[43] López D., Pastor O., García Villalba L.J. (2013). Dynamic Risk Assessment In Information Systems: State-Of-The-Art, ICIT 2013 South Africa

[44] Manas, J. A. (2009). PILAR–Risk Analysis and Management Tool. (Last accessed 15 November 2014) http://www.pilar-tools.com/en/tools/pilar/v54/help_en/cia/index.html

[45] Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI), (2007). Data Management Working Group, Spiral 2, Vocabulary Handbook Version 2.0.2, http://www.uscg.mil/acquisition/nais/RFP/SectionJ/MDA-COI-vocab.pdf

[46] Markowsky, G. (2011). Universal asset assessment system based on excel™. In Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011 IEEE 6th International Conference on (Vol. 2, pp. 747-752). IEEE.

[47] Mayerfeld, H. T. (1989). Framework for Risk Management. A Synthesis of the Working Group Reports from the First Computer Security Risk Management Model Builders Workshop. In Proceedings of the Second Computer Security Risk Management Model Builders Workshop (pp. 1-19).

[48] Mays, N., & Pope, C. (2000). Assessing quality in qualitative research. Bmj, 320(7226), 50-52.

[49] McManus, J. (2012). Risk management in software development projects. Routledge.

[50] McNeil, A. J., Frey, R., & Embrechts, P. (2010). Quantitative risk management: concepts, techniques, and tools. Princeton university press.

[51] Min, H. S. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. Iie Transactions, 39(1), 57-71.

[52] Mirkin, B.G., 1979. Group Choice, Halsted Press, New York.

[53] Morgan, M. G., Florig, H. K., DeKay, M. L., & Fischbeck, P. (2000). Categorizing risks for risk ranking. Risk analysis, 20(1), 49-58.

[54] Munteanu, A. (2006). Information security risk assessment: The qualitative versus quantitative dilemma. In Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference (pp. 227-232).

[55] Myers, Stewart C., and Nicholas S. Majluf, 1984, "Corporate Financing and Investment Decisions When Firms Have Information That Investors Do Not Have," Journal of Financial Economics 13, 187-221.

[56] Nastase P, Stanciu V, Eden A., Auditul si controlul sistemelor informationale,Editura ECONOMICA , Bucuresti, 2007.

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

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

[59] Ntouskas T., Polemi N. (2012a). Collaborative security management services for Port Information Systems", in Proc. of International Conference on e-Business, pp. 305-308, SciTePress, Italy

[60] Ntouskas T., Polemi N. (2012b). STORM-RM: A collaborative and multicriteria risk management methodology, International Journal of Multicriteria Decision Making, Vol. 2, No. 2, pp. 159-177

[61] Ntouskas T., Polemi N., (2010b). STORM-RA: An implemented, collaborative, multicriteria decision making risk assessment methodology, 7th Meeting Multicriteria Decision Analysis, Greece

[62] OCTAVE Method Implementation Guide Version 2.0 (2010). Carnegie Mellon University, June 2001. Available at http://www.cert.org/octave/

[63] Peltier, T. R. (2005). Information security risk analysis. CRC press.

[64] Pickard, A. J. (2013). Research methods in information. Facet Publications.

[65] Polemi N. (2013). Security management of the ports' information systems. ENISA project, http://www.enisa.europa.eu last accessed March 4, 2014

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

[67] Pritsker, Matthew, 1997, "Evaluating Value at Risk Methodologies: Accuracy versus Computational Time," Journal of Financial Services Research 12, 201-241.

[68] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE, 21(6), 11-25.

[69] S. ichael Gibson, The Implications of Risk Management Information, Federal Reserve Board

[70] Systems for the Organization of Financial Firms

[71] Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 800-30.

[72] Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. Mis Quarterly, 441-469.

[73] Subramanian, N., & Ramanathan, R. (2012). A review of applications of Analytic Hierarchy Process in operations management. International Journal of Production Economics, 138(2), 215-241.

[74] Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. Information & Management, 41(2), 149-158.

[75] Syalim A., Hori Y., Sakurai K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, International Conference on Availability, Reliability and Security

[76] Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-based criticality In Critical infrastructure protection III (pp. 35-49). Springer Berlin Heidelberg.

[77] Thompson, K. M., & Graham, J. D. (1996). Going beyond the single number: using probabilistic risk assessment to improve risk management. Human and Ecological Risk Assessment, 2(4), 1008-1034.

[78] Tipton, H. F., & Krause, M. (2012). Information security management handbook. CRC Press.

[79] Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. Procedia Computer Science, 3, 881-887.

[80] Turner, B. L., Kasperson, R. E., Matson, P. A., McCarthy, J. J., Corell, R. W., Christensen, L., & Schiller, A. (2003). A framework for vulnerability analysis in sustainability science. Proceedings of the national academy of sciences, 100(14), 8074-8079.

[81] United Kingdom Central Computer and Telecommunication Agency (1996), CCTA Risk Analysis and Management Method: User Manual, version 3.0 edition, HMSO, London.

[82] Utne, I. B., Hokstad, P., & Vatn, J. (2011). A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety, 96(6), 671-678.

[83] Vose, D. (2008). Risk analysis: a quantitative guide. John Wiley & Sons.

[84] Wahlgren, G., Bencherifa, K., & Kowalski, S. (2013). A Framework for selecting IT Security Risk Management Methods based on ISO27005. In MIC-CPE 2013: 6th International Conference on Communications, Propagation and Electronics. Kenitra, Morocco: 1-3 Februari 2013. Academy Publisher.

[85] Wang, A. J. A. (2005). Information security models and metrics. In Proceedings of the 43rd annual Southeast regional conference-Volume 2 (pp. 178-184). ACM.

[86] Weber R., Information Systems Control and Audit, Editura Prentice Hall, USA, 1998. Bank for International Settlements, 1997, "Survey of Disclosures about Trading and Derivatives Activities of Banks and Securities Firms," Joint report by the Basle Committee on Banking Supervision and the Technical Committee of the International Organisation of Securities Commissions.

[87] Webler, T., Rakel, H., Renn, O., & Johnson, B. (1995). Eliciting and classifying concerns: A methodological critique. Risk Analysis, 15(3), 421-436.

[88] Weiss, J. (Ed.). (2010). Protecting industrial control systems from electronic threats. Momentum Press.

[89] Xenakis, C., & Wolthusen, S. (Eds.). (2011). Critical Information Infrastructure Security: 5th International Workshop, CRITIS 2010, Athens, Greece, September 2010, Revised Papers (Vol. 6712). Springer.

[90] Yazar, Z. (2002). A qualitative risk analysis and management tool–CRAMM. SANS InfoSec Reading Room White Paper.

[91] Zsidisin, G. A., Ellram, L. M., Carter, J. R., & Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. International Journal of Physical Distribution & Logistics Management, 34(5), 397-413.

[92] Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ.. (2003). Ασφάλεια Υπολογιστών και Δικτύων, Παπασωτηρίου.

[93] Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.). (2004). Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών.

[94] Σαραβάνου Μαρία-Χριστίνα, (2014), Μελέτη μεθόδων διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων και υλοποίηση μελέτης περίπτωσης (case study) με τη μέθοδο Magerit και το εργαλείο EAR/Pilar, , Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής, Αθήνα